CaMUS **4**, 1 – 15

Frises, polynômes continuants non signés et algorithme d'Euclide

Véronique Bazier-Matte

RÉSUMÉ Il est possible d'appliquer l'algorithme d'Euclide en se servant de frises semblables à celles étudiées par Conway et Coxeter. Pour ce faire, la première section de cet article définit et présente des propriétés de ces frises. Par la suite, une section est consacrée aux polynômes continuants non signés, puisqu'ils servent à établir un lien entre les frises et l'agorithme d'Euclide. Cet algorithme est donc présenté dans la section suivante, de même que la manière de l'appliquer avec des frises. Finalement, il est expliqué que trouver deux entiers s et t tels que $sa+tb=1$, où a et b sont deux entiers copremiers, nécessite de conserver moins de nombres en mémoire dans l'algorithme en se servant des frises, plutôt que de l'algorithme traditionnel d'Euclide.

1 Introduction

L'algorithme d'Euclide est un algorithme très puissant qui permet de calculer le plus grand dénominateur commun, noté (a,b) de deux entiers a et b et de trouver deux entiers s et t tels que $sa + tb = (a,b)$. Cet algorithme, élaboré environ 300 ans avant Jésus-Christ est encore utilisé aujourd'hui, entre autres, à des fins cryptographiques. Or, certains nombres utilisés au cours de l'algorithme d'Euclide peuvent s'exprimer comme l'évaluation d'un polynôme continuant non signé en fonction d'autres nombres issus de l'algorithme. Il existe aussi des liens entre les polynômes continuants non signés et les frises de nombres ressemblant à celles décrites par Conway et Coxeter [CC73]. Il est donc intéressant de se pencher sur les relations entre ces trois objets – les frises, les polynômes continuants et l'algorithme d'Euclide – et d'étudier comment les uns peuvent s'exprimer en fonction des autres. Cet article propose donc, premièrement, une étude des frises de nombres axée principalement sur la manière de les construire. Les frises étudiées dans cet article diffèrent de celles étudiées par Conway et Coxeter par la règle appliquée à chaque maille, mais conservent la même structure. Il s'agit en fait d'un cas particulier des frises étudiées dans [BMRDSM12]. Par la suite, les polynômes continuants non signés et leurs propriétés sont étudiés. Ceci mène à prouver que tout polynôme continuant peut être exprimé comme élément d'une

J'aimerais remercier le CRSNG pour le financement du stage. J'aimerais également remercier Ibrahim Assem pour son soutien et ses judicieux conseils. Finalement, un merci spécial à David Racicot-Desloges et à Tanna Sánchez McMillan pour leur aide.

frise où les polynômes continuants d'indice moins élevé se trouvent sur les rangées précédentes. Finalement, nous nous intéressons à l'algorithme d'Euclide en décrivant d'abord son fonctionnement pour ensuite expliciter les liens avec les polynômes continuants et donc, avec les frises. Pour conclure, nous élaborons une technique d'application de l'algorithme d'Euclide au moyen des frises.

2 Frises et règle anti-modulaire

Les définitions et les résultats énoncés dans cette section, de même que ceux dans la section suivante sont des cas particuliers de ceux que l'on retrouve dans [BMRDSM12].

Définition 2.1. Pour $n \geq 1$, notons B_n l'ensemble des paires $(i,j) \in \mathbb{Z}^2$ telles que $-2 \leq j-i \leq n+1$. Convenons de disposer ces paires de nombres de la façon suivante :

$$\begin{array}{ccccccccccccccccc}
 & (i{-}1,i{-}3) & & & & (i,i{-}2) & & & & (i{+}1,i{-}1) & & & & (i{+}2,i) & \\
 & & (i{-}1,i{-}2) & & & & (i,i{-}1) & & & & (i{+}1,i) & & & & \\
 & (i{-}2,i{-}2) & & & & (i{-}1,i{-}1) & & & & (i,i) & & & & (i{+}1,i{+}1) & \\
\cdots & & & \ddots & & & & \ddots & & & & \ddots & & & & \cdots \\
 & (i{-}3,i{+}n{-}4) & & & & (i{-}2,i{+}n{-}3) & & & & (i{-}1,i{+}n{-}2) & & & & (i,i{+}n{-}1) & \\
 & & (i{-}3,i{+}n{-}3) & & & & (i{-}2,i{+}n{-}2) & & & & (i{-}1,i{+}n{-}1) & & & & \\
 & (i{-}4,i{+}n{-}3) & & & & (i{-}3,i{+}n{-}2) & & & & (i{-}2,i{+}n{-}1) & & & & (i{-}1,i{+}n) &
\end{array}$$

Un *pavage de nombres* est une fonction $f : B_n \to \mathbb{Q}$.

Remarque 2.2. Les *rangées* d'un pavage sont définies de sorte que les éléments de la forme $(i,i+k-1)$ composent la k-ième rangée de ce pavage. Ainsi, un pavage de la forme ci-dessus comporte $n+4$ rangées, numérotées de -1 à $n+2$.

Exemple 2.3. Voici un pavage à cinq rangées :

$$\begin{array}{ccccccccccc}
 & \frac{1}{5} & & -1 & & \frac{1}{2} & & -5 & & & \\
 & & 3 & & 0 & & \frac{9}{4} & & & & \\
\cdots & 2 & & \frac{2}{3} & & 4 & & 2 & \cdots & & \\
 & & -\frac{5}{6} & & 11 & & \frac{3}{4} & & & & \\
 & -2 & & -1 & & 0 & & \frac{1}{7} & & &
\end{array}$$

Définition 2.4. Chaque portion de pavage de la forme

$$\begin{array}{ccc}
 & (i+1,j-1) & \\
(i,j-1) & & (i+1,j) \\
 & (i,j) &
\end{array}$$

est appelée *maille de but* $(i+1,j)$.

Définition 2.5. Une *frise de nombres* est un pavage de nombres $f : B_n \to \mathbb{Q}$, où chaque maille de but $(i+1,j)$ satisfait à la règle antimodulaire :

$$f(i,j-1)f(i+1,j) - f(i+1,j-1)f(i,j) = (-1)^{j-i},$$

de telle sorte que :

i) la rangée -1 est composée de 0, c'est-à-dire que $f(i,i-2)=0$ pour tout i ;

ii) la rangée 0 est composée de 1, c'est-à-dire que $f(i,i-1)=1$ pour tout i ;

iii) la rangée $n+1$ est composée de 1 ou de -1, c'est-à-dire que $f(i,i+n)=1$ ou -1 pour tout i ;

iv) La rangée $n+2$ est composée de 0, c'est-à-dire que $f(i,i+n+1)=0$ pour tout i.

Remarque 2.6.

a) En fixant ainsi les rangées -1 et 0, la règle antimodulaire est respectée sur les mailles de but $(i+1,i)$ pour tout i. En effet,

$$\begin{aligned} f(i,i-1)f(i+1,i)-f(i+1,i-1)f(i,i) &= 1\cdot 1-0\cdot f(i,i) \\ &= 1 \\ &= (-1)^{i-i} \text{ pour tout } i. \end{aligned}$$

b) De même, afin que la règle antimodulaire soit respectée sur toutes les mailles de but $(i+1,i+n+1)$, nous fixerons la rangée $n+1$ d'une frise à

$$\cdots \quad 1 \quad -1 \quad 1 \quad -1 \quad \cdots$$

si n est pair. De cette manière, nous retrouvons en alternance des mailles des formes suivantes dans les frises où n est pair :

$$\begin{array}{ccc} & f(i+1,i+n) & \\ -1 & & 1 \\ & 0 & \end{array} \quad \text{et} \quad \begin{array}{ccc} & f(i+1,i+n) & \\ 1 & & -1. \\ & 0 & \end{array}$$

Ainsi, on obtient que

$$\begin{aligned} &f(i,i+n)f(i+1,i+n+1)-f(i+1,i+n)f(i,i+n+1) \\ &\quad = 1\cdot -1-f(i,i+n+1)\cdot 0 \\ &\quad = -1 \\ &\quad = (-1)^{n+1}. \end{aligned}$$

Fixer la rangée $n+1$ à $\cdots \quad 1 \quad -1 \quad 1 \quad -1 \quad \cdots$ quand n est pair permet non seulement de toujours respecter la règle antimodulaire sur les mailles de but $(i+1,i+n+1)$, mais aussi de construire des frises composées d'entiers. En effet, il aurait été suffisant de fixer la rangée $n+1$ à :

$$\cdots \frac{a}{b} \quad -\frac{b}{a} \quad \frac{a}{b} \quad -\frac{b}{a} \cdots,$$

où $a,\ b \in \mathbb{N}_*$, car la fonction de frise aurait été respectée. Toutefois, ceci aurait empêché l'étude des frises d'entiers.

Par ailleurs, si n est impair, soit la rangée $n+1$ est composée entièrement de 1, soit elle est composée entièrement de -1. Pour chaque n impair, ces deux options sont possibles et permettent d'obtenir deux ensembles de frises différents. Nous retrouvons ainsi dans ces frises des mailles de l'une des deux formes suivantes :

$$\begin{array}{ccc} & f(i+1,i+n) & \\ 1 & & 1 \\ & 0 & \end{array} \quad \text{ou} \quad \begin{array}{ccc} & f(i+1,i+n) & \\ -1 & & -1. \\ & 0 & \end{array}$$

Ainsi, la règle antimodulaire est toujours respectée pour les mailles de but $f(i+1,i+n+1)$:

$$\begin{aligned} &f(i,i+n)f(i+1,i+n+1) - f(i+1,i+n)f(i,i+n+1) \\ &\quad = 1 - f(i,i+n+1)\cdot 0 \\ &\quad = 1 \\ &\quad = (-1)^{n+1}. \end{aligned}$$

Encore une fois, nous aurions pu fixer la rangée $n+1$ quand n est impair différemment, tout en respectant la règle antimodulaire. Toutefois, la fixer uniquement à 1 ou à -1 est la seule manière d'obtenir des entiers sur la rangée $n+1$, donc éventuellement sur la frise au complet. En effet, si nous l'avions fixé à

$$\cdots \ \tfrac{a}{b} \ \ \tfrac{b}{a} \ \ \tfrac{a}{b} \ \ \tfrac{b}{a} \ \cdots, \text{ où } a,\, b \in \mathbb{N}_*,$$

la règle antimodulaire aurait été respectée pour toute maille de but $(i+1,i+n+1)$, mais aucune frise ne serait composée que d'entiers.

Définition 2.7. L'*ordre* d'une frise, noté n, est le nombre de rangées non fixées qu'elle comporte. Autrement dit, il s'agit du nombre de rangées de la frise en excluant la rangée -1, la rangée 0, la rangée $n+1$ et la rangée $n+2$, soit les rangées fixées.

Exemple 2.8. Voici une portion d'une frise d'ordre 2 :

$$\begin{array}{ccccccccccccccccccc} & 0 & & 0 & & 0 & & 0 & & 0 & & 0 & \\ & & 1 & & 1 & & 1 & & 1 & & 1 & & \\ \cdots & -2 & & 2 & & -1 & & 3 & & -1 & & 2 & \cdots \\ & & -3 & & -1 & & -2 & & -2 & & -1 & & \\ & -1 & & 1 & & -1 & & 1 & & -1 & & 1 & \\ & & 0 & & 0 & & 0 & & 0 & & 0 & & \end{array}$$

Dans l'exemple 2.8, nous avons une frise à 6 rangées d'ordre 2. Toutefois, ces quatre rangées supplémentaires sont très importantes. En effet, elles servent à déterminer, au moins en partie, une frise lorsqu'on en connait une section (voir la définition ci-bas). De plus, les deux premières rangées permettent d'établir un lien avec les polynômes continuants non signés, comme ceci sera expliqué à la section 3.

Définition 2.9. Une *section* d'une frise est une portion de cette frise qui comporte un et un seul élément par rangée de telle sorte que si $f(i,j)$ fait partie de la section avec $-1 \leq j - i \leq n$, alors

- soit $f(i+1,j)$, soit $f(i,j-1)$ en fait partie et
- soit $f(i-1,j)$, soit $f(i,j+1)$ en fait partie.

En d'autres termes, si un élément d'une frise, $f(i,j)$, fait partie d'une section, alors un élément de la rangée inférieure et un élément de la rangée supérieure formant une maille commune avec $f(i,j)$ font également partie de la section.

Exemple 2.10. Voici une section de la frise donnée dans l'exemple 2.8 :

$$\begin{array}{ccccc} & & 0 & & \\ & 1 & & & \\ 3 & & & & \\ & -2 & & & \\ 1 & & & & \\ & 0 & & & \end{array}$$

Lemme 2.11. *Si une section d'éléments non nuls (mis à part les éléments sur les rangées -1 et $n+2$) d'une frise est fixée, alors il est possible de déterminer de manière unique les deux sections adjacentes et parallèles.*

Démonstration. Il suffit d'appliquer successivement la règle antimodulaire à chacune des mailles des éléments de la section connue. □

Exemple 2.12. Soit une frise d'ordre $n = 3$, où la dernière rangée est composée de -1. Supposons que l'on connaisse la section de la frise suivante :

- $f(i+2,i) = 0$;
- $f(i+1,i) = 1$;
- $f(i,i) = -5$;
- $f(i-1,i) = 1$;
- $f(i-1,i+1) = 1$;
- $f(i-1,i+2) = -1$;
- $f(i-2,i+2) = 0$.

Voici donc une portion d'une telle frise :

$$\begin{array}{ccccccccccc} & & 0 & & 0 & & 0 & & & & \\ & 1 & & 1 & & 1 & & 1 & & & \\ & & & & -5 & & & & & & \\ \cdots & & & 1 & & & & & \cdots & & \\ & & & & 1 & & & & & & \\ & -1 & & -1 & & -1 & & -1 & & & \\ & & 0 & & 0 & & 0 & & & & \end{array}$$

Déterminons les éléments des sections adjacentes. Nous cherchons dans la section de gauche $f(i-1,i-1)$, $f(i-2,i-1)$ et $f(i-2,i)$ et dans la section de droite $f(i+1,i+1)$, $f(i,i+1)$ et $f(i,i+2)$. Il est à noter que nous n'avons pas besoin de calculer les éléments des rangées -1, 0, 4 et 5, car ils sont trivialement connus.

En vertu de la règle antimodulaire, $f(i-1,i-1)\cdot -5-1\cdot 1=-1$, d'où on déduit que $f(i-1,i-1)=0$. De même, $f(i-2,i)\cdot 1-1\cdot =-1$ donc $f(i-2,i)=-2$. Finalement, $f(i-2,i-1)\cdot -1-f(i-1,i-1)\cdot f(i-2,i)=1$, ce qui revient à $f(i-2,i-1)\cdot -1-0\cdot -2=1$ et ainsi $f(i-2,i-1)=1$.

De la même manière, en utilisant toujours la règle antimodulaire, il est possible de trouver les éléments de la seconde section : $f(i+1,i+1)=1$, $f(i,i+1)=-4$ et $f(i,i+2)=3$.

Définition 2.13. Une *section oblique* d'une frise est une section d'une frise dont tous les éléments sont de la forme $f(i,\lambda)$ ou $f(\lambda,i)$, où λ est fixe et i varie.

Exemple 2.14. Voici des sections obliques de la frise donnée dans l'exemple 2.8 :

$$\begin{array}{ccccccccccccc} 0 & & & & & & & & & & & & 0 \\ & 1 & & & & & & & & & & 1 & \\ & & -1 & & & & & & & & 3 & & \\ & & & -2 & & & & & & -2 & & & \\ & & & & 1 & & & & -1 & & & & \\ & & & & & 0 & & 0 & & & & & \end{array} \quad \text{et} \quad .$$

Le lemme suivant stipule que, dans une frise, si les $k+2$ premiers éléments d'une section oblique de la forme (λ,i), où λ est fixe et i varie (ou de la forme (i,λ)) d'une frise sont connus, alors, à partir de $(\lambda,\lambda-2)$, $(\lambda,\lambda-1),\ldots,(\lambda,\lambda+k-1)$, il est possible de déterminer $(\lambda+1,\lambda-1)$, $(\lambda+1,\lambda),\ldots,(\lambda+1,\lambda+k-1)$. De la même manière, à partir de $(\lambda+2,\lambda)$, $(\lambda+1,\lambda),\ldots,(\lambda-k+1,\lambda)$, il est possible de déterminer $(\lambda+1,\lambda-1)$, $(\lambda,\lambda-1),\ldots,(\lambda-k+1,\lambda-1)$.

Lemme 2.15. *Soit λ fixe et i variant. Si les $k+2$ premiers éléments d'une section oblique de la forme (λ,i) (ou de la forme (i,λ)) d'une frise sont connus, les $k+1$ premiers éléments de la section oblique de la forme $(\lambda+1,i)$ (ou $(i,\lambda-1)$, respectivement) sont également connus.*

Démonstration. Montrons l'énoncé par récurrence. Supposons que les $k+2$ premiers termes de la section oblique de la forme (λ,i) soient connus. Par définition, $f(\lambda+1,\lambda-1)=0$ et $f(\lambda+1,\lambda)=1$. Supposons que $f(\lambda+1,\lambda+i)$ est connu pour un certain i tel que $-1\leq i<k-1$ et prouvons que $f(\lambda+1,\lambda+i+1)$ s'en déduit. En vertu de la règle unimodulaire, on sait que

$$f(\lambda,\lambda+i)f(\lambda+1,\lambda+i+1)-f(\lambda+1,\lambda+i)f(\lambda,\lambda+i+1)=(-1)^{i+1},$$

d'où

$$f(\lambda+1,\lambda+i+1)=\frac{f(\lambda+1,\lambda+i)f(\lambda,\lambda+i+1)+(-1)^{i+1}}{f(\lambda,\lambda+i)}.$$

Par récurrence, on en déduit la valeur de $f(\lambda+1, i+1)$ pour tout i tel que $-1 \leq i < k$. □

Pour établir un lien avec l'algorithme d'Euclide, qui utilise uniquement des nombres entiers, nous nous intéressons aux conditions d'obtention de frises d'entiers à partir d'une section oblique de cette frise.

Proposition 2.16. *Si les $k+2$ premiers termes $f(i,i-2)$, $f(i,i-1)$, ..., $f(i,i+k-1)$ d'une section oblique d'une frise sont entiers, non nuls et tels que*

$$f(i,i+m) | f(i,i+m+1) - f(i,i+m-1)$$

pour tout m tel que $-1 \leq m \leq k-2$, alors les $k+1$ premiers termes de la section adjacente $f(i+1,i-1)$, $f(i+1,i)$, ..., $f(i+1,i+k-1)$ sont aussi entiers.

De même, si les $k+2$ premiers termes $f(j+2,j)$, $f(j+1,j)$, ..., $f(j-k+1,j)$ d'une section oblique d'une frise sont entiers, non nuls et tels que $f(j-m,j) | f(j-m-1,j) - f(j-m+1,j)$ pour tout m tel que $-1 \leq m \leq k-2$, alors les $k+1$ premiers termes de la section adjacente $f(j+1,j-1)$, $f(j,j-1)$, ..., $f(j-k+1,j-1)$ sont aussi entiers.

Démonstration. Montrons la première partie de cette proposition. Afin d'alléger la lecture, notons $x_m = f(i,i+m-1)$ et $y_m = f(i+1,i+m)$. Par définition, y_{-1} et $y_0 \in \mathbb{Z}$. Supposons que y_{m-1} et $y_m \in \mathbb{Z}$ pour un certain m tel que $-1 \leq m < k-1$ et montrons que $y_{m+1} \in \mathbb{Z}$:

$$\begin{aligned}
y_{m+1} &= -y_m \frac{y_{m-1} - y_{m+1}}{y_m} + y_{m-1} \\
&= \frac{-y_m}{x_{m+1}} \left(\frac{x_{m+1}y_{m-1} - x_{m+1}y_{m+1} + (-1)^m + (-1)^{m+1}}{y_m} \right) + y_{m-1} \\
&= \frac{-y_m}{x_{m+1}} \left(\frac{x_{m+1}y_{m-1} + (-1)^m}{y_m} - \frac{x_{m+1}y_{m+1} + (-1)^{m+1}}{y_m} \right) + y_{m-1} \\
&= \frac{-y_m (x_m - x_{m+2})}{x_{m+1}} + y_{m-1}.
\end{aligned}$$

Puisque $x_{m+1} | x_m - x_{m+2}$ et que y_m et $y_{m-1} \in \mathbb{Z}$, $y_{m+1} \in \mathbb{Z}$. Par récurrence, on en déduit que $y_1, y_2, \cdots, y_{k-1}$ sont tous des entiers.

La deuxième partie de la proposition se démontre exactement de la même manière en posant plutôt $x_m = f(j-m+1,j)$ et $y_m = f(j-m,j-1)$. □

3 Polynômes continuants non signés

Nous abordons maintenant les polynômes continuants non signés. Comme ils sont à la fois reliés aux frises et à l'algorithme d'Euclide, leur étude permettra d'établir ultérieurement un lien entre ces deux sujets.

Définition 3.1. Le *k-ième polynôme continuant non signé* est défini par récurrence à partir des deux précédents par :

$$p_k(x_i, \ldots, x_{i+k-1}) = x_{i+k-1} p_{k-1}(x_i, \ldots, x_{i+k-2}) + p_{k-2}(x_i, \ldots, x_{i+k-3}),$$

où $\{x_i\}_{i\in\mathbb{Z}}$ est une famille dénombrable d'indéterminées telle que $x_i \in \mathbb{Q}$ avec les conditions initiales suivantes :

$$p_{-1} = 0 \text{ et } p_0 = 1.$$

Exemple 3.2. Par exemple, on évalue

$$\begin{aligned} p_3(2,-1,3) &= 3p_2(2,-1) + p_1(2) \\ &= 3(-1p_1(2) + p_0) + p_1(2) \\ &= -2p_1(2) + 3p_0 \\ &= -2(2p_0 + p_{-1}) + 3p_0 \\ &= -p_0 - 2p_{-1} \\ &= -1. \end{aligned}$$

Afin d'établir un lien avec les frises, nous devons connaitre quelques propriétés des polynômes continuants non signés, en particulier la suivante.

Proposition 3.3. *Soit $k \geq 0$. Alors, on obtient que*

$$p_k(x_i, \ldots x_{i+k-1})\, p_k(x_{i+1}, \ldots, x_{i+k}) - p_{k-1}(x_{i+1}, \ldots, x_{i+k-1})\, p_{k+1}(x_i, \ldots, x_{i+k}) = (-1)^k.$$

Démonstration. Montrons l'énoncé par récurrence. Commençons avec $k = 0$:

$$p_0 \cdot p_0 - p_{-1} \cdot p_1(x_i) = (-1)^0.$$

Supposons que l'énoncé est vrai pour un $k \geq 0$ et prouvons-le pour $k+1$:

$$\begin{aligned} & p_{k+1}(x_i, \ldots, x_{i+k})\, p_{k+1}(x_{i+1}, \ldots, x_{i+k+1}) \\ & \quad - p_k(x_{i+1}, \ldots, x_{i+k})\, p_{k+2}(x_i, \ldots, x_{i+k+1}) \\ &= p_{k+1}(x_i, \ldots, x_{i+k}) \\ & \qquad (x_{i+k+1} p_k(x_{i+1}, \ldots, x_{i+k}) + p_{k-1}(x_{i+1}, \ldots, x_{i+k-1})) \\ & \quad - p_k(x_{i+1}, \ldots, x_{i+k})\, p_{k+2}(x_i, \ldots, xi+k+1) \\ & \qquad (x_{i+k+1} p_{k+1}(x_i, \ldots, x_{i+k}) + p_k(x_i, \ldots, x_{i+k-1})) \\ &= -p_k(x_i, \ldots, x_{i+k-1})\, p_k(x_{i+1}, \ldots, x_{i+k}) \\ & \quad + p_{k-1}(x_{i+1}, \ldots, x_{i+k-1})\, p_{k+1}(x_i, \ldots, x_{i+k}) \\ &= -(-1)^k \text{ par hypothèse} \\ &= (-1)^{k+1}. \end{aligned}$$

Par récurrence, on en déduit que l'énoncé est vrai pour tout $k \geq 0$. □

Remarquons qu'en posant $p_k(x_i,\dots,x_{i+k-1}) = f(i,i+k-1)$ pour tout $k \geq -1$, la proposition 3.3 devient exactement la règle antimodulaire qui régit les frises. Ainsi, il est possible d'exprimer l'évaluation en des variables x_i de tout polynôme continuant non signés comme un élément d'une frise dont $\{x_i\}$ forme la rangée 1. Réciproquement, un élément $f(i,j)$ sur la $j-i+1$-ième rangée d'une frise s'écrit $p_{j-i+1}(x_i,\dots,x_j)$, où $x_m = f(m,m)$.

Toute frise d'ordre n peut donc s'écrire ainsi :

$$\begin{array}{ccccccccccc}
 & p_{-1} & & & p_{-1} & & & p_{-1} & & & p_{-1} & & \\
 & & p_0 & & & p_0 & & & p_0 & & & & \\
 & x_i & & & x_{i+1} & & & x_{i+2} & & & x_{i+3} & & \\
\dots & & p_2(x_ix_{i+1}) & & & p_2(x_{i+1}x_{i+2}) & & & p_2(x_{i+2}x_{i+3}) & & & \dots, \\
 & \ddots & & & \ddots & & & \ddots & & & \ddots & & \\
 & & p_{n+2}(x_{i-1},\dots,x_{i+n}) & & & p_{n+2}(x_i,\dots,x_{i+n+1}) & & & p_{n+2}(x_{i+1},\dots,x_{i+n+2}) & & & &
\end{array}$$

où $p_{n+2}(x_i,\dots,x_{n+1}) = 0$ pour tout i et $p_{n+1}(x_i,\dots,x_{i+n}) = 1$ ou -1 pour tout i, selon la frise.

Remarque 3.4. La règle antimodulaire se déduit de la définition des polynômes continuants non signés, mais l'inverse n'est pas vrai. Ainsi, dans certains cas, la règle antimodulaire ne permet pas de déterminer de manière unique les éléments d'une frise, alors que les polynômes continuants non signés le permettent.

Lemme 3.5. *Il est possible d'évaluer un polynôme continuant non signé à partir des premières indéterminées plutôt que des dernières :*

$$p_k(x_i,\dots,x_{i+k-1}) = x_i p_{k-1}(x_{i+1},\dots,x_{i+k-1}) + p_{k-2}(x_{i+2},\dots,x_{i+k-1}).$$

Démonstration. Cet énoncé se montre par récurrence. Pour $k=1$ et $k=2$:

$$\begin{aligned}
p_1(x_i) &= x_i p_0 + p_{-1} \\
p_2(x_i,x_{i+1}) &= x_{i+1}p_1(x_i) + p_0 = x_i x_{i+1} + 1 = x_i p(x_{i+1}) + p_0
\end{aligned}$$

Supposons que l'énoncé est vrai pour un certain $k \geq 1$ et prouvons-le pour $k+1$.

$$\begin{aligned}
p_{k+1}(x_i,\dots,x_{i+k}) &= x_{i+k}p_k(x_i,\dots,x_{i+k-1}) + p_{k-1}(x_i,\dots,x_{i+k-2}) \\
&= x_{i+k}\left(x_i p_{k-1}(x_{i+1},\dots,x_{i+k-1}) + p_{k-2}(x_{i+2},\dots,x_{i+k-1})\right) \\
&+ \quad \left(x_i p_{k-2}(x_{i+1},\dots,x_{i+k-2}) + p_{k-3}(x_{i+2},\dots,x_{i+k-2})\right) \\
&= x_i\left(x_{i+k}p_{k-1}(x_{i+1},\dots,x_{i+k-1}) + p_{k-2}(x_{i+1},\dots,x_{i+k-2})\right) \\
&+ \quad \left(x_{i+k}p_{k-2}(x_{i+2},\dots,x_{i+k-1}) + p_{k-3}(x_{i+2},\dots,x_{i+k-2})\right) \\
&= x_i p_k(x_{i+1},\dots,x_{i+k}) + p_{k-1}(x_{i+2},\dots,x_{i+k})
\end{aligned}$$

Par récurrence, on en déduit que l'énoncé est vrai pour tout $k \geq 1$. □

4 Algorithme d'Euclide

L'algorithme d'Euclide permet de calculer le plus grand commun diviseur de deux nombres entiers a et b. L'algorithme permet également de déterminer s et $t \in \mathbb{Z}$ tels que $as + tb = (a,b)$.

Il existe un lien entre l'algorithme d'Euclide (décrit à l'Algorithme 1) et les frises que nous explorerons plus tard.

Exemple 4.1. Trouvons le pgcd de 118 et 66 et trouvons s et $t \in \mathbb{Z}$ tels que $118s + 66t = (118,66)$:

$$\begin{aligned} 118 &= 1 \cdot 66 + 52 \\ 66 &= 1 \cdot 52 + 14 \\ 52 &= 3 \cdot 14 + 10 \\ 14 &= 1 \cdot 10 + 4 \\ 10 &= 2 \cdot 4 + 2 \\ 4 &= 2 \cdot 2 + 0. \end{aligned}$$

Ainsi, on trouve $(118,66) = 2$. Trouvons maintenant s et t :

$$\begin{aligned} 2 &= 10 - 2 \cdot 4 \\ &= 10 - 2(14 - 1 \cdot 10) \\ &= 3 \cdot 10 - 2 \cdot 14 \\ &= 3(52 - 3 \cdot 14) - 2 \cdot 14 \\ &= 3 \cdot 52 - 11 \cdot 14 \\ &= 3 \cdot 52 - 11(66 - 1 \cdot 52) \\ &= 14 \cdot 52 - 11 \cdot 66 \\ &= 14(118 - 1 \cdot 66) - 11 \cdot 66 \\ &= 14 \cdot 118 - 25 \cdot 66, \end{aligned}$$

d'où $s = 14$ et $t = -25$.

Remarquons ici que :

$$p_5(1,1,3,1,2) = 25 \text{ et } p_4(1,3,1,2) = 14.$$

Or, 1, 1, 3, 1 et 2 sont les quotients à chaque étape de l'algorithme.

Le lemme suivant, exposé de manière informelle dans [Hag05], stipule que les coefficients de l'algorithme d'Euclide correspondent à des polynômes continuant non signés.

Pour simplifier la lecture, nous noterons $a = r_{-1}$ et $b = r_0$.

Le lemme suivant explique que le entiers s et t tels que $sa + tb = 1$ s'expriment comme l'évaluation de polynômes continuants en les quotients obtenus par l'algorithme d'Euclide.

Lemme 4.2. *Soient a, $b \in \mathbb{N}_*$, $r_1, \ldots, r_k$ les k restes obtenus par l'algorithme d'Euclide appliqué au calcul de quotient (r_k étant le dernier reste non nul) et $q_1, \ldots, q_k$ les k quotients obtenus par cet algorithme. Alors, on a que*

$$(-1)^i p_i(q_{k-i+1}, \ldots, q_k) r_{k-i} + (-1)^{i-1} p_{i-1}(q_{k-i+2}, \ldots, q_k) r_{k-i-1} = (a,b)$$

pour tout $i \leq k - 1$.

Données : $a = r_{-1}$ et $b = r_0 \in \mathbb{N}_*$
Résultat : pgcd de a et b et $s, t \in \mathbb{Z}$ tel que $sa + tb = (a,b)$
Posons $i = 0$.
Tant que $r_i \neq 0$ **faire**
  $r_{i-1} = q_{i+1} r_i + r_{i+1}$ (En vertu du théorème de divisibilité, il existe q_{i+1}, $r_{i+1} \in \mathbb{N}_*$ tels que $r_{i-1} = r_i qi_{+1} + r_{i+1}$, où $0 \leq r_{i+1} < r_i$).
  Posons $i = i + 1$.
Si $r_{i+1} = 0$ **alors**
  $(a,b) = r_i$.
Comme $r_1 > r_2 > r_3 > \cdots$ et que $r_i \in \mathbb{N}$ pour tout i, il existe un plus petit k tel que $r_{k+1} = 0$. Posons k tel que $r_k = (a,b)$. On sait que $(a,b) = r_{k-1} - q_{k+1} r_k$.
Pour *i tel que* $1 \leq i \leq k$
  réécrire r_i avec $r_{i-2} - q_i r_{i-1}$.
Ainsi, ultimement, il est possible d'exprimer (a,b) en fonction de a et de b.

Algorithme 1 : Algorithme d'Euclide

Démonstration. Cet énoncé se prouve par récurrence. Commençons par le montrer pour $i = 0$:

$$(-1)^0 p_0 r_k + (-1)^{-1} p_{-}1 r_{k-1} = r_k = (a,b) \text{ en vertu de la définition 1.}$$

Supposons que l'énoncé est vrai pour un certain $i \geq 1$ et prouvons-le pour $i+1$:

$$\begin{aligned}
&(-1)^{i+1} p_{i+1}(q_{k-i}, \ldots, q_k) r_{k-i-1} + (-1)^i p_i(q_{k-i+1}, \ldots, q_k) r_{k-i-2} \\
&\quad = (-1)^{i-1} \left(q_{k-i}(p_i(q_{k-i+1}, \ldots, q_k)) + p_{i-1}(q_{k-i+2}, \ldots, q_k)\right) r_{k-i-1} \\
&\qquad + (-1)^i p_i(q_{k-i+1}, \ldots, q_k) \left(q_{k-i} r_{k-i-1} + r_{k-i}\right) \\
&\quad = (-1)^i p_i(q_{k-i+1}, \ldots, q_k) r_{k-i} + (-1)^{i-1} p_{i-1}(q_{k-i+2}, \ldots, q_k) r_{k-i-1} \\
&\qquad + \left((-1)^{i-1} + (-1)^i\right) \left(q_{k-i} p_i(q_{k-i+1}, \ldots, q_k) r_{k-i-1}\right) \\
&\quad = (a,b).
\end{aligned}$$

□

La prochaine proposition permet de déterminer une paire de valeurs possible pour s et $t \in \mathbb{Z}$ tels que $sa + tb = (a,b)$. En fait, une infinité de paires nombres entiers (s,t) vérifient $sa + tb = (a,b)$; la proposition suivante ne permet d'en déterminer qu'une seule. Une fois que l'on connait (s,t) qui respectent ces conditions, il est possible d'en déterminer une infinité d'autres puisque, si $sa + tb = (a,b)$, alors $(s + mb)a + (t - ma)b = (a,b), m \in \mathbb{Z}$.

Proposition 4.3. *Soient a, $b \in \mathbb{N}_*$, $r_1, \ldots, r_k$ les k restes de l'algorithme d'Euclide appliqué au calcul du pgcd de a et de b (r_k étant le dernier reste non nul) et $q_1, \ldots, q_k$ les k quotients obtenus par cet algorithme. Alors, on trouve que*

$$(-1)^{k-1} p_{k-1}(q_2, \ldots, q_k) \cdot a + (-1)^k p_k(q_1, \ldots, q_k) \cdot b = (a,b).$$

Démonstration. Cela découle du lemme 4.2 en posant $i = k$. □

La proposition 4.3 relie l'algorithme d'Euclide et les polynômes continuants non signés, et, ainsi, l'algorithme d'Euclide et les frises. En effet, selon cette proposition, en disposant $q_1, \ldots, q_k$ sur la première rangée d'une frise, nous obtenons la frise suivante :

$$\begin{array}{ccccccccccc} q_1 & & q_2 & & \cdots & & q_k \\ & \ddots & & \ddots & & \iddots & & & \\ \cdots & & & & & & & \cdots & \\ & & & \ddots & & s & & & \\ & & & & t & & & & \end{array}$$

Exemple 4.4. Reprenons l'exemple 4.1 en utilisant la proposition 4.3 pour déterminer les valeurs de s et de t.

Nous connaissons les valeurs de $q_1 = 1, q_2 = 1, q_3 = 1, q_4 = 1, q_5 = 2$. Plaçons donc ces valeurs sur la première rangée de la frise et déterminons les éléments de la frise sur les rangées subséquentes :

$$\begin{array}{ccccccccccc} 0 & & 0 & & 0 & & 0 & & 0 \\ & 1 & & 1 & & 1 & & 1 & \\ 1 & & 1 & & 3 & & 1 & & 2 \\ & 2 & & 4 & & 4 & & 3 & \\ & & 7 & & 5 & & 11 & & \\ & & & 9 & & 14 & & & \\ & & & & 25 & & & & \end{array}$$

On en déduit que $s = 14$ et $t = -25$ (la variable négative entre s et t est celle qui se trouve sur une rangée impaire).

Calculer des valeurs de s et de t à l'aide des polynômes continuants non signés ou des frises s'effectue en autant, sinon plus, d'étapes qu'en utilisant l'algorithme traditionnel d'Euclide. Il n'y a donc pas d'avantages apparents à utiliser ces méthodes. Cependant, si $(a,b) = 1$, s et t se déterminent plus rapidement à l'aide des frises, comme le montrent le théorème 4.6 et l'exemple 4.7. Il faut toutefois d'abord énoncer le lemme suivant qui servira à démontrer le théorème 4.6.

Proposition 4.5. *Soient $a, b \in \mathbb{N}_*$, $r_1, \ldots, r_k$ les k restes de l'algorithme d'Euclide appliqué au calcul du pgcd de a et de b (r_k étant le dernier reste non nul) et $q_1, \ldots, q_k$ les k quotients obtenus par cet algorithme. Alors, on trouve que*

$$r_i \mid (r_{i-1} - r_{i+1})$$

pour tout i tel que $0 \leq i \leq k$.

Démonstration. En vertu de la définition 1, on sait que

$$r_{i-1} = q_{i-1} r_i + r_{i+1}.$$

On en déduit que

$$r_{i-1} - r_{i+1} = q_{i-1}r_i + r_{i+1} - r_{i+1} = q_{i-1}r_i. \qquad \square$$

Théorème 4.6. *Soient a, $b \in \mathbb{N}_*$ tels que $(a,b) = 1$ et $k+1$ le nombre d'étapes de l'algorithme d'Euclide appliqué au calcul de (a,b), c'est-à-dire que $(a,b) = r_k$ et le reste $k+1$ est nul. Soient $r_1, \ldots, r_k$ et $q_1, \ldots, q_k$ respectivement les k restes et les k quotients obtenus par l'algorithme d'Euclide. Si nous posons $r_j = p_{k-j}(x_i, \ldots, x_{i+k-j-1})$ pour un certain i et pour tout j tel que $-1 \leq j \leq k+1$, alors on obtient que*

$$(-1)^{k-1}p_{k-1}(x_{i+1}, \ldots, x_{i+k-1}) \cdot a + (-1)^k p_k(x_{i+1}, \ldots, x_{i+k}) \cdot b = (a,b).$$

Démonstration. En vertu de la règle antimodulaire, on sait que :

$$p_k(x_i, \ldots, x_{i+k-1})p_k(x_{i+1}, \ldots, x_{i+k}) - p_{k-1}(x_{i+1}, \ldots, x_{i+k-1})p_{k+1}(x_i, \ldots, x_{i+k}) = (-1)^k.$$

Comme $r_0 = p_k(x_i, \ldots, x_{i+k-1})$ et $r_{-1} = p_{k+1}(x_i, \ldots, x_{i+k})$, on déduit que

$$r_0 p_k(x_{i+1}, \ldots, x_{i+k}) - p_{k-1}(x_{i+1}, \ldots, x_{i+k-1})r_{-1} = (-1)^k.$$

Ainsi,

$$(-1)^{k-1}p_{k-1}(x_{i+1}, \ldots, x_{i+k-1}) \cdot a + (-1)^k p_k(x_{i+1}, \ldots, x_{i+k}) \cdot b = 1.$$

Or, en vertu du lemme 4.5, on sait que

$$p_{k-j}(x_i, \ldots, x_{i+k-j-1}) | p_{k-j+1}(x_i, \ldots, x_{i+k-j}) - p_{k-j-1}(x_i, \ldots, x_{i+k-j-2})$$

pour tout j tel que $-1 < j < k$. Donc la propositon 2.16 appliquée au polynôme continuant nous assure que $p_{k-1}(x_{i+1}, \ldots, x_{i+k-1})$, $p_k(x_{i+1}, \ldots, x_{i+k}) \in \mathbb{Z}$. Finalement, en vertu du lemme 2.15, $p_{k-j}(x_{i+1}, \ldots, x_{i+k-j})$ est déterminé pour tout j tel que $0 \leq j \leq k+1$ à partir de la section oblique r_{k+1}, r_k, …, r_{-1}. $\square$

Notons que poser $r_j = p_{k-j}(x_i, \ldots, x_{i+k-j-1})$ pour un certain i et pour tout j tel que $-1 \leq j \leq k+1$ est équivalent à considérer la portion de section suivante dans une frise :

$$\begin{array}{ccccccccccc}
 & & r_{k+1} & & 0 & & 0 & & 0 & & \\
1 & & & r_k & & 1 & & 1 & & & \\
 & & & & r_{k-1} & & & & & & \\
 & & & & & \ddots & & & & & \\
 & & & & & & r_1 & & & & \\
 & & & & & & & b & & & \\
 & & & & & & & & a & &
\end{array}$$

En vertu du lemme 3.5, il aurait été également possible d'obtenir une diagonale dans l'autre sens en posant plutôt $r_j = p_{k-j}(x_{i-k+j+1}, \ldots, x_i)$ pour un certain

i et pour tout j tel que $-1 \leq j \leq k+1$. Le théorème 4.6 aurait été modifié en conséquence.

Grâce au théorème 4.6, il est possible de trouver des entiers s et t tels que $sa + tb = 1$ si a et b sont copremiers. Il suffit d'écrire a et b sur une section oblique d'une frise, puis d'écrire les restes successifs d'un élément de la section divisé par le précédent jusqu'à $r_k = 1$ et en posant $p_0 = r_k$. Ainsi, r_k fait partie de la rangée 0 de la frise, c'est-à-dire la rangée composée de 1. En vertu du lemme 2.15, il est possible de trouver $k-1$ éléments de la diagonale adjacente, en plus du 0 et du 1 sur les deux premières rangées qui sont déjà connus.

Exemple 4.7. Calculons le pgcd de 67 et 55 et, s'il vaut 1, déterminons des entiers s et t tels que $67s + 55t = 1$.

Divisons 67 par 55, 55 par le reste de cette division et ainsi de suite en inscrivant 67, 55 et les différents restes les uns après les autres sur la diagonale d'une frise :

0
1
2
3
5
7
12
55
67

Remarquons ici que (67,55) = 1.

Complétons cette frise en écrivant la ligne de 0 à la hauteur du 0 déjà inscrit et la ligne de 1 à la hauteur du 1 déjà inscrit. Servons-nous-en pour déterminer la diagonale adjacente à celle ci-dessus. On obtient :

0 0 0 0 0
1 1 1 1
2 2
5 3
7 5
12 23
55 28
67

Ainsi, en observant que $23 \cdot 67 - 28 \cdot 55 = 1$, on déduit que $s = 23$ et $t = -28$. Notons que s est positif et t est négatif, car s est sur une rangée d'ordre pair tandis que t est sur une rangée d'ordre impair.

Les frises peuvent donc être utilisées pour trouver deux entiers s et t tels que $sa + tb = 1$ quand a et b sont deux naturels copremiers. La définition suivante servira par la suite à expliquer l'avantage de déterminer s et t à l'aide des frises plutôt que de l'algorithme d'Euclide traditionnel.

Définition 4.8. Définissons une étape d'algorithme comme :

a) le fait de trouver le reste d'une division d'entiers ou

b) une addition, une soustraction ou une multiplication d'entiers ou

c) la substitution d'un entier par une expression équivalente.

Remarque 4.9. Soient a, $b \in \mathbb{N}_*$ copremiers et $k+1$ le nombre d'étapes de l'algorithme d'Euclide appliqué au calcul de (a,b), c'est-à-dire que $(a,b) = r_k$ et le reste $k+1$ est nul. Alors, déterminer des valeurs de s et de t au moyen de l'algorithme d'Euclide traditionnel ou des frises avec le théorème 4.6 nécessite $4k+1$ étapes. Toutefois, l'algorithme d'Euclide traditionnel, contrairement à la méthode par les frises, nécessite de garder en mémoire les quotients obtenus par l'algorithme.

Démonstration. La première partie de chacune de ces deux méthodes, celle qui consiste à calculer le pgcd et ainsi déterminer les différents quotients et les différents restes s'effectue en $k+1$ étapes, car il y a $k+1$ restes de divisions à déterminer.

Par la suite, déterminer s et t en remplaçant successivement chacun des restes par les deux précédents requiert $3k$ étapes. En effet, pour tout i tel que $1 \leq i \leq k$, il faut premièrement remplacer r_i par $r_{i-2} - q_i r_{i-1}$ (une étape de substitution). Par la suite, il faut multiplier le facteur de r_i par q_i (une multiplication) et additioner le résultat au facteur de r_{i-1} dans l'expression initiale (une addition). Cela totalise $3k$ étapes.

Avec les frises, pour calculer les k éléments de la diagonale adjacente à celle des restes, il faut chaque fois trois étapes. En effet, déterminer un élément à l'aide de la fonction de frise requiert une multiplication, une addition de ± 1 et une division. On obtient donc $3k$ étapes encore une fois, mais les k quotients obtenus par l'algorithme d'Euclide n'ont pas besoin d'être gardés en mémoire. □

Références

[BMRDSM12] Véronique Bazier-Matte, David Racicot-Desloges et Tanna Sánchez McMillan : Friezes and continuant polynomials with parameters. 2012.

[CC73] J. H. Conway et H. S. M. Coxeter : Triangulated polygons and frieze patterns. *The Mathematical Gazette*, 57(400):pp. 87–94, 1973.

[Hag05] R. Haggarty : *Mathématiques discrètes appliquées à l'informatique*. Synthex : informatique. Pearson Education France, 2005.

Véronique Bazier-Matte
Département de mathématiques, Université de Sherbrooke
Courriel: Veronique.Bazier-Matte@USherbrooke.ca