Mots circulaires: Structure algébrique et système de numération

Isabelle Dubois

Laboratoire IECL - Metz - Université de Lorraine

Séminaire Combinatoire et Théorie des Nombres - Institut Camille Jordan - Mai 2018

Travail en cours, en collaboration avec Benoît Rittaud

Point de départ:

Considérons l'addition de deux rationnels en ne se préoccupant que de la partie périodique:

Soit $A = 178/55 = 3,2\overline{36}$... et $B = 421/330 = 1,2\overline{75}\ldots$.
Alors $A + B = 4,5\overline{12}\ldots$.
Si nous n'additionnons que les périodes, nous obtenons:

$$\overline{3\ 6} + \overline{7\ \ 5} = \overline{10\ 11}$$

Point de départ:

Considérons l'addition de deux rationnels en ne se préoccupant que de la partie périodique:

Soit $A = 178/55 = 3,2\overline{36}$... et $B = 421/330 = 1,2\overline{75}\dots$.
Alors $A + B = 4,5\overline{12}\dots$.
Si nous n'additionnons que les périodes, nous obtenons:

$$\overline{3\ 6} + \overline{7\ \ 5} = \overline{10\ 11} \quad \approx \quad \overline{(10+1)\ (11-10)} = \overline{(11)\ 1}$$

Point de départ:

Considérons l'addition de deux rationnels en ne se préoccupant que de la partie périodique:

Soit $A = 178/55 = 3,2\overline{36}$... et $B = 421/330 = 1,2\overline{75}\ldots$.
Alors $A + B = 4,5\overline{12}\ldots$.
Si nous n'additionnons que les périodes, nous obtenons:

$$\begin{aligned}\overline{3\ 6} + \overline{7\ \ 5} = \overline{10\ 11} \quad &\approx \quad \overline{(10+1)\ (11-10)} = \overline{(11)\ 1} \\ &\approx \quad \overline{(11-10)\ (1+1)} = \overline{1\ 2}\end{aligned}$$

Point de départ:

Considérons l'addition de deux rationnels en ne se préoccupant que de la partie périodique:

Soit $A = 178/55 = 3,2\overline{36}$... et $B = 421/330 = 1,2\overline{75}\ldots$.
Alors $A + B = 4,5\overline{12}\ldots$.
Si nous n'additionnons que les périodes, nous obtenons:

$$\begin{aligned} \overline{3\ 6} + \overline{7\ \ 5} = \overline{10\ 11} \quad &\approx \quad \overline{(10+1)\ (11-10)} = \overline{(11)\ 1} \\ &\approx \quad \overline{(11-10)\ (1+1)} = \overline{1\ 2} \end{aligned}$$

Nous pouvons interpréter cette opération en tant qu'addition de deux mots circulaires de longueur 2, dans le contexte de la numération en base 10:

$$(3\ 6) + (7\ 5) \approx_{\text{base }10} (1\ 2).$$

Point de départ:

Considérons l'addition de deux rationnels en ne se préoccupant que de la partie périodique:

Soit $A = 178/55 = 3,2\overline{36}...$ et $B = 421/330 = 1,2\overline{75}\ldots$.
Alors $A + B = 4,5\overline{12}\ldots$.
Si nous n'additionnons que les périodes, nous obtenons:

$$\begin{array}{rcl} \overline{3\ 6} + \overline{7\ \ 5} = \overline{10\ 11} & \approx & \overline{(10+1)\ (11-10)} = \overline{(11)\ 1} \\ & \approx & \overline{(11-10)\ (1+1)} = \overline{1\ 2} \end{array}$$

Nous pouvons interpréter cette opération en tant qu'addition de deux mots circulaires de longueur 2, dans le contexte de la numération en base 10:

$$(3\ 6) + (7\ 5) \approx_{\text{base } 10} (1\ 2).$$

La notion de mot circulaire a été introduit initialement par B. Rittaud et L. Vivier (2011-2012) dans le contexte de la numération de Fibonacci. Après la venue de Benoît au séminaire de Nancy, nous avons entamé une collaboration sur ce sujet.

Sommaire

Soit $\ell \in \mathbb{N}^*$ fixé.

Définition (Mot circulaire de longueur ℓ)

Un mot circulaire de longueur ℓ est un mot fini $(w_0 \dots w_i \dots w_{\ell-1})$ constitué de ℓ lettres sur l'alphabet $\mathbb{Z}$ et dont les indices sont dans $\mathbb{Z}/\ell\mathbb{Z}$.

L'ensemble des mots circulaires de longueur ℓ est un groupe abélien:

$$W + W' = ((w_0 + w'_0) \dots (w_i + w'_i) \dots (w_{\ell-1} + w'_{\ell-1}))$$

Soit $\ell \in \mathbb{N}^*$ fixé.

Définition (Mot circulaire de longueur ℓ)

Un mot circulaire de longueur ℓ est un mot fini $(w_0 \dots w_i \dots w_{\ell-1})$ constitué de ℓ lettres sur l'alphabet $\mathbb{Z}$ et dont les indices sont dans $\mathbb{Z}/\ell\mathbb{Z}$.

L'ensemble des mots circulaires de longueur ℓ est un groupe abélien:

$$W + W' = ((w_0 + w'_0) \dots (w_i + w'_i) \dots (w_{\ell-1} + w'_{\ell-1}))$$

Soit P un polynôme entier $P(X) = \sum_{0 \leq i \leq d} a_i X^i \in \mathbb{Z}[X]$ ($d \in \mathbb{N}^*$).

Définition (Relation de retenue définie par P)

La relation d'équivalence de retenue $\approx_P$ définie par P sur les mots circulaires $W = (w_0 \dots w_{\ell-1})$ est basée sur les relations: pour tout i modulo ℓ,

$$W \approx_P (w_0 \dots (w_{i-d} + a_0) \dots (w_{i-1} + a_{d-1})(w_i + a_d) w_{i+1} \dots w_{\ell-1}).$$

Soit $\ell \in \mathbb{N}^*$ fixé.

Définition (Mot circulaire de longueur ℓ)

Un mot circulaire de longueur ℓ est un mot fini $(w_0 \dots w_i \dots w_{\ell-1})$ constitué de ℓ lettres sur l'alphabet $\mathbb{Z}$ et dont les indices sont dans $\mathbb{Z}/\ell\mathbb{Z}$.

L'ensemble des mots circulaires de longueur ℓ est un groupe abélien:

$$W + W' = ((w_0 + w'_0) \dots (w_i + w'_i) \dots (w_{\ell-1} + w'_{\ell-1}))$$

Soit P un polynôme entier $P(X) = \sum_{0 \leq i \leq d} a_i X^i \in \mathbb{Z}[X]$ ($d \in \mathbb{N}^*$).

Définition (Relation de retenue définie par P)

La relation d'équivalence de retenue $\approx_P$ définie par P sur les mots circulaires $W = (w_0 \dots w_{\ell-1})$ est basée sur les relations: pour tout i modulo ℓ,

$$W \approx_P (w_0 \dots (w_{i-d} + a_0) \dots (w_{i-1} + a_{d-1})(w_i + a_d) w_{i+1} \dots w_{\ell-1}).$$

Exemple. "Fibonacci" $P(X) = X^2 - X - 1$, $\ell = 4$.

$$(1\,2\,3\,4) \approx_P (0\,1\,4\,4) \approx_P (4\,1\,0\,0) \approx_P (3\,0\,1\,0) \approx_P (2\,1\,1\,(-1))$$
$$\approx_P (2\,0\,0\,0) \approx_P (1\,0\,1\,1) \approx_P (0\,1\,1\,0) \approx_P (0\,0\,0\,1)$$

On se donne $\ell \in \mathbb{N}^*$ et $P(X) = \sum_{0\leq i\leq d} a_i X^i \in \mathbb{Z}[X]$.

Soit σ l'action de décalage définie par
$$\sigma((w_0 \dots w_{\ell-1})) = (w_1 \dots w_{\ell-1} w_0).$$
Soit $A_\ell := (a_0 \dots a_i \dots a_d 0 \dots 0)$ si $\ell > d$, resp. $:= ((\sum_{j\equiv i \bmod \ell} a_j)_i)$ si $\ell \leq d$, le mot circulaire associé à P.

Définition (Groupe de mots circulaires modulo la retenue P)

La relation de retenue $\approx_P$ définie par P sur les mots circulaires de longueur ℓ est : $W \approx_P W'$ ssi il existe $(v_0, \dots, v_{\ell-1}) \in \mathbb{Z}^\ell$ tel que
$$W = W' + \sum_{0\leq i\leq \ell-1} v_i \sigma^{-i}(A_\ell).$$

On définit alors $\mathcal{G}_{\ell,P}$ le groupe quotient (abélien) des mots circulaires de longueur ℓ par cette relation d'équivalence.

On se donne $\ell \in \mathbb{N}^*$ et $P(X) = \sum_{0 \le i \le d} a_i X^i \in \mathbb{Z}[X]$.

Soit σ l'action de décalage définie par

$$\sigma((w_0 \dots w_{\ell-1})) = (w_1 \dots w_{\ell-1} w_0).$$

Soit $A_\ell := (a_0 \dots a_i \dots a_d 0 \dots 0)$ si $\ell > d$, resp. $:= ((\sum_{j \equiv i \bmod \ell} a_j)_i)$ si $\ell \le d$, le mot circulaire associé à P.

Définition (Groupe de mots circulaires modulo la retenue P)

La relation de retenue $\approx_P$ définie par P sur les mots circulaires de longueur ℓ est : $W \approx_P W'$ ssi il existe $(v_0, \dots, v_{\ell-1}) \in \mathbb{Z}^\ell$ tel que

$$W = W' + \sum_{0 \le i \le \ell-1} v_i \sigma^{-i}(A_\ell).$$

On définit alors $\mathcal{G}_{\ell,P}$ le groupe quotient (abélien) des mots circulaires de longueur ℓ par cette relation d'équivalence.

Exemples.

- "Base 2" : $P(X) = X - 2$, $\ell = 2$, $\mathcal{G}_{2,P} = \{(0\,0), (1\,0), (0\,1)\}$
- "Fibonacci" : $P(X) = X^2 - X - 1$, $\ell = 4$, $\mathcal{G}_{4,P} = \{(0\,0\,0\,0), (1\,0\,0\,0), (0\,1\,0\,0), (0\,0\,1\,0), (0\,0\,0\,1)\}$.

Le groupe des mots circulaires de longueur ℓ et de retenue P peut être étudié via les isomorphismes entre $\mathcal{G}_{\ell,P}$ et:

1. L'ensemble des points équivalents du réseau $\mathbb{Z}^\ell$ sous l'action de la matrice circulante de taille $\ell \times \ell$ dont la première ligne est A_ℓ (ou associée à P).
2. Le groupe abélien (pour $+$) de l'anneau quotient $\mathbb{Z}[X]/(P(X), X^\ell - 1)$. La multiplication par X correspond alors à l'action de σ^{-1}.

Le groupe des mots circulaires de longueur ℓ et de retenue P peut être étudié via les isomorphismes entre $\mathcal{G}_{\ell,P}$ et:

1. L'ensemble des points équivalents du réseau $\mathbb{Z}^\ell$ sous l'action de la matrice circulante de taille $\ell \times \ell$ dont la première ligne est A_ℓ (ou associée à P).
2. Le groupe abélien (pour $+$) de l'anneau quotient $\mathbb{Z}[X]/(P(X), X^\ell - 1)$. La multiplication par X correspond alors à l'action de σ^{-1}.

Proposition (Groupe fini)

$\mathcal{G}_{\ell,P}$ est un groupe abélien fini si et seulement si P ne possède pas de racines ℓ-ème de l'unité.

A partir de maintenant:

Hypothèse: P ne possède pas de racines de l'unité.

Le groupe des mots circulaires de longueur ℓ et de retenue P peut être étudié via les isomorphismes entre $\mathcal{G}_{\ell,P}$ et:

1. L'ensemble des points équivalents du réseau $\mathbb{Z}^\ell$ sous l'action de la matrice circulante de taille $\ell \times \ell$ dont la première ligne est A_ℓ (ou associée à P).
2. Le groupe abélien (pour $+$) de l'anneau quotient $\mathbb{Z}[X]/(P(X), X^\ell - 1)$. La multiplication par X correspond alors à l'action de σ^{-1}.

Proposition (Groupe fini)

$\mathcal{G}_{\ell,P}$ est un groupe abélien fini si et seulement si P ne possède pas de racines ℓ-ème de l'unité.

A partir de maintenant:

Hypothèse: P ne possède pas de racines de l'unité.

Liens avec d'autres domaines:

- systèmes dynamiques: points périodiques d'endomorphismes toraux
- résultants cycliques, produisant de grands nombres premiers
- ...

Soit $g_{\ell,P}$ le cardinal du groupe $\mathcal{G}_{\ell,P}$. On a:

Proposition (Propriétés concernant le cardinal)

(i) $g_{\ell,P} = |\mathrm{Resultant}(P(X), X^\ell - 1)| = |\prod_{0\leq k<\ell} P(e^{2i\pi k/\ell})|$.

(ii) $(g_{\ell,P})_\ell$ *est une suite de divisibilité.*

(iii) Croissance exponentielle : $\lim_{\ell\to+\infty} \ln g_{\ell,P}/\ell = \ln M(P)$, *où $M(P)$ est la mesure de Mahler de P.*

(iv) Apparition de facteurs premiers primitifs : *Si P est irréductible, il existe une infinité de facteurs premiers primitifs dans la suite $(g_{\ell,P})_\ell$ (et des résultats plus précis).*

Soit $g_{\ell,P}$ le cardinal du groupe $\mathcal{G}_{\ell,P}$. On a:

Proposition (Propriétés concernant le cardinal)

(i) $g_{\ell,P} = |\mathrm{Resultant}(P(X), X^\ell - 1)| = |\prod_{0\leq k<\ell} P(e^{2i\pi k/\ell})|$.

(ii) $(g_{\ell,P})_\ell$ *est une suite de divisibilité.*

(iii) Croissance exponentielle : $\lim_{\ell\to+\infty} \ln g_{\ell,P}/\ell = \ln M(P)$, *où* $M(P)$ *est la mesure de Mahler de* P.

(iv) Apparition de facteurs premiers primitifs : *Si* P *est irréductible, il existe une infinité de facteurs premiers primitifs dans la suite* $(g_{\ell,P})_\ell$ *(et des résultats plus précis).*

Exemple. Cas Fibonacci, $(g_{\ell,X^2-X-1})_\ell$=suite A001350 "Associated Mersenne numbers". Liste des facteurs premiers primitifs:
2, 5, 11, 29, 3, 19, 199, 521, 31, 7, 3571....

Questions ouvertes.

Trouver des résultats plus généraux/profonds sur les facteurs premiers primitifs.

Est-ce que tous les nombres premiers se retrouvent dans la suite A001350 ?

A partir d'ici, on omet la dépendance d'avec P.

Soit $B^{(\ell)}(X) = \sum_{0\le i<\ell} b_i^{(\ell)} X^i$ le polynôme entier tel que

$$\pm g_\ell = P(X)B^{(\ell)}(X) + (X^\ell - 1)\sum_{0\le i\le d-1} v_i^{(\ell)} X^i.$$

Proposition (Structure du groupe)

(i) *Le mot* $G_\ell := (10^{\ell-1})$ *est un élément d'ordre maximal.*

(ii) *L'exposant du groupe* $\mathcal{G}_\ell$ *est égal à* $g_\ell/\gcd((b_i^{(\ell)}),(v_j^{(\ell)}))$.

(iii) *Le groupe* $\mathcal{G}_\ell$ *est cyclique engendré par* G_ℓ *ssi* $\gcd(b_i^{(\ell)}, g_\ell) = 1$ *pour un certain (tout)* i. *Dans ce cas, la suite* $(b_i^{(\ell)} \pmod{g_\ell})_i$ *est géométrique, et l'inverse de sa raison est racine de* P *et racine* ℓ*-ème de l'unité dans* $\mathbb{Z}/g_\ell\mathbb{Z}$.

A partir d'ici, on omet la dépendance d'avec P.

Soit $B^{(\ell)}(X) = \sum_{0 \leq i < \ell} b_i^{(\ell)} X^i$ le polynôme entier tel que

$$\pm g_\ell = P(X) B^{(\ell)}(X) + (X^\ell - 1) \sum_{0 \leq i \leq d-1} v_i^{(\ell)} X^i.$$

Proposition (Structure du groupe)

(i) *Le mot $G_\ell := (10^{\ell-1})$ est un élément d'ordre maximal.*

(ii) *L'exposant du groupe $\mathcal{G}_\ell$ est égal à $g_\ell / \gcd((b_i^{(\ell)}), (v_j^{(\ell)}))$.*

(iii) *Le groupe $\mathcal{G}_\ell$ est cyclique engendré par G_ℓ ssi $\gcd(b_i^{(\ell)}, g_\ell) = 1$ pour un certain (tout) i. Dans ce cas, la suite $(b_i^{(\ell)} \pmod{g_\ell})_i$ est géométrique, et l'inverse de sa raison est racine de P et racine ℓ-ème de l'unité dans $\mathbb{Z}/g_\ell\mathbb{Z}$.*

Exemples.

- "Base b": ($b \geq 2$): $P(X) = X - b$, $g_\ell = b^\ell - 1$, $b_i^{(\ell)} = b^{\ell-1-i}$, $\mathcal{G}_\ell = \langle (10^{\ell-1}) \rangle \simeq \mathbb{Z}/(b^\ell - 1)\mathbb{Z}$.
- "Base rationnelle": $P(X) = pX - q$ ($q > p$ premiers entre eux), $g_\ell = q^\ell - p^\ell$, $b_i^{(\ell)} = p^i q^{\ell-1-i}$, $\mathcal{G}_\ell = \langle (10^{\ell-1}) \rangle \simeq \mathbb{Z}/(q^\ell - p^\ell)\mathbb{Z}$.

Afin de décrire plus précisément la structure des groupes $\mathcal{G}_\ell$, nous devons utiliser des outils algébriques.
Un outil simple est d'utiliser les relations de Bezout entre P et $X^\ell - 1$ (comme cela a été fait dans la proposition précédente). Mais il est difficile d'obtenir des résultats généraux pour des familles de polynômes.

Exemple. "Cas quadratique, généralisant Fibonacci"
Soit $P(X) = X^2 - kX - 1$, où $k \in \mathbb{N}^*$. Alors:

- Si ℓ est impair, $\mathcal{G}_\ell \simeq \mathbb{Z}/g_\ell\mathbb{Z}$, sauf pour $\ell \in 3\mathbb{N}$ et k impair, où $\mathcal{G}_\ell \simeq \mathbb{Z}/g_\ell/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
- Si $\ell \equiv 2 \bmod 4$, $\mathcal{G}_\ell \simeq \mathbb{Z}/\sqrt{g_\ell}\mathbb{Z} \times \mathbb{Z}/\sqrt{g_\ell}\mathbb{Z}$.
- Si $\ell \equiv 0 \bmod 4$, $\mathcal{G}_\ell \simeq \mathbb{Z}/\sqrt{\Delta g_\ell}\mathbb{Z} \times \mathbb{Z}/\sqrt{g_\ell/\Delta}\mathbb{Z}$ (cas k impair), ou $\mathcal{G}_\ell \simeq \mathbb{Z}/\sqrt{\Delta g_\ell/4}\mathbb{Z} \times \mathbb{Z}/\sqrt{4g_\ell/\Delta}\mathbb{Z}$ (cas k pair).
  ($\Delta = k^2 + 4$ est le discriminant de P)

(améliorations de résultats précédemment obtenus combinatoirement par Benoît Rittaud)

Remarque. On peut "expliciter" les générateurs correspondant à ces décompositions.

Autre Exemple. "Cas quadratique, généralisant encore plus Fibonacci".
Soit $P(X) = X^2 - qX + p$, avec $p, q \in \mathbb{Z}^*$ (+ conditions). Soit $\ell \geq 1$.
Alors:

- $\pm g_\ell = p^\ell - L_\ell + 1$
- pour $0 \leq i < \ell$, $b_i^{(\ell)} = p^{\ell-1-i}(F_i - F_{i-\ell})$
- $\mathcal{G}_\ell \simeq \mathbb{Z}/e_\ell\mathbb{Z} \times \mathbb{Z}/\delta_\ell\mathbb{Z}$, avec $\delta_\ell | e_\ell$, $g_\ell = e_\ell \cdot \delta_\ell$.
  Il peut être cyclique si $\delta_\ell = 1$.

où

$(L_n)_{n\in\mathbb{Z}}$ est une suite de type Lucas :
$$L_0 = 2,\ L_1 = q,\ L_{n+2} = qL_{n+1} - pL_n,$$
$(F_n)_{n\in\mathbb{Z}}$ est une suite de type Fibonacci :
$$F_0 = 1,\ F_1 = q,\ F_{n+2} = qF_{n+1} - pF_n.$$

Autre Exemple. "Cas quadratique, généralisant encore plus Fibonacci".
Soit $P(X) = X^2 - qX + p$, avec $p, q \in \mathbb{Z}^*$ (+ conditions). Soit $\ell \geq 1$.
Alors:

- $\pm g_\ell = p^\ell - L_\ell + 1$
- pour $0 \leq i < \ell$, $b_i^{(\ell)} = p^{\ell-1-i}(F_i - F_{i-\ell})$
- $\mathcal{G}_\ell \simeq \mathbb{Z}/e_\ell\mathbb{Z} \times \mathbb{Z}/\delta_\ell\mathbb{Z}$, avec $\delta_\ell | e_\ell$, $g_\ell = e_\ell \cdot \delta_\ell$.
  Il peut être cyclique si $\delta_\ell = 1$.

où

$(L_n)_{n\in\mathbb{Z}}$ est une suite de type Lucas :

$$L_0 = 2,\ L_1 = q,\ L_{n+2} = qL_{n+1} - pL_n,$$

$(F_n)_{n\in\mathbb{Z}}$ est une suite de type Fibonacci :

$$F_0 = 1,\ F_1 = q,\ F_{n+2} = qF_{n+1} - pF_n.$$

Questions Ouvertes

- Etudier plus précisément ce cas.
- Etudier des cas où P n'est pas unitaire.
- Trouver des outils algébriques/calculatoires plus pertinents.

Rappelons que $(g_\ell)_\ell$ est une suite de divisibilité: $g_\ell | g_{\ell\ell'}$.

Théorème (Sous-groupes)

Soit ℓ et ℓ' des entiers ≥ 1.

L'application $\begin{array}{ccc} \mathcal{G}_\ell & \longrightarrow & \mathcal{G}_{\ell\ell'} \\ W & \longmapsto & W^{\ell'} = W \dots W \ \ (\ell' \ fois) \end{array}$

est un morphisme injectif de $\mathcal{G}_\ell$ dans $\mathcal{G}_{\ell\ell'}$.

De même, $\mathcal{G}_{\ell'}$ s'injecte dans $\mathcal{G}_{\ell\ell'}$ par $W \mapsto W^\ell$.

Considérant $\mathcal{G}_\ell$ et $\mathcal{G}_{\ell'}$ comme sous-groupes de $\mathcal{G}_{\ell\ell'}$, leur intersection est égale à $\mathcal{G}_{gcd(\ell,\ell')}$:

$$\mathcal{G}_{gcd(\ell,\ell')} = \mathcal{G}_\ell \cap \mathcal{G}_{\ell'} \subset \mathcal{G}_\ell (ou\ \mathcal{G}_{\ell'}) \subset \mathcal{G}_{\ell\ell'}.$$

Démonstration: Outils algébriques simples, travail sur les polynômes entiers.

Remarque. Malgré tout, en général, $g_{\mathrm{gcd}(\ell,\ell')} \neq \mathrm{gcd}(g_\ell, g_{\ell'})$.

Définition (Groupe global de mots circulaires)

On peut définir la limite inductive $\mathcal{G} = \varinjlim \mathcal{G}_\ell$ *selon les morphismes*

$\begin{array}{l} \mathcal{G}_\ell \longrightarrow \mathcal{G}_m \\ W \longmapsto W^{m/\ell} \end{array}$ *, définis dès que* ℓ *divise* m*.*

Addition de deux mots circulaires de différentes longueurs.

Exemple:

Soit $W = (w_0 w_1 w_2)$ et $W' = (w'_0 w'_1)$, alors

$W + W' = (w_0 w_1 w_2 w_0 w_1 w_2) + (w'_0 w'_1 w'_0 w'_1 w'_0 w'_1)$.

Plus généralement:

Si W (resp. W') est un mot circulaire de longueur ℓ (resp. ℓ'), alors

$W + W' = W^{n/\ell} + W'^{n/\ell'} \in \mathcal{G}_n$, avec $n = \mathrm{ppcm}(\ell, \ell')$.

But: Associer une valeur numérique aux mots circulaires.

But: Associer une valeur numérique aux mots circulaires.

On peut définir un morphisme de groupes abéliens:

$$\begin{array}{cccc} N_\ell : & \mathcal{G}_\ell & \longrightarrow & \mathbb{Z}/g_\ell\mathbb{Z} \\ & (w_0 \ldots w_{\ell-1}) & \longmapsto & \displaystyle\sum_{0 \le i < \ell} w_i b_{\ell-i}^{(\ell)} \pmod{g_\ell}. \end{array}$$

Remarque. En terme de polynômes, cela revient à considérer $(W(X)B(X) \mod X^\ell - 1)(0)$ modulo g_ℓ.

Proposition (Propriétés de N_ℓ)

- *Si $\mathcal{G}_\ell$ est cyclique, alors N_ℓ est un isomorphisme.*
- *L'image de N_ℓ est $\mathbb{Z}/e_\ell\mathbb{Z}$ où e_ℓ est l'exposant du groupe $\mathcal{G}_\ell$.*
- *Les morphismes N_ℓ sont compatibles avec la limite inductive des $\mathcal{G}_\ell$.*

Cette application va nous permettre de définir un système de numération.

Soit e_ℓ l'exposant du groupe $\mathcal{G}_\ell$.
On a : e_ℓ divise g_ℓ, la suite $(e_\ell)_\ell$ est une suite de divisibilité et possède les mêmes facteurs premiers que $(g_\ell)_\ell$.

Nous pouvons alors définir :

Proposition (Système de numération sur $\mathcal{G}$)

Le morphisme $N : \mathcal{G} \to [0,1[$, tel que pour tout $W \in \mathcal{G}_\ell$,

$$N(W) = \{\frac{1}{e_\ell} \cdot \frac{e_\ell}{g_\ell} N_\ell(W)\} = \{\frac{1}{e_\ell} \cdot \frac{e_\ell}{g_\ell} \sum_{0 \leq i < \ell} w_i b_{\ell-i}^{(\ell)}\},$$

où $\{x\}$ est la partie fractionnaire de x, est bien défini.

Remarque. La somme $\frac{e_\ell}{g_\ell} \sum_{0 \leq i < \ell} w_i b_{\ell-i}^{(\ell)}$ est définie modulo e_ℓ.

Cela nous donne une représentation de certains rationnels de $[0,1[$ par un mot circulaire, compatible avec l'addition et la relation de retenue définie par P.

Exemples.

- "Base b" $(b \geq 2)$: $P(X) = X - b$, $g_\ell = b^\ell - 1$, $b_i^{(\ell)} = b^{\ell-1-i}$, $\mathcal{G}_\ell \simeq \mathbb{Z}/(b^\ell - 1)\mathbb{Z}$. Alors:

$$N((w_0 \ldots w_{\ell-1})) = \{\frac{1}{b^\ell - 1} \sum_{1 \leq i \leq \ell} w_i b^{i-1}\} \in [0,1[$$

Exemples.

- "Base b" $(b \geq 2)$: $P(X) = X - b$, $g_\ell = b^\ell - 1$, $b_i^{(\ell)} = b^{\ell-1-i}$, $\mathcal{G}_\ell \simeq \mathbb{Z}/(b^\ell - 1)\mathbb{Z}$. Alors:
$$N((w_0 \dots w_{\ell-1})) = \{\frac{1}{b^\ell - 1} \sum_{1 \leq i \leq \ell} w_i b^{i-1}\} \in [0,1[$$

  Cela est similaire à l'expression usuelle de l'écriture en base b:
$$0.\overline{w_0 \cdots w_{\ell-1}} = \sum_{0 \leq i < \ell} w_i \sum_{k \geq 0} \frac{1}{b^{k\ell+i+1}} = \frac{1}{b^\ell - 1} \sum_{0 \leq i < \ell} w_i b^{\ell-i-1}.$$

  Nous obtenons alors tous les nombres rationnels de dénominateurs de la forme $b^\ell - 1$.

Exemples.

- "Base b" $(b \geq 2)$: $P(X) = X - b$, $g_\ell = b^\ell - 1$, $b_i^{(\ell)} = b^{\ell-1-i}$, $\mathcal{G}_\ell \simeq \mathbb{Z}/(b^\ell - 1)\mathbb{Z}$. Alors:

$$N((w_0 \dots w_{\ell-1})) = \{\frac{1}{b^\ell - 1} \sum_{1 \leq i \leq \ell} w_i b^{i-1}\} \in [0,1[$$

Cela est similaire à l'expression usuelle de l'écriture en base b:
$$0.\overline{w_0 \cdots w_{\ell-1}} = \sum_{0 \leq i < \ell} w_i \sum_{k \geq 0} \frac{1}{b^{k\ell+i+1}} = \frac{1}{b^\ell - 1} \sum_{0 \leq i < \ell} w_i b^{\ell-i-1}.$$

Nous obtenons alors tous les nombres rationnels de dénominateurs de la forme $b^\ell - 1$.
Par exemple, en base 10, on obtient l'isomorphisme de groupes abéliens: $\begin{array}{ccc} \mathcal{G} & \longrightarrow & E = \quad \{n \in [0,1[, n = a/99\cdots 9,\ a \in \mathbb{N}\} \\ W & \longmapsto & N(W) \end{array}$
E est l'ensemble des rationnels de $[0,1[$ dont les dénominateurs sont premiers avec 10 (sauf 0).

Exemples.

- "Base Rationnelle": $P(X) = pX - q$ ($q > p$ premiers entre eux), $g_\ell = q^\ell - p^\ell$, $b_i^{(\ell)} = p^i q^{\ell-1-i}$, $\mathcal{G}_\ell \simeq \mathbb{Z}/(q^\ell - p^\ell)\mathbb{Z}$. Alors:
$$N((w_0 \dots w_{\ell-1})) = \{\frac{1}{q^\ell - p^\ell} \cdot \frac{1}{q} \sum_{1 \leq i \leq \ell} w_i p^{\ell-i} q^i\} \in [0,1[$$

Exemples.

- "Base Rationnelle" : $P(X) = pX - q$ ($q > p$ premiers entre eux), $g_\ell = q^\ell - p^\ell$, $b_i^{(\ell)} = p^i q^{\ell-1-i}$, $\mathcal{G}_\ell \simeq \mathbb{Z}/(q^\ell - p^\ell)\mathbb{Z}$. Alors:
$$N((w_0 \dots w_{\ell-1})) = \{\frac{1}{q^\ell - p^\ell} \cdot \frac{1}{q} \sum_{1 \leq i \leq \ell} w_i p^{\ell-i} q^i\} \in [0,1[$$
C'est similaire à l'expression trouvée lorsque nous considérons un développement en "base p/q" :
$$0.\overline{w_0 \cdots w_{\ell-1}} = \sum_{0 \leq i < \ell} w_i \sum_{k \geq 0} \frac{p^{k\ell+i}}{q^{k\ell+i+1}} = \frac{1}{q^\ell - p^\ell} \cdot \frac{1}{q} \sum_{0 \leq i < \ell} w_i p^i q^{\ell-i}.$$
Ainsi, on peut représenter tout nombre rationnel de $[0,1[$, dont les dénominateurs (forme irréductible) sont premiers avec p et q, par un mot circulaire de longueur finie.

Exemples.

- "Base Rationnelle": $P(X) = pX - q$ ($q > p$ premiers entre eux), $g_\ell = q^\ell - p^\ell$, $b_i^{(\ell)} = p^i q^{\ell-1-i}$, $\mathcal{G}_\ell \simeq \mathbb{Z}/(q^\ell - p^\ell)\mathbb{Z}$. Alors:

$$N((w_0 \dots w_{\ell-1})) = \{\frac{1}{q^\ell - p^\ell} \cdot \frac{1}{q} \sum_{1 \leq i \leq \ell} w_i p^{\ell-i} q^i\} \in [0,1[$$

C'est similaire à l'expression trouvée lorsque nous considérons un développement en "base p/q":

$$0.\overline{w_0 \cdots w_{\ell-1}} = \sum_{0 \leq i < \ell} w_i \sum_{k \geq 0} \frac{p^{k\ell+i}}{q^{k\ell+i+1}} = \frac{1}{q^\ell - p^\ell} \cdot \frac{1}{q} \sum_{0 \leq i < \ell} w_i p^i q^{\ell-i}.$$

Ainsi, on peut représenter tout nombre rationnel de $[0,1[$, dont les dénominateurs (forme irréductible) sont premiers avec p et q, par un mot circulaire de longueur finie.

Exemple numérique: Considérons $P(X) = 2X - 3$.

Pour $a = 13/35$: $\ell = 6$, $g_6 = 665 = 35 * 19$, $a = N((2\,0\,1\,0\,2\,1))$.

Pour $b = 4/5$: $\ell = 2$, $g_2 = 5$, $b = N((0\,2)) = N((0\,2\,0\,2\,0\,2))$.

Alors $a + b = 6/35 = N((2\,2\,1\,2\,2\,3)) = N((1\,1\,0\,1\,1\,2))$.

Exemples.

- "Fibonacci": $P(X) = X^2 - X - 1$.
  Avec la suite de Fibonacci: $f_0 = 0$, $f_1 = 1$, $f_{n+2} = f_{n+1} + f_n$,
  on obtient: $g_\ell = f_{\ell-1} + f_{\ell+1} - 1 + (-1)^{\ell+1}$,
  $e_\ell = g_\ell$, ou $g_\ell/2$ ou $\sqrt{g_\ell}$ ou $\sqrt{5g_\ell}$ et

$$
\begin{aligned}
N((w_0 \dots w_{\ell-1})) &= \{\frac{1}{e_\ell} \cdot \frac{e_\ell}{g_\ell} \sum_{0\le i<\ell} w_{i+1} \left[f_i + (-1)^i f_{\ell-i}\right]\} \\
&= \{\frac{1}{e_\ell} \cdot \frac{e_\ell}{g_\ell} \sum_{0\le i<\ell} w_{i+1} \left[f_i + (-1)^{\ell+1} f_{-\ell+i}\right]\} \in [0,1[
\end{aligned}
$$

Exemples.

- "Fibonacci": $P(X) = X^2 - X - 1$.
  Avec la suite de Fibonacci: $f_0 = 0$, $f_1 = 1$, $f_{n+2} = f_{n+1} + f_n$,
  on obtient: $g_\ell = f_{\ell-1} + f_{\ell+1} - 1 + (-1)^{\ell+1}$,
  $e_\ell = g_\ell$, ou $g_\ell/2$ ou $\sqrt{g_\ell}$ ou $\sqrt{5g_\ell}$ et

$$\begin{aligned} N((w_0 \dots w_{\ell-1})) &= \{\frac{1}{e_\ell} \cdot \frac{e_\ell}{g_\ell} \sum_{0 \le i < \ell} w_{i+1} \left[f_i + (-1)^i f_{\ell-i}\right]\} \\ &= \{\frac{1}{e_\ell} \cdot \frac{e_\ell}{g_\ell} \sum_{0 \le i < \ell} w_{i+1} \left[f_i + (-1)^{\ell+1} f_{-\ell+i}\right]\} \in [0,1[\end{aligned}$$

  Liens avec le système de numération usuel de Fibonacci ?

  Exemple numérique: $\ell = 5$, $g_5 = e_5 = 11$,
  $N((1\,0\,0\,0\,0)) = 4/11$, $N((0\,1\,0\,0\,0)) = 5/11$, $N((0\,0\,1\,0\,0)) = 9/11$,
  $N((0\,0\,0\,1\,0)) = 3/11$, $N((0\,0\,0\,0\,1)) = 1/11$, $N((1\,0\,1\,0\,0)) = 2/11$,
  $N((1\,0\,0\,1\,0)) = 7/11$, $N((0\,1\,0\,1\,0)) = 8/11$, $N((0\,1\,0\,0\,1)) = 6/11$,
  $N((0\,0\,1\,0\,1)) = 10/11$

Travail en cours, cas Fibonacci:

Démontrer que tout nombre x de $\mathbb{Q}(\sqrt{5}) \cap [0;1[$ peut s'écrire comme limite d'une suite de mots circulaires "périodiques", c'est-à-dire:

$$x = \lim_{n \to +\infty} N\left(w_0 \cdots w_{r-1} \overline{w_r \cdots w_{r+p-1}}^{n}\right)$$

où $w_0 \cdots w_{r-1}$ représente une pré-période, et $w_r \cdots w_{r+p-1}$ une période.

Cela suppose que tous les nombres premiers se retrouvent dans la suite des (g_ℓ) (ou (e_ℓ)).
Si cela n'est pas le cas, on pourra atteindre tous les nombres dont le dénominateur est composé de nombres premiers apparaissant dans ces suites.

Travail en cours - Questions ouvertes.

Pour un polynôme P fixé (ou une famille de polynômes):

- En théorie et de façon algorithmique, décrire les rationnels qui sont dans $N(\mathcal{G})$, déterminer le plus petit entier ℓ tel que $a \in N(\mathcal{G}_\ell)$.
- Pour un réel x de $[0, 1[$, peut-on trouver une suite de mots circulaires dont les valeurs convergent vers x ? Etudier la convergence des valeurs de certaines suites de mots.
- Quelles sont les représentations canoniques d'un mot circulaire décrites en terme de conditions sur les chiffres ?
  (déjà fait pour les cas $X - b$, $pX - q$, $X^2 - kX - 1$)
- Etudier plus en détail les relations entre les sous-groupes de $\mathcal{G}$, les racines de P modulo n, les racines/facteurs de $X^\ell - 1$, et autres. Quand p est un facteur premier primitif de g_ℓ, il existe un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z}$, qui n'est pas de type $\mathcal{G}_n$. Interprétation ?

Travail en cours - Questions ouvertes.

- Quand $\mathcal{G}_\ell$ n'est pas cyclique, par exemple est de type $E = \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, chaque élément de E a une unique représentation par un mot circulaire.
  Représentation par un mot du couple $(a, b) \in [0, 1[^2$: interprétation ?
- Multiplication de mots circulaires ?
- Autres questions...
- Et bien sûr, autres connections avec des sujets usuels en numération ? en théorie des nombres ?

Merci !

- Benoît RITTAUD, "Structure of Classes of Circular Words defined by a Quadratic Equivalence", *RIMS Kôkyûroku Bessatsu*, **B 46**, 231-239 (2014-06).
- Benoît RITTAUD & Laurent VIVIER, "Circular words and three applications: factors of the Fibonacci word, $\mathcal{F}$-adic numbers, and the sequence 1, 5, 16, 45, 121, 320,. . . ", *Functiones et Approximatio* **47**, n°2, 207-231 (2012).