Fractions continues et actions des groupes de congruence sur la droite réelle

Cedric TROESSAERT *
(avec un appendice par Alain VALETTE)

Abstract

We characterize the orbits of the principal congruence subgroup $\Gamma(n)$ of $GL_2(\mathbb{Z})$ acting by fractional linear transformations on the real line. The characterization is in terms of congruence properties $\pmod n$ of the numerators and denominators of the convergents of some number in a given orbit.

1 Introduction

Soit x un nombre réel: notons

$$x = [a_0; a_1, a_2, \ldots]$$

son développement en fraction continue régulière, c-à-d.:

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

où $a_0 \in \mathbb{Z}$ et $a_n \in \mathbb{N} - \{0\}$ pour $n \geq 1$. Le développement est fini si x est rationnel, infini sinon. Les réduites de x sont les fractions irréductibles $\frac{p_n}{q_n} = [a_0; a_1, a_2, \ldots, a_n]$. Si $x = [a_0; a_1, a_2, \ldots]$ et $y = [b_0; b_1, b_2, \ldots]$ sont deux nombres irrationnels, nous dirons que x et y *ont la même queue* s'il existe $N, M \in \mathbb{N}$ tels que $a_{N+k} = b_{M+k}$ pour tout $k > 0$.

Le groupe $GL_2(\mathbb{Z})$ agit par homographies sur la droite projective réelle $P^1(\mathbb{R}) = \mathbb{R} \cup \{\infty\}$: pour une matrice $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$, notons α_A l'homographie $x \mapsto \frac{ax+b}{cx+d}$. On notera aussi $A \cdot x$ pour $\alpha_A(x)$. Un résultat classique (voir l'appendice pour une preuve

*Ce travail a été réalisé grâce au subside 20.101469 du FNRS suisse.

ainsi que des références) dit que deux réels sont dans la même orbite de $GL_2(\mathbb{Z})$ si et seulement si ils ont même queue.

Les *groupes de congruence* sont les sous-groupes normaux d'indice fini de $GL_2(\mathbb{Z})$ définis par:

$$\Gamma(n) = \{\gamma \in GL_2(\mathbb{Z}),\ \gamma \equiv \pm I \pmod{n}\}$$

$(n \geq 2)$. Le but de cet article est de caractériser les orbites de $\Gamma(n)$ sur $P^1(\mathbb{R})$. Nous verrons qu'il y a trois cas à considérer: nombres rationnels, nombres irrationnels non quadratiques, nombres irrationnels quadratiques. Les résultats correspondants sont les Théorèmes 1, 5 et 6. Par exemple, le Théorème 5 s'énonce:

Soient x, y sont deux irrationnels non quadratiques ayant la même queue: $x = [a_0; a_1, a_2, ..., a_N, c_0, c_1, ...]$ et $y = [b_0; b_1, b_2, ..., b_M, c_0, c_1, ...]$ (avec $N, M \geq 1$); notons $\frac{p_i}{q_i}$ (resp. $\frac{A_j}{B_j}$) les réduites de x (resp. y). Les nombres x et y appartiennent à la même orbite de $\Gamma(n)$ si et seulement si

$$p_N \equiv A_M,\ p_{N-1} \equiv A_{M-1},\ q_N \equiv B_M,\ q_{N-1} \equiv B_{M-1} \pmod{n}$$

ou

$$p_N \equiv -A_M,\ p_{N-1} \equiv -A_{M-1},\ q_N \equiv -B_M,\ q_{N-1} \equiv -B_{M-1} \pmod{n}.$$

On peut donc lire les orbites en comparant les réduites des irrationnels.

Notation: Dans tout l'article, pour deux réels x et y, nous noterons $x = [a_0; a_1, a_2, ...]$ (resp. $\frac{p_i}{q_i}$) le développement en fraction continue (resp. les réduites) de x, et $y = [b_0; b_1, b_2, ...]$ (resp. $\frac{A_j}{B_j}$) le développement (resp. les réduites) de y.

Remerciements: Mes plus vifs remerciements au professeur Alain Valette qui durant un mois m'a accueilli à Neuchâtel. Je remercie aussi le FNRS suisse qui a pris en charge les frais de séjour.

2 Orbites sur les rationnels

Pour commencer, étudions les orbites de $\Gamma(n)$ sur les rationnels que nous considérerons comme des fractions irréductibles d'entiers à dénominateur positif (en prenant $0 = 0/1$ et $\infty = 1/0$).

Lemme 1 *Soit $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ un élément de $GL_2(\mathbb{Z})$; si $\alpha_S \begin{pmatrix} p \\ q \end{pmatrix} = \dfrac{A}{B}$, alors*

- *$A = ap + bq$ et $B = cp + dq$ si $cp + dq > 0$,*

- $A = -(ap+bq)$ *et* $B = -(cp+dq)$ *si* $cp+dq < 0$.

Preuve: On a $S \cdot \begin{pmatrix} \frac{p}{q} \end{pmatrix} = \frac{ap+bq}{cp+dq} = \frac{A}{B}$, donc, en appliquant $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$:

$$\begin{cases} d(ap+bq) - b(cp+dq) & = & \pm p \\ -c(ap+bq) + a(cp+dq) & = & \pm q, \end{cases}$$

ce qui montre que $ap+bq$ et $cp+dq$ sont premiers entre eux. Comme B est positif, il vient

- $A = ap+bq$ et $B = cp+dq$ si $cp+dq > 0$,
- $A = -(ap+bq)$ et $B = -(cp+dq)$ si $cp+dq < 0$. $\square$

Les orbites de $\Gamma(n)$ sur les rationnels sont décrites par le:

Théorème 1 *Les rationnels* $\frac{p}{q}$, $\frac{A}{B}$ *appartiennent à la même orbite de* $\Gamma(n)$ *si et seulement si* $p \equiv A \pmod{n}$ *et* $q \equiv B \pmod{n}$ *ou* $p \equiv -A \pmod{n}$ *et* $q \equiv -B \pmod{n}$.

Preuve:

Condition nécessaire : Soit $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(n)$ tel que $\alpha_S \begin{pmatrix} \frac{p}{q} \end{pmatrix} = \frac{A}{B}$.

On a deux possibilités:

- soit $cp+dq > 0$ et donc par le lemme 1: $ap+bq = A$ et $cp+dq = B$. Si $S \equiv I \pmod{n}$ alors $a \equiv d \equiv 1 \pmod{n}$ et $b \equiv c \equiv 0 \pmod{n}$, donc $p \equiv A$ et $q \equiv B \pmod{n}$; si $S \equiv -I \pmod{n}$ alors $a \equiv d \equiv -1 \pmod{n}$ et $b \equiv c \equiv 0 \pmod{n}$, donc $p \equiv -A$ et $q \equiv -B \pmod{n}$;
- soit $cp+dq < 0$, on a $ap+bq = -A$ et $cp+dq = -B$ qui mènent aux mêmes conclusions.

Deux cas peuvent poser problème: $\frac{p}{q} = 0$ ou $\frac{p}{q} = \infty$, traitons les à part:

- si $\alpha_S(0) = \frac{A}{B}$ avec $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(n)$, alors $\frac{b}{d} = \frac{A}{B}$ et comme b et d sont premiers entre eux, on a $A = b$, $B = d$ ou $A = -b$, $B = -d$. Dès lors $A \equiv 0 \pmod{n}$ et $B \equiv \pm 1 \pmod{n}$.

- si $\alpha_S(\infty) = \dfrac{A}{B}$ avec $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(n)$, alors $\dfrac{a}{c} = \dfrac{A}{B}$ et comme a et c sont premiers entre eux, on a $A = a$, $B = c$ ou $A = -a$, $B = -c$. Dès lors $A \equiv \pm 1 \pmod n$ et $B \equiv 0 \pmod n$.

Condition suffisante : Prouvons en premier lieu que l'orbite de 0 sous $\Gamma(n)$ est

$$\left\{ \frac{p}{q} \mid p \equiv 0 \pmod n,\ \ q \equiv \pm 1 \pmod n \right\}.$$

Il suffit de prouver que si $\dfrac{p}{q}$ est tel que $p \equiv 0 \pmod n$ et $q \equiv \pm 1 \pmod n$ alors il existe $S \in \Gamma(n)$ tel que $\alpha_S(0) = \dfrac{p}{q}$. Prenons $p = na$ et $q = nb + 1$ (le cas $q \equiv -1 \pmod n$ est similaire); comme p et q sont premiers entre eux, il existe $x, y \in \mathbb{Z}$ tels que $xq - yp = -b$, d'où: $(nx + 1)q - nyp = 1$. On en tire que $S = \begin{pmatrix} nx + 1 & p \\ ny & q \end{pmatrix}$ appartient à $\Gamma(n)$ car $p \equiv 0 \pmod n$ et $q \equiv 1 \pmod n$. De plus $\alpha_S(0) = \dfrac{p}{q}$. On

prouve de manière semblable que l'orbite de ∞ sous $\Gamma(n)$ est

$$\left\{ \frac{p}{q} \mid p \equiv \pm 1 \pmod n,\ \ q \equiv 0 \pmod n \right\} \cup \{\infty\}.$$

Maintenant, nous pouvons démontrer que si $\dfrac{p}{q}, \ \dfrac{A}{B} \in \mathbb{Q}$ sont tels que $p \equiv A,\ q \equiv B$

$\pmod n$, (le cas $p \equiv -A$, $q \equiv -B \pmod n$ est similaire) alors il existe $S \in \Gamma(n)$ telle que $\alpha_S\left(\dfrac{p}{q}\right) = \dfrac{A}{B}$. Comme $\mathbb{Q} \cup \{\infty\}$ est une orbite de $GL_2(\mathbb{Z})$, il existe $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ tel que $\alpha_T\left(\dfrac{p}{q}\right) = \dfrac{n}{n+1} \in \Gamma(n)(0)$, c-à-d. $\begin{cases} ap + bq = n \\ cp + dq = n + 1 \end{cases}$. Prouvons maintenant que $\alpha_T\left(\dfrac{A}{B}\right) \in \Gamma(n)(0)$. Deux possi-

bilités doivent être envisagées:

- si $cA + dB > 0$, alors on a $\begin{cases} aA + bB \equiv ap + dq \equiv 0 \pmod n \\ cA + dB \equiv cp + dq \equiv 1 \pmod n \end{cases}$,
- si $cA + dB < 0$, alors on a $\begin{cases} -(aA + bB) \equiv -(ap + dq) \equiv 0 \pmod n \\ -(cA + dB) \equiv -(cp + dq) \equiv -1 \pmod n \end{cases}$,

et $\alpha_T\left(\dfrac{A}{B}\right) \in \Gamma(n)(0)$. Le cas $cA+dB=0$ est exclu car $cA+dB \equiv cp+dq \not\equiv 0 \pmod n$. Nous avons montré que $\alpha_T\left(\dfrac{p}{q}\right)$ et $\alpha_T\left(\dfrac{A}{B}\right)$ appartiennent tous deux à l'orbite de 0 sous $\Gamma(n)$. On en déduit qu'il existe $C \in \Gamma(n)$ tel que $(C \circ T) \cdot \left(\dfrac{p}{q}\right) = T \cdot \left(\dfrac{A}{B}\right)$ et donc $(T^{-1} \circ C \circ T) \cdot \left(\dfrac{p}{q}\right) = \dfrac{A}{B}$. Comme $\Gamma(n)$ est un sous-groupe normal de $GL_2(\mathbb{Z})$, on a $S = T^{-1} \circ C \circ T \in \Gamma(n)$. □

3 Orbites sur les irrationnels

L'objet de cette partie est d'étudier les orbites de $\Gamma(n)$ sur les irrationnels. Nous aurons besoin de quelques résultats décrivant l'action de $GL_2(\mathbb{Z})$ sur ceux-ci.

3.1 Résultats préliminaires

Proposition 2 *Soit* $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ *et* $x, y \in \mathbb{R} \setminus \mathbb{Q}$ *tels que*

$$\begin{cases} \alpha_T(x) = y \\ cx+d > 0 \end{cases} \quad \textit{avec} \quad \begin{cases} x = [a_0; a_1, ...] \textit{ de réduites } p_i/q_i \\ y = [b_0; b_1, ...] \textit{ de réduites } A_j/B_j \end{cases}$$

alors il existe $u \in \mathbb{N}_0$, $v > -u$ *tels que*

$$a_i = b_{i+v} \qquad \textit{pour tout } i > u \quad \textit{(c-à-d.: } x \textit{ et } y \textit{ ont même queue), et}$$

$$\begin{cases} ap_u + bq_u = A_{v+u} \\ cp_u + dq_u = B_{v+u} \end{cases} \quad \begin{cases} ap_{u-1} + bq_{u-1} = A_{v+u-1} \\ cp_{u-1} + dq_{u-1} = B_{v+u-1} \end{cases}.$$

La démonstration de cette Proposition découle directement de la preuve du Théorème 174 à la page 143 dans [HW75].

Proposition 3 *Soit* $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ *et* $x, y \in \mathbb{R}$, $x = [a_0; a_1, ...]$, $y = [b_0; b_1, ...]$ *tels qu'il existe* $i, j \geq 1$ *pour lesquels*

$$\begin{cases} ap_i + bq_i = A_j \\ cp_i + dq_i = B_j \end{cases} \quad \textit{et} \quad \begin{cases} ap_{i-1} + bq_{i-1} = A_{j-1} \\ cp_{i-1} + dq_{i-1} = B_{j-1} \end{cases};$$

alors

1) si $i, j \geq 2$ *et* $a_i = b_j$ *alors* $\left\{ \begin{array}{l} ap_{i-2} + bq_{i-2} = A_{j-2} \\ cp_{i-2} + dq_{i-2} = B_{j-2} \end{array} \right.$;

2) si $a_{i+1} = b_{j+1}$ *alors* $\left\{ \begin{array}{l} ap_{i+1} + bq_{i+1} = A_{j+1} \\ cp_{i+1} + dq_{i+1} = B_{j+1} \end{array} \right.$.

Preuve: Si $a_i = b_j$, on a

$$A_{j-2} = A_j - b_j A_{j-1} = ap_i + bq_i - b_j(ap_{i-1} + bq_{i-1}) = a(p_i - a_i p_{i-1}) + b(q_i - a_i q_{i-1}) = ap_{i-2} + bq_{i-2}.$$

Toutes les autres égalités s'obtiennent grâce à des calculs analogues. □

Pour décider pratiquement si deux irrationnels sont dans la même orbite sous $GL_2(\mathbb{Z})$, on ne sait pas *a priori* faire la différence entre le début et la queue d'un développement en fraction continue. Les deux résultats précédents montrent que toutes les découpes sont équivalentes.

3.2 Irrationnels non quadratiques

Théorème 4 *Soit* x, y *deux irrationnels non quadratiques ayant même queue, c-à-d. tels que* $x = [a_0; a_1, a_2, ...]$, $y = [b_0; b_1, b_2, ...]$ *avec* $a_i = b_{i+M-N}$ *pour* $i > N$. *Soit* $T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$. *Sont équivalentes:*

i) $\left\{ \begin{array}{l} \alpha_T(x) = y \\ cx + d > 0 \end{array} \right.$;

ii) $\left\{ \begin{array}{l} ap_N + bq_N = A_M \\ cp_N + dq_N = B_M \end{array} \right.$ *et* $\left\{ \begin{array}{l} ap_{N-1} + bq_{N-1} = A_{M-1} \\ cp_{N-1} + dq_{N-1} = B_{M-1} \end{array} \right.$.

Preuve:

$(i) \Rightarrow (ii)$: En appliquant la Proposition 2 aux hypothèses, on voit qu'il existe $u \in \mathbb{N}_0$, $v > -u$ tels que

(1) Pour tout $i > u$: $a_i = b_{i+v}$,

(2) $\left\{ \begin{array}{l} ap_u + bq_u = A_{u+v} \\ cp_u + dq_u = B_{u+v} \end{array} \right.$ et $\left\{ \begin{array}{l} ap_{u-1} + bq_{u-1} = A_{u+v-1} \\ cp_{u-1} + dq_{u-1} = B_{u+v-1} \end{array} \right.$.

On a donc, par **(1)** , pour i assez grand: $a_i = b_{i+v} = a_{i+N-M+v}$. Comme la queue est non périodique, puisque x, y sont non quadratiques, le décalage $N - M + v$ est nul et donc $v = M - N$. Nous pouvons maintenant appliquer la Proposition 3:

- si $u \leq N$ alors **(1)** assure les égalités $a_{i+1} = b_{i+M-N+1}$ pour $i \geq u$, et on obtient

$$\begin{cases} ap_N + bq_N = A_M \\ cp_N + dq_N = B_M \end{cases} \text{ et } \begin{cases} ap_{N-1} + bq_{N-1} = A_{M-1} \\ cp_{N-1} + dq_{N-1} = B_{M-1} \end{cases}.$$

- si $u > N$ on utilise le fait que x et y ont la même queue et on obtient les mêmes égalités.

$(ii) \Rightarrow (i)$: Soit $c_i = a_{i+N+1} = b_{i+M+1}$ $(i \geq 0)$. Les matrices $\begin{pmatrix} p_N & p_{N-1} \\ q_N & q_{N-1} \end{pmatrix}$ et $\begin{pmatrix} A_M & A_{M-1} \\ B_M & B_{M-1} \end{pmatrix}$ appartiennent à $GL_2(\mathbb{Z})$, et on a, par la formule 11 du Chapitre 1 de [Per13]:

$$x = \begin{pmatrix} p_N & p_{N-1} \\ q_N & q_{N-1} \end{pmatrix} \cdot [c_0, c_1, c_2, ...] \text{ et } y = \begin{pmatrix} A_M & A_{M-1} \\ B_M & B_{M-1} \end{pmatrix} \cdot [c_0, c_1, c_2, ...].$$

Ainsi:

$$\begin{aligned} y &= \begin{pmatrix} A_M & A_{M-1} \\ B_M & B_{M-1} \end{pmatrix} \begin{pmatrix} p_N & p_{N-1} \\ q_N & q_{N-1} \end{pmatrix}^{-1} \cdot x \\ &= \begin{pmatrix} A_M & A_{M-1} \\ B_M & B_{M-1} \end{pmatrix} \begin{pmatrix} (-1)^{N-1} q_{N-1} & (-1)^N p_{N-1} \\ (-1)^N q_N & (-1)^{N-1} p_N \end{pmatrix} \cdot x \\ &= \begin{pmatrix} (-1)^{N-1}(A_M q_{N-1} - A_{M-1} q_N) & (-1)^{N-1}(-A_M p_{N-1} + A_{M-1} p_N) \\ (-1)^{N-1}(B_M q_{N-1} - B_{M-1} q_N) & (-1)^{N-1}(-B_M p_{N-1} + B_{M-1} p_N) \end{pmatrix} \cdot x. \end{aligned}$$

Les hypothèses sur A_M, B_M, A_{M-1}, B_{M-1} permettent finalement d'écrire

$$y = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot x.$$

En appliquant la Proposition 3, on obtient pour tout $i \geq N$:

$$cp_i + dq_i = B_{M+i-N} > 0.$$

On peut écrire $x = \dfrac{p_i}{q_i} + \dfrac{\delta}{q_i^2}$ où $|\delta| < 1$ (voir Théorème 171 dans [HW75]). Par conséquent

$$cx + d = c\left(\frac{p_i}{q_i} + \frac{\delta}{q_i^2}\right) + d = \frac{1}{q_i}\left(cp_i + dq_i + \frac{c\delta}{q_i}\right)$$

qui est positif pour un i suffisamment grand car $cp_i + dq_i \in \mathbb{N}_0$. $\square$

On voit que le lien entre deux nombres non quadratiques ayant même queue est entièrement déterminé par le morceau de fraction continue qui n'est pas commun, la queue ne compte pas.

Nous pouvons maintenant décrire les orbites de $\Gamma(n)$ sur les irrationnels non quadratiques:

Théorème 5 *Soient x, y deux irrationnels non quadratiques ayant la même queue: $x = [a_0; a_1, a_2, ..., a_N, c_0, c_1, ...]$ et $y = [b_0; b_1, b_2, ..., b_M, c_0, c_1, ...]$ avec $N, M \geq 1$.*

Les nombres x et y appartiennent à la même orbite de $\Gamma(n)$ si et seulement si

$$p_N \equiv A_M,\ p_{N-1} \equiv A_{M-1},\ q_N \equiv B_M,\ q_{N-1} \equiv B_{M-1} \pmod n$$

ou

$$p_N \equiv -A_M,\ p_{N-1} \equiv -A_{M-1},\ q_N \equiv -B_M,\ q_{N-1} \equiv -B_{M-1} \pmod n.$$

Preuve:

Condition nécessaire : Comme x, y appartiennent à la même orbite de $\Gamma(n)$, il existe $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(n)$ telle que $S \cdot x = y$ et $cx + d > 0$ (cette dernière condition est toujours réalisable car $-S \in \Gamma(n)$). Le théorème 4 nous donne

$$\left\{ \begin{array}{l} ap_N + bq_N = A_M \\ cp_N + dq_N = B_M \end{array} \right. \quad \text{et} \quad \left\{ \begin{array}{l} ap_{N-1} + bq_{N-1} = A_{M-1} \\ cp_{N-1} + dq_{N-1} = B_{M-1} \end{array} \right. .$$

On a deux possibilités:

1. $S \equiv I \pmod n$ Dans ce cas, $a \equiv d \equiv 1 \pmod n$ et $c \equiv b \equiv 0 \pmod n$ ce qui implique

$$A_M \equiv ap_N + bq_N \equiv 1.p_N + 0.q_N \equiv p_N \pmod n$$

et par un calcul semblable:

$$p_{N-1} \equiv A_{M-1},\ \ q_N \equiv B_M \ \text{ et } \ q_{N-1} \equiv B_{M-1} \pmod n.$$

2. $S \equiv -I \pmod n$ Dans ce cas, $a \equiv d \equiv -1 \pmod n$ et $c \equiv b \equiv 0 \pmod n$ ce qui implique

$$A_M \equiv -p_N,\ \ p_{N-1} \equiv -A_{M-1},\ \ q_N \equiv -B_M \ \text{ et } \ q_{N-1} \equiv -B_{M-1} \pmod n.$$

Condition suffisante : Supposons que $p_N \equiv A_M,\ p_{N-1} \equiv A_{M-1},\ q_N \equiv B_M$ et $q_{N-1} \equiv B_{M-1} \pmod n$. Dans $\mathbb{Z}^2$, considérons les paires de vecteurs $\left\{ \begin{pmatrix} p_N \\ q_N \end{pmatrix}, \begin{pmatrix} p_{N-1} \\ q_{N-1} \end{pmatrix} \right\}$ et $\left\{ \begin{pmatrix} A_M \\ B_M \end{pmatrix}, \begin{pmatrix} A_{M-1} \\ B_{M-1} \end{pmatrix} \right\}$. Comme $p_N q_{N-1} - p_{N-1} q_N = (-1)^{N-1}$ et $A_M B_{M-1} - A_{M-1} B_M = (-1)^{M-1}$, il s'agit de deux bases de $\mathbb{Z}^2$. Il existe donc une unique matrice $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$ telle que

$$\left\{ \begin{array}{l} ap_N + bq_N = A_M \\ cp_N + dq_N = B_M \end{array} \right. \quad \text{et} \quad \left\{ \begin{array}{l} ap_{N-1} + bq_{N-1} = A_{M-1} \\ cp_{N-1} + dq_{N-1} = B_{M-1} \end{array} \right. .$$

On applique le théorème 4 et on obtient $S \cdot x = y$. Prouvons maintenant que $S \in \Gamma(n)$. Grâce aux hypothèses sur les réduites, on a

$$\left\{ \begin{array}{c} ap_N + bq_N \equiv A_M \equiv p_N \\ ap_{N-1} + bq_{N-1} \equiv A_{M-1} \equiv p_{N-1} \end{array} \right. \quad \text{et} \quad \left\{ \begin{array}{c} cp_N + dq_N \equiv B_M \equiv q_N \\ cp_{N-1} + dq_{N-1} \equiv B_{M-1} \equiv q_{N-1} \end{array} \right. \qquad \pmod n$$

ce qui implique

$$\left\{ \begin{array}{l} (a-1)p_N p_{N-1} + bq_N p_{N-1} \equiv 0 \\ (a-1)p_{N-1} p_N + bq_{N-1} p_N \equiv 0 \end{array} \right. \qquad \pmod n$$

et

$$b(q_{N-1}p_N - q_N p_{N-1}) \equiv 0 \pmod n \text{ donc } b \equiv 0 \pmod n.$$

De même, on aura $(a-1) \equiv c \equiv (d-1) \equiv 0 \pmod n$, ce qui signifie que $S \equiv I \pmod n$ et donc $S \in \Gamma(n)$.

Si $p_N \equiv -A_M,\ p_{N-1} \equiv -A_{M-1},\ q_N \equiv -B_M$ et $q_{N-1} \equiv -B_{M-1} \pmod n$, on obtiendra de manière analogue $(a+1) \equiv b \equiv c \equiv (d+1) \equiv 0 \pmod n$ c'est-à-dire $S \equiv -I \pmod n$ et donc $S \in \Gamma(n)$. □

3.3 Irrationnels quadratiques

Dans le cas de deux irrationnels quadratiques, le théorème 4 devient:

Théorème 6 *Soient x, y deux irrationnels quadratiques ayant même queue: $x = [a_0; a_1, a_2, ..., a_N, \overline{c_0, c_1, ...,}$ et $y = [b_0; b_1, b_2, ..., b_M, \overline{c_0, c_1, ...c_{k-1}}]$ avec $N, M, k \geq 1$; soit $S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$.*

On a $\left\{\begin{array}{c} S\cdot x=y \\ cx+d>0 \end{array}\right.$ *si et seulement s'il existe* $l\in\mathbb{Z}$ *tel que*

$$\left\{\begin{array}{ll} \left\{\begin{array}{l} ap_N+bq_N=A_{M+kl} \\ cp_N+dq_N=B_{M+kl} \end{array}\right. \textit{ et } \left\{\begin{array}{l} ap_{N-1}+bq_{N-1}=A_{M+kl-1} \\ cp_{N-1}+dq_{N-1}=B_{M+kl-1} \end{array}\right. & \textit{si } l\geq 0 \\ \\ \left\{\begin{array}{l} ap_{N-kl}+bq_{N-kl}=A_M \\ cp_{N-kl}+dq_{N-kl}=B_M \end{array}\right. \textit{ et } \left\{\begin{array}{l} ap_{N-kl-1}+bq_{N-kl-1}=A_{M-1} \\ cp_{N-kl-1}+dq_{N-kl-1}=B_{M-1} \end{array}\right. & \textit{si } l<0 \end{array}\right. .$$

On démontre le Théorème 6 comme le Théorème 4, mais en faisant attention à la période. On peut se représenter qu'on a une infinité de matrices qui envoient x sur y par le fait qu'il y a une infinité de façons de choisir les deux parties précédant la queue. Chaque décalage possible, chaque valeur de l, correspond à une matrice qui envoie x sur y.

L'analogue du Théorème 5 est:

Théorème 7 *Soient* x, y *sont deux irrationnels quadratiques ayant même queue:* $x=[a_0;a_1,a_2,...,a_N,\overline{c_0,c_1,...,c_{k-1}}]$ *et* $y=[b_0;b_1,b_2,...,b_M,\overline{c_0,c_1,...,c_{k-1}}]$ *(où* $N,M,k\geq 1$*).*

Les nombres x *et* y *appartiennent à la même orbite de* $\Gamma(n)$ *si et seulement s' il existe* $l\in\mathbb{Z}$ *tel que*

- *si* $l\geq 0$

$$p_N\equiv A_{M+kl},\ p_{N-1}\equiv A_{M+kl-1},\ q_N\equiv B_{M+kl},\ q_{N-1}\equiv B_{M+kl-1}\pmod n$$

  ou

$$p_N\equiv -A_{M+kl},\ p_{N-1}\equiv -A_{M+kl-1},\ q_N\equiv -B_{M+kl},\ q_{N-1}\equiv -B_{M+kl-1}\pmod n.$$

- *si* $l<0$

$$p_{N-kl}\equiv A_M,\ p_{N-kl-1}\equiv A_{M-1},\ q_{N-kl}\equiv B_M,\ q_{N-kl-1}\equiv B_{M-1}\pmod n$$

  ou

$$p_{N-kl}\equiv -A_M,\ p_{N-kl-1}\equiv -A_{M-1},\ q_{N-kl}\equiv -B_M,\ q_{N-kl-1}\equiv -B_{M-1}\pmod n.$$

La démonstration du Théorème 7 est analogue à celle du Théorème 5, en utilisant le Théorème 6 en lieu et place du Théorème 4.

A Fractions continues et équivalence sous $GL_2(\mathbb{Z})$, *par Alain VALETTE*

Nous nous intéressons dans cet Appendice au résultat suivant:

Théorème 8 *: Soient x, y deux irrationnels. Les nombres x et y ont la même queue si et seulement s'ils sont dans la même orbite de $GL_2(\mathbb{Z})$ agissant par homographies sur $\mathbb{R} \cup \{\infty\}$.*

Ce résultat a été obtenu par J.A. Serret en 1878 (voir le Théorème 23 du Chapitre 2 dans [Per13]). Plus récemment, ce résultat a inspiré des travaux de dynamique symbolique, par exemple [BS79], [Ser85]. L'implication directe dans le Théorème 8 n'est pas très difficile; nous verrons qu'elle résulte des formules qui lient x et ses quotients complets

$$x_n = [a_n; a_{n+1} a_{n+2} \ldots];$$

en effet, on a $x = \frac{A_{n-1}x_n + A_{n-2}}{B_{n-1}x_n + B_{n-2}}$ où $\frac{A_k}{B_k} = [a_0; a_1 \ldots a_k]$ est la k-ème réduite de x, et $\begin{pmatrix} A_{n-1} & A_{n-2} \\ B_{n-1} & B_{n-2} \end{pmatrix} \in GL_2(\mathbb{Z})$ (voir [Per13], formules 11 et 30 du Chapitre 1). Pour la réciproque, nous connaissons deux preuves classiques:

- l'une consiste à se ramener au lemme suivant (voir [Per13], Théorème 13 du Chapitre 2; [HW75], Théorème 172): si $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$, avec $c > d > 0$, si $y > 1$, et si $x = \frac{ay+b}{cy+d}$, alors $\frac{a}{c}$ et $\frac{b}{d}$ sont deux réduites consécutives de x; de plus, si $\frac{a}{c}$ est la $(n-1)$-ème réduite et $\frac{b}{d}$ la n-ème, alors y est le $(n+1)$-ème quotient complet de x;
- si $x = \frac{ay+b}{cy+d}$, avec $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{Z})$, on peut montrer comme au Théorème IV du Chapitre I de [Cas57], que les images par la même homographie de deux réduites consécutives de y, de rang assez grand, sont deux meilleures approximations rationnelles consécutives de x, donc fournissent des réduites (pas nécessairement de même rang) de x. On en déduit aisément que x et y ont même queue.

Notre but ici est d'attirer l'attention sur une autre façon de démontrer le Théorème 8. Au vu de la littérature considérable sur les fractions continues (voir le Chapitre A de [LeV74]), il serait téméraire de notre part d'affirmer que cette preuve est originale! Nous commençons avec la formule suivante, qui se trouve à la page 65 du livre de 0. Perron [Per13]:

Proposition 9 *: Soit* $x = [a_0; a_1, a_2, \ldots]$ *un irrationnel. Alors*

$$-x = \begin{cases} [-(a_0+1); 1, a_1 - 1, a_2, a_3, \ldots] & si\ a_1 > 1 \\ [-(a_0+1); a_2+1, a_3, a_4 \ldots] & si\ a_1 = 1. \end{cases}$$

La preuve de la Proposition 9 est une vérification immédiate.

Proposition 10 *: Soit* $x = [a_0; a_1, a_2, \ldots]$ *un irrationnel. Alors:*

$$-\frac{1}{x} = \begin{cases} [1; a_1 - 1, a_2, a_3, \ldots] & si\ -1 < x < 0 & et\ a_1 > 1; \\ [a_2+1; a_3, a_4, \ldots] & si\ -1 < x < 0 & et\ a_1 = 1; \\ [0; -(a_0+1), 1, a_1 - 1, a_2, \ldots] & si\ x < -1 & et\ a_1 > 1; \\ [0; -(a_0+1), a_2+1, a_3, a_4, \ldots] & si\ x < -1 & et\ a_1 = 1; \\ [-(a_1+1); 1, a_2 - 1, a_3, a_4, \ldots] & si\ 0 < x < 1 & et\ a_2 > 1; \\ [-(a_1+1); a_3+1, a_4, a_5, \ldots] & si\ 0 < x < 1 & et\ a_2 = 1; \\ [-1; 1, a_0 - 1, a_1, a_2, \ldots] & si\ x > 1 & et\ a_0 > 1; \\ [-1; a_1+1, a_2, a_3, \ldots] & si\ x > 1 & et\ a_0 = 1. \end{cases}$$

Preuve: Pour $x > 0$, on a

$$\frac{1}{x} = \begin{cases} [0; a_0, a_1.a_2, \ldots] & si\ x > 1; \\ [a_1; a_2, a_3, \ldots] & si\ 0 < x < 1. \end{cases}$$

Si $x < 0$, on calcule $-\frac{1}{x} = \frac{1}{(-x)}$ en appliquant d'abord la formule de la Proposition 9, puis la formule ci-dessus. Si $x > 0$, on calcule $-\frac{1}{x} = -(\frac{1}{x})$ en appliquant ces formules dans l'ordre inverse. $\square$

Preuve du Théorème 8: Si $x = [a_0; a_1, a_2, \ldots]$ et $x_1 = [a_1; a_2, a_3, \ldots]$, alors $\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \cdot (x_1) = x$. Ainsi x est dans la même orbite sous $GL_2(\mathbb{Z})$ que tous ses quotients complets. Donc, si x et y ont la même queue, c-à-d. si x et y ont un quotient complet en commun, x et y sont dans la même orbite sous $GL_2(\mathbb{Z})$. Pour la réciproque, nous utiliserons le fait bien connu (voir [Ser70], Théorème 2 du Chapitre VII) que le groupe $SL_2(\mathbb{Z})$ est engendré par les matrices $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ et $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Donc $GL_2(\mathbb{Z})$ est engendré par les matrices S, T et $P = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, puisque $[GL_2(\mathbb{Z}) : SL_2(\mathbb{Z})] = 2$ et $P \notin SL_2(\mathbb{Z})$. Les homographies associées sont $\alpha_S(x) = -\frac{1}{x}$, $\alpha_T(x) = x + 1$, $\alpha_P(x) = -x$. Il résulte des Propositions 9 et 10 que $\alpha_P(x)$ et $\alpha_S(x)$ ont la même queue que x; c'est d'autre part clair pour $\alpha_T(x)$. Si $A \in GL_2(\mathbb{Z})$, en écrivant A comme un mot sur l'alphabet $\{S, T^{\pm 1}, P\}$, on voit que $\alpha_A(x)$ a la même queue que x. $\square$

Corollaire 11 *:*

Deux irrationnels $x = [a_0; a_1, a_2, \ldots]$ *et* $y = [b_0; b_1, b_2, \ldots]$ *sont dans la même orbite sous* $SL_2(\mathbb{Z})$ *si et seulement si* $x = [a_0; a_1, a_2, \ldots, a_m, c_1, c_2, c_3, \ldots]$ *et* $y = [b_0; b_1, b_2, \ldots, b_n, c_1, c_2, c_3, \ldots]$, *où* m *et* n *ont la même parité.*

Preuve: $\Longleftarrow$): L'homographie associée à $\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}$, qui fait passer de x au premier quotient complet $x_1 = [a_1; a_2, a_3, \ldots]$, est de déterminant -1; donc il y a une homographie de $GL_2(\mathbb{Z})$, de déterminant $(-1)^{m+1}$, qui fait passer de x à $[c_1; c_2, c_3, \ldots]$. De même, il y a une homographie de $GL_2(\mathbb{Z})$, de déterminant $(-1)^{n+1}$, qui fait passer de y à $[c_1; c_2, c_3, \ldots]$. Il y a donc une homographie de $GL_2(\mathbb{Z})$, de déterminant $(-1)^{m+n+2} = 1$, qui fait passer de x à y.

$\Longrightarrow$): La Proposition 10 montre que $-\frac{1}{x}$ a la même queue que x, avec un décalage de -2, 0 ou 2. Comme $SL_2(\mathbb{Z})$ est engendré par les matrices S et T, on voit que tout élément de $SL_2(\mathbb{Z})$ décale la queue de x d'un nombre pair. $\square$

References

[BS79] R. Bowen and C. Series. Markov maps associated with Fuchsian groups. *Publ. Math. I.H.E.S.*, 50:153–170, 1979.

[Cas57] J.W.S. Cassels. *An introduction to Diophantine approximation.* Cambridge Univ. Press, 1957.

[HW75] G.H. Hardy and E.M. Wright. *An introduction to the theory of numbers (corrected 4th edition).* Oxford Clarendon Press, 1975.

[LeV74] W.J. LeVeque. *Reviews in number theory.* Amer. Math. Soc., 1974.

[Per13] O. Perron. *Die Lehre von den Kettenbrüchen.* Teubner, 1913.

[Ser85] C. Series. The modular surface and continued fractions. *J. London Math. Soc.*, 31:69–80, 1985.

[Ser70] J.-P. Serre. *Cours d'arithmétique.* Presses Univ. France, 1970.

Adresse des auteurs:

Recogne, Sur le Chêne 58
B-6800 Libramont - BELGIQUE
ctroessa@ulb.ac.be

Institut de Mathématiques - Université de Neuchâtel
Rue Emile Argand 11
CH-2007 Neuchâtel - SUISSE
alain.valette@unine.ch