2. Seit Abel (J. Reine Angew. Math. 1 (1826), S. 185–221) ist bekannt, daß mit der Lösbarkeit der Pellschen Gleichung (5) in Polynomen $p(z)$, $q(z)$ äquivalent die logarithmische Integrierbarkeit gewisser algebraischer Differentiale ist. Zur expliziten Lösung dieses Problems sind soeben von J. H. Davenport („On the integration of algebraic functions", Lecture Notes in Computer Science Nr. 102, Springer: Berlin–Heidelberg–New York 1981) zum Einsatz in Computern geeignete Algorithmen angegeben worden. Damit kann man also nun auch die Frage nach der Existenz von z-Einheiten im Falle $w^2 = D(z)$ mit grad $D \geqslant 4$ entscheiden (vgl. Abschnitt 6. dieser Arbeit).

Literatur

[1] L. Bernstein und H. Hasse, *Ein formales Verfahren zur Herstellung parameterabhängiger Scharen quadratischer Grundeinheiten*, J. Reine Angew. Math. 276 (1975), S. 206–212.

[2] G. Degert, *Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg 22 (1958), S. 92–97.

[3] Ch. Denenberg, *Periodic expansions and units in quadratic and cubic number fields*, J. Reine Angew. Math. 278/279 (1975), S. 266–277.

[4] L. Euler, *De usu novi algorithmi in problemate Pelliano solvendo*, Werke, ser. I, vol. 3 (1765).

[5] B. Mazur, *Rational points on modular curves*, in: Serre and Zagier (Ed.), *Modular functions of one variable. V*. Proceedings Int. Conf. Bonn 1976. Lecture Notes in Math. 601 (1977).

[6] M. B. Nathanson, *Polynomial Pell's equation*, Proc. Amer. Math. Soc. 56 (1976), S. 89–92.

[7] M. Neubrand, *Einheiten in algebraischen Funktionen- und Zahlkörpern*, J. Reine Angew. Math. 303/304 (1978), S. 170–204.

[8] H. U. Nordhoff, *Explizite Darstellung von Einheiten und ihre Anwendung auf Mehrklassigkeitsfragen bei reell-quadratischen Zahlkörpern. I*, ibid. 268/269 (1974), S. 131–149.

[9] A. Schinzel, *On some problems of the arithmetical theory of continued fractions*, Acta Arith. 6 (1961), S. 393–413.

[10] –, –. *II*, ibid. 7 (1962), S. 287–298.

[11] Herm. Schmidt, *Zur Approximation und Kettenbruchentwicklung quadratischer Zahlen*, Math. Z. 52 (1948), S. 168–192.

[12] – *Über einheitliche Kettenbruchentwicklungen für die Quadratwurzel aus einem Polynom in einer ganzzahligen Variablen*, Manuskript 1975.

SEMINAR FÜR DIDAKTIK DER MATHEMATIK
DER UNIVERSITÄT, Bonn

Eingegangen am 17.4.1978
und in reviedierter Form am 30.8.1978 (1064)

ACTA ARITHMETICA
XXXIX (1981)

Propriétés arithmétiques de séries rationnelles et ensembles denses

par

C. Reutenauer (Paris)

1. Introduction. Une *série rationnelle* (cf. G. Pólya 10]) est le développement en série de Taylor d'une fraction rationnelle régulière à l'origine. De nombreuses propriétés de la fraction rationnelle se déduisent de propriétés arithmétiques des coefficients de la série associée. Il en est ainsi du lemme de Fatou: si les coefficients de la série sont entiers alors la fraction rationnelle est un quotient P/Q de deux polynômes premiers entr'eux à coefficients entiers avec $Q(0) = 1$.

G. Rauzy a montré que la même conclusion subsiste avec une hypothèse plus faible: il suffit de supposer que l'ensemble des coefficients qui sont entiers rencontre toute progression arithmétique [12]. Un tel ensemble est appelé arithmétiquement dense par Rauzy; dans d'autres problèmes des ensembles de cette nature on été considérés (voir par exemple Lewis, Davenport et Schinzel [15]). Un tel ensemble est dense pour la topologie sur $\boldsymbol{N}$ qui rend continues les injections $\boldsymbol{N} \to \boldsymbol{Z}_p$. Une fonction continue qui s'annule sur un ensemble dense est donc nulle. Parallèlement, on déduit d'un théorème de Skolem (voir [9]) que si les coefficients d'une série sont nuls sur un ensemble dense, cette série se réduit à un polynôme.

Dans cet article, nous étudions des propriétés arithmétiques des séries rationnelles en plusieurs variables non commutatives (cf. S. Eilenberg [3]). Remarquons que si $\sum a_n t^n$ est une série rationnelle, le coefficient a_n est égal à une combinaison linéaire fixe des coefficients de la puissance $n$ème d'une matrice fixe; la matrice en question n'est autre que la matrice compagnon de la relation de récurrence vérifiée par la suite (a_n). Ainsi est on amené à généraliser la notion de séries rationnelles (définition 1). On se donne un nombre fini $A_1, \ldots, A_r$ de matrices carrées et l'on étudie une combinaison linéaire fixée des coefficients des matrices éléments du semigroupe engendré par les $A_1, \ldots A_r$; si $t_1, \ldots, t_r$ désignent des variables non commutatives, on obtient ainsi une série formelle en les t_i: le coefficient de $t_{i_1} t_{i_2} \ldots t_{i_k}$ est combinaison linéaire des coefficients de $A_{i_1} A_{i_2} \ldots A_{i_k}$. Les séries obtenus de cette façon seront appelées les séries rationnelles; M. P. Schützenberger a montré (voir par exemple S. Eilenberg [3], th. 5.1,

du chap. VII) que les séries rationnelles sont exactement les séries qui appartiennent à la sous-algèbre des séries formelles qui est fermée par passage à l'inverse et qui contient les polynômes: ainsi se retrouve le lien avec les séries rationnelles d'une variable, considérées comme quotient de deux polynômes.

Nous montrons ici que la généralisation par Rauzy du lemme de Fatou reste vraie pour les séries rationnelles en plusieurs variables non commutatives (théorème 1). Ce résultat résulte essentiellement d'une proposition sur les semi-groupes de matrices: nous caractérisons les semi-groupes $\subset \mathscr{M}_n(Q)$ qui sont semblables à des semi-groupes $\subset \mathscr{M}_n(Z)$ (proposition 1). Nous généralisons ensuite un résultat de Lamèche–Jacob ([8], [6]) qui étend un théorème de Pólya [10] sur l'intégrale d'une série rationnelle. (Théorème 2.) Au dernier paragraphe, nous étudions l'image d'une série rationnelle (l'ensemble de ses coefficients) et montrons, par exemple, qu'une telle série est un polynôme dès que ses coefficients sont nuls sur un ensemble dense.

2. Définitions. Soit X un ensemble fini, X^* le monoïde libre engendré par X: son élément neutre est noté 1.

Une série formelle S sur X à coefficients dans Q est une application $X^* \to Q$. On la note: $S = \sum_{w \in X^*} S(w)w$; $S(w)$ est le *coefficient* de w, et l'ensemble $\{S(w) \mid w \in X^*\}$ est *l'image de* S. Un *polynôme* est une série formelle de support fini, i.e. $S(w)$ est nul pour presque tout $w \in X^*$. Nous notons $Q\langle\langle X\rangle\rangle$ l'ensemble des séries formelles et $Q\langle X\rangle$ l'ensemble des polynômes.

Définition 1. (i) Soit S une série formelle. S est dite *rationnelle* s'il existe un entier $r \geqslant 1$, un homomorphisme $\mu: X^* \to \mathscr{M}_r(Q)$, deux matrices $\lambda \in \mathscr{M}_{1,r}(Q)$ et $\gamma \in \mathscr{M}_{r,1}(Q)$ tels que: $\forall w \in X^*$, $S(w) = \lambda\mu w\gamma$.

(ii) Dans les hypothèses précédentes, S est dite *Z-rationnelle* si de plus λ, μ et γ sont à coefficients entiers.

En particulier, une série Z-rationnelle a tous ses coefficients entiers. Réciproquement une série rationnelle à coefficients dans Z est Z-rationnelle ([16] ou [4]).

Remarque. $Q\langle\langle X\rangle\rangle$ est muni canoniquement d'une structure de Q-algèbre, qui prolonge la structure multiplicative de X^*. Schützenberger a montré (cf. S. Eilenberg [3]) que les séries rationnelles sont exactement les séries appartenant à la petite sous-algèbre de $Q\langle\langle X\rangle\rangle$ qui est stable par passage à l'inverse et qui contient les polynômes.

Pour une variable, on retrouve donc la notion de série de Taylor d'une fraction rationnelle régulière à l'origine.

Sous les hypothèses de la définition 1, nous dirons que (λ, μ, γ) est une *représentation* de S. Les représentations de S où $r = \dim(\mu)$ est minimum seront appelées ses *représentations minimales*.

Schützenberger a montré que *deux représentations minimales d'une série rationnelle sont conjuguées*, et que *si tous les coefficients de la série sont entiers, alors elle est Z-rationnelle et admet une représentation minimale à coefficients entiers* ([16], III. B. 1 voir aussi M. Fliess [4], th. 2.1.2).

Si $v \in X^*$, nous noterons v^* l'ensemble $\{v^n \mid n \in N\}$.

Définition 2. (i) Un *rayon* est une partie de X^* de la forme uv^*w avec $u, v, w \in X^*$, $v \neq 1$.

(ii) $A \subset X^*$ est *dense* dans X^* si A rencontre tout rayon.

Remarquons que si $\mathrm{Card}(X) = 1$, X^* est isomorphe à N et les rayons coïncident avec les progressions arithmétiques. De plus, dans ce cas, les ensembles denses sont exactement les ensembles denses dans N pour la topologie borne supérieure des topologies p-adiques.

Cette topologie s'étend de manière naturelle au monoïde libre X^*: c'est la topologie obtenue par restriction de la topologie des sous-groupes d'indice fini sur le groupe libre engendré par X (cf. M. Hall [5]); nous étudions cette topologie dans [14]. Cependant, si $\mathrm{Card}(X) \geqslant 2$, il n'y a pas identité entre les ensembles denses pour cette topologie et les ensembles denses au sens de la définition 2.

Le résultat suivant est immédiat.

Lemme 1. *Soit A dense dans X^* et uv^*w un rayon. L'ensemble $\{n \in N \mid uv^nw \in A\}$ est dense dans N.*

3. Sur un lemme de Fatou. G. Rauzy a généralisé le lemme de Fatou (cité dans l'introduction) de la manière suivante:

Théorème (Rauzy [12]). *Soit $\sum_{n \geqslant 0} a_n t^n$ le développement en série de la fraction P/Q, où P et Q sont deux polynômes $\in Q[t]$ premiers entr'eux, Q étant à coefficients entiers premiers entr'eux avec $Q(0) \geqslant 1$. Soit A dense dans N. Si $\forall n \in A$, $a_n \in Z$, alors $Q(0) = 1$.*

Le résultat que nous voulons démontrer est l'analogue de ce théorème pour les séries en plusieurs variables non commutatives; nous obtenons aussi que pour presque tout $w \in X^*$, le coefficient de w est entier.

Théorème 1. *Soit S une série rationnelle et A dense dans X^*. On suppose: $\forall w \in A$, $S(w) \in Z$.*

(i) *S admet une représentation minimale (λ, μ, γ) où μ est à coefficients entiers.*

(ii) *Pour presque tout $w \in X^*$, $S(w)$ est entier et il existe une série Z-rationnelle S_1 et un polynôme P tels que: $S = S_1 + P$.*

Pour démontrer ce résultat, nous avons besoin de deux lemmes et d'un résultat sur les semi-groupes de matrices.

Le premier lemme découle du théorème de Rauzy.

LEMME 2 (Hypothèses du théorème de Rauzy).

(i) *Il existe des entiers* $p \geqslant 1$, $r_1, \dots, r_p$ *tels que*

$$\forall n \geqslant 0, \quad a_{n+p} = r_1 a_{n+p-1} + r_2 a_{n+p-2} + \dots + r_p a_n.$$

(ii) *Il existe des matrices* $M \in \mathscr{M}_p(Z)$, $\lambda \in \mathscr{M}_{1,p}(Q)$, $\gamma \in \mathscr{M}_{p,1}(Q)$ *tels que*

$$\forall n \geqslant 0, \quad a_n = \lambda M^n \gamma.$$

Preuve. (i) On considère la relation de récurrence linéaire associée au polynôme réciproque de Q. (ii) On prend pour M la matrice compagnon de la relation de récurrence linéaire. ■

Le second lemme est combinatoire.

LEMME 3. *Soit* T *une série* $\boldsymbol{Z}$*-rationnelle,* d *un entier* $\geqslant 1$ *et* a *un entier. Si l'ensemble* $\{w \in X^* \mid T(w) \equiv a \bmod d\}$ *est infini, il contient un rayon.*

Preuve. Soit p la projection canonique $\boldsymbol{Z} \to \boldsymbol{Z}/d\boldsymbol{Z}$; nous noterons encore p la projection canonique $\mathscr{M}_{a,b}(\boldsymbol{Z}) \to \mathscr{M}_{a,b}(\boldsymbol{Z}/d\boldsymbol{Z})$. Soit $\bar{\mu} = p \circ \mu$, $\bar{\lambda} = p(\lambda)$, $\bar{\gamma} = p(\gamma)$ et $\bar{a} = p(a)$. On a:

$$T(w) \equiv a \bmod d \Leftrightarrow \bar{\lambda}\bar{\mu}w\bar{\gamma} = \bar{a}.$$

Si l'ensemble $\{w \mid T(w) \equiv a \bmod d\}$ est infini, il existe $w = x_1 x_2 \dots x_s$ dans cet ensemble avec $s > \operatorname{Card}(\mathscr{M}_r(\boldsymbol{Z}/d\boldsymbol{Z}))$ et $x_i \in X, \forall i$. Par suite, deux éléments de la suite $\bar{\mu}x_1, \bar{\mu}x_1x_2, \dots, \bar{\mu}x_1 \dots x_s$ sont égaux et il s'en déduit que w peut s'écrire

$$w = w_1 w_2 w_3 \quad \text{avec} \quad \bar{\mu}w_1 = \bar{\mu}w_1 w_2, \quad w_2 \neq 1.$$

Donc: $\forall n \in \boldsymbol{N}$, $\bar{\mu}w_1 w_2^n = \bar{\mu}w_1 = \bar{\mu}w_1 w_2$ et: $\bar{\lambda}\bar{\mu}w_1 w_2^n w_3 \bar{\gamma} = \bar{a}$. Par suite: $T(w_1 w_2^n w_3) \equiv a \bmod d$. ■

Le résultat suivant, sur lequel repose la preuve du théorème 1, caractérisé les semi-groupes de type fini $\subset \mathscr{M}_r(Q)$ qui sont semblables à un semi-groupe $\subset \mathscr{M}_r(\boldsymbol{Z})$.

PROPOSITION 1. *Soit* S *un sous-semi-groupe de type fini de* $\mathscr{M}_r(Q)$. *Les conditions suivantes sont équivalentes.*

(i) *Toutes les valeurs propres des matrices de* S *sont des entiers algébriques.*

(ii) S *est semblable à un sous-semi-groupe de* $\mathscr{M}_r(\boldsymbol{Z})$, *i.e. il existe* $P \in \mathrm{GL}_r(Q)$ *tel que* $P^{-1}SP \subset \mathscr{M}_r(\boldsymbol{Z})$.

(Cette proposition s'étend aux anneaux principaux, comme le montrera la preuve.)

Preuve. L'implication (ii) ⇒ (i) est claire.

Pour (i) ⇒ (ii) on peut supposer que S contient la matrice identité.

1. Montrons qu'il existe $d \in \boldsymbol{N}^*$ tel que $dS \subset \mathscr{M}_r(\boldsymbol{Z})$.

(a) Nous nous plaçons d'abord dans le cas où S est irréductible, i.e. il n'existe aucun sous-espace de $\boldsymbol{Q}^r$ stable sous tous les endomorphismes définis par S. La Q-algèbre $\mathfrak{M}$ engendrée par S est donc aussi irréductible, et par suite, d'après [2] (exercice 1 du § 2) la forme bilinéaire sur $\mathfrak{M}$: $(M', M'') \mapsto \operatorname{Tr}(M'M'')$ est non dégénérée. Par hypothèse: $\forall M \in S, \operatorname{Tr}(M) \in \boldsymbol{Z}$.

Comme S est un semi-groupe, l'algèbre engendrée par S est égale à l'espace vectoriel engendré par S et il existe $M_1, \dots, M_s \in S$ formant une base de $\mathfrak{M}$. Si $M \in S$, on a:

$$M = \sum_{1 \leqslant i \leqslant s} x_i M_i, \quad x_i \in \boldsymbol{Q}.$$

Par suite:

$$\forall j, 1 \leqslant j \leqslant s: \quad \operatorname{Tr}(MM_j) = \sum_{1 \leqslant i \leqslant s} x_i \operatorname{Tr}(M_i M_j).$$

On obtient ainsi un système de Cramer (puisque, la forme bilinéaire $\operatorname{Tr}(\cdot)$ étant non dégénérée, le déterminant $d' = |\operatorname{Tr}(M_i M_j)|$, $1 \leqslant i, j \leqslant s$, est $\neq 0$) en les x_i. Comme $\operatorname{Tr}(MM_j) \in \boldsymbol{Z}$, on a: $\forall i, d'x_i \in \boldsymbol{Z}$.

Soit d'' un dénominateur commun aux M_i et $d = d'd''$.

Alors: $dM = d'x_i \cdot d''M_i \in \mathscr{M}_r(\boldsymbol{Z})$.

(b) Si S n'est pas irréductible, on se ramène par changement de base au cas où S s'écrit:

$$S = \begin{pmatrix} S_1 & T \\ 0 & S_2 \end{pmatrix}$$

où S_1 est irréductible et $r_2 = \dim(S_2) < r = \dim(S)$.

Par récurrence sur r, il existe $d_2 \in \boldsymbol{N}^*$ tel que $d_2 \cdot S_2 \subset \mathscr{M}_{r_2}(\boldsymbol{Z})$, et d'après (a), il existe $d_1 \in \boldsymbol{N}^*$ tel que: $d_1 \cdot S_1 \subset \mathscr{M}_{r_1}(\boldsymbol{Z})$.

S est un semi-groupe de type fini, donc il existe des matrices $M^1, \dots, M^t \in S$ telles que tout $M \in S$ s'écrive: $M = \prod_{1 \leqslant i \leqslant k} M^{j_i}$. Posons:

$$M^j = \begin{pmatrix} M_1^j & T^j \\ 0 & M_2^j \end{pmatrix}, \quad 1 \leqslant j \leqslant t.$$

Soit d un dénominateur commun aux T^j et $d = d'd_1d_2$. Alors:

$$dM = d \begin{pmatrix} \prod_i M_1^{j_i} & \sum_i M_1^{j_1} \dots M_1^{j_{i-1}} T^{j_i} M_2^{j_{i+1}} \dots M_2^{j_k} \\ 0 & \prod_i M_2^{j_i} \end{pmatrix},$$

$$dM = \begin{pmatrix} (d'd_2)d_1N_1 & \sum_i (d_1N_1^i)(d'T^{j_i})(d_2N_2^i) \\ 0 & (d'd_1)d_2N_2 \end{pmatrix}$$

avec $N_1, N_1^i \in S_1$, $N_2, N_2^i \in S_2$ donc $dM \in \mathscr{M}_r(\boldsymbol{Z})$.

2. Il existe donc $d \in \boldsymbol{N}^*$ tel que $d \cdot S \subset \mathscr{M}_r(\boldsymbol{Z})$. Soit V le sous-$\boldsymbol{Z}$-module de $\boldsymbol{Q}^r$ engendré par les vecteurs $M \cdot v$, $M \in S$, $v \in \boldsymbol{Z}^r$. On a: $d(M \cdot v) = (dM) \cdot v \in \boldsymbol{Z}^r$.

Donc $V \subset d^{-1} \cdot \mathbf{Z}^r$ est un $\mathbf{Z}$-module libre, de rang r puisqu'il contient $\mathbf{Z}^r$. Il existe donc une base de $\mathbf{Q}^r$ qui est une base du $\mathbf{Z}$-module V. Par ailleurs, V est stable sous S; donc, écrivant S dans cette base, on voit que S est semblable à un sous-semi-groupe de $\mathscr{M}_r(\mathbf{Z})$. ■

Preuve du théorème 1. (i) D'après M. Fliess [4] (th. 2.1.1), il existe une représentation minimale $(\lambda_1, \mu_1, \gamma_1)$ de S, où μ_1 est de dimension r, des éléments u_i, v_j de X^*, $1 \leqslant i, j \leqslant r$, des matrices $m_{i,j} \in \mathscr{M}_r(\mathbf{Q})$ telles que:

$$\forall w \in X^*, \quad \mu_1 w = \sum_{i,j} m_{i,j} S(u_i w v_j).$$

Soit $w \in X^*$ et $T_{i,j}$ la série formelle de la variable t:

$$T_{i,j} = \sum_{n \geqslant 0} S(u_i w^n v_j) t^n = \sum_{n \geqslant 0} T_{i,j}(n) t^n.$$

$T_{i,j}$ est rationnelle car: $a_n = \lambda_1 \mu_1 u_i (\mu_1 w)^n \mu_1 v_j \gamma_1$. Soit $a\mathbf{N} + b$ une progression arithmétique dans $\mathbf{N}$ $(a \geqslant 1)$; alors $u_i w^b (w^a)^* v_j$ est un rayon et par suite rencontre A. Il existe donc $n \in \mathbf{N}$ tel que: $S(u_i w^{an+b} v_j) = T_{i,j}(an + b) \in \mathbf{Z}$.

Donc l'ensemble des m tels que $T_{i,j}(m) \in \mathbf{Z}$ est dense dans $\mathbf{N}$, et d'après le lemme 2 la suite $(T_{ij}(n))$ vérifie une relation de récurrence linéaire à coefficients entiers. Il existe donc une relation de récurrence linéaire à coefficients entiers comme à toutes les suites $T_{i,j}(n)$, $1 \leqslant i, j \leqslant r$: $\forall i, j, \forall n \geqslant 0$,

$$T_{i,j}(n+q) = a_1 T_{i,j}(n+q-1) + a_2 T_{i,j}(n+q-2) + \ldots + a_q T_{i,j}(n).$$

Par suite:

$$\mu_1 w^{n+q} = \sum_{i,j} m_{i,j} T_{i,j}(n+q) = \sum_{i,j} m_{i,j} \sum_{k=1} a_k T_{i,j}(n+q-k)$$
$$= \sum_{k=1} a_k \sum_{i,j} m_{i,j} T_{i,j}(n+q-k) = \sum_{k=1} a_k \mu_1 w^{n+q-k}.$$

Donc les valeurs propres de $\mu_1 w$ sont des entiers algébriques. Par suite, d'après la proposition 1, il existe $P \in \mathrm{GL}_r(\mathbf{Q})$ tel que: $P^{-1} \mu_1 X^* P \subset \mathscr{M}_r(\mathbf{Z})$. Soit $\mu: X^* \to \mathscr{M}_r(\mathbf{Z})$ défini par: $\mu w = P^{-1} \mu_1 w P$, et $\lambda = \lambda_1 P$, $\gamma = P^{-1} \gamma_1$. Alors: $\forall w \in X^*$, $\lambda \mu w \gamma = \lambda_1 P P^{-1} \mu_1 w P P^{-1} \gamma_1 = S(w)$, donc (λ, μ, γ) est une représentation de S et μ est à coefficients entiers.

(ii) Soit d' un dénominateur commun aux matrices λ, γ et $d = d'^2$. Alors la série T dont une représentation est $(d'\lambda, \mu, d'\gamma)$ est $\mathbf{Z}$-rationnelle et vérifie: $\forall w \in X^*$, $T(w) = d \cdot S(w)$. L'ensemble des w tels que d divise $T(w)$ contient A, par hypothèse. Par suite, aucun des ensembles $\{w \in X^* \mid T(w) \equiv a \bmod d\}$ $(a = 1, \ldots, d-1)$ ne contient de rayon, donc ces ensembles sont finis (lemme 3). Par suite, pour presque tout w, d divise $T(w)$, i.e. $S(w)$ est entier.

Soit

$$S_1 = \sum_{\substack{w \in X^* \\ S(w) \in \mathbf{Z}}} S(w) w \quad \text{et} \quad P = \sum_{\substack{w \in X^* \\ S(w) \notin \mathbf{Z}}} S(w) w.$$

P est un polynôme, et d'après les remarques qui suivent la définition 1, S_1 est une série $\mathbf{Z}$-rationnelle.

Le théorème 1 est donc démontré. ■

4. Sur un théorème de Pólya. Soit $\sum a_n t^n$ la série de Taylor d'une fraction rationnelle régulière à l'origine. G. Pólya a montré [10] que si $a_n \in (n+1)\mathbf{Z}$ alors la série $\sum (a_n/n+1) t^n$ est encore rationnelle. K. Lamèche et G. Jacob ont étendu ce résultat de la manière suivante ($|w|$ désigne la *longueur* de $w \in X^*$): si $w = x_{i_1} x_{i_2} \ldots x_{i_k}$ avec $x_{i_j} \in X$, alors $|w| = k$:

Théorème (Lamèche [8], Jacob [6]). *Soit S une série rationnelle. Si pour tout $w \in X^*$, $S(w) \in (|w|+1)\mathbf{Z}$, alors la série*

$$\sum_w \frac{S(w)}{|w|+1} w$$

est rationnelle.

Le résultat que nous nous proposons de démontrer est le

Théorème 2. *Soit S une série rationnelle et A dense dans X^*. Si pour tout $w \in A$, $S(w) \in (|w|+1)\mathbf{Z}$ alors la série*

$$\sum_w \frac{S(w)}{|w|+1} w$$

est rationnelle.

Nous avons besoin d'un résultat intermédiaire.

Proposition 2. *Soit S une série rationnelle et Q un ensemble fini de nombre premiers tel que les facteurs premiers du dénominateur des fractions réduites $S(w)/(|w|+1)$ soient tous dans Q. Alors la série*

$$\sum_w \frac{S(w)}{|w|+1} w$$

est rationnelle.

Avant de démontrer cette proposition, énonçons un lemme, dont la preuve s'obtient en considérant la représentation d'une série rationnelle.

Lemme 4. *Soit S une série formelle et $a, b \in \mathbf{N}^*$.*

(i) *S est rationnelle si et seulement si la série $\sum_w a b^{|w|} S(w) w$ est rationnelle.*

(ii) (Propriété d'Eisenstein) *Si S est rationnelle, il existe $a, b \in \mathbf{N}^*$ tels que $\sum_w a b^{|w|} S(w) w$ soit $\mathbf{Z}$-rationnelle.*

Preuve de la proposition 2. En vertu du lemme 4, on peut supposer que S est $\boldsymbol{Z}$-rationnelle, donc que $S(w) \in \boldsymbol{Z}$. Soit $d = \prod_{p \in Q} p$ et $T = \sum_w d^{|w|} S(w) w$.

T est rationnelle; soit p un nombre premier et v_p la valuation p-adique. On a: $\forall n \in \boldsymbol{N}$, $v_p(n+1) \leqslant n$. Par suite:

(i) Si $p \in Q$ on a:

$$v_p[T(w)/(|w|+1)] = v_p\big(S(w)\big) + |w| - v_p(w+1) \geqslant 0.$$

(ii) Si $p \notin Q$, par hypothèse:

$$v_p[T(w)/(|w|+1)] \geqslant 0.$$

Par suite $T(w) \in (|w|+1)\boldsymbol{Z}$ et d'après le théorème de Lamèche–Jacob, $\sum (T(w)/(|w|+1))w$ est rationnelle; on conclut avec le lemme 4.

Lemme 5. *Soit (u_n) une suite d'entiers vérifiant une relation de récurrence à coefficients entiers:*

$$\forall n \geqslant 0, \quad u_{n+q} = a_1 u_{n+q-1} + a_2 u_{n+q-2} + \ldots + a_q u_n \quad (a_i \in \boldsymbol{Z}).$$

Soit p un nombre premier ne divisant pas a_q. Il existe $T \in \boldsymbol{N}^*$ tel que l'application $n \mapsto u_{i+Tn}$ soit continue pour la topologie p-adique ($i \in \boldsymbol{N}$).

Preuve. Soit $M \in \mathscr{M}_q(\boldsymbol{Z})$ la matrice compagnon de la relation de récurrence; il existe alors $\lambda \in \mathscr{M}_{1,q}(\boldsymbol{Z})$ et $\gamma \in \mathscr{M}_{q,1}(\boldsymbol{Z})$ tels que: $\forall n \in \boldsymbol{N}$, $u_n = \lambda M^n \gamma$. Comme p ne divise pas $\det(M) = \pm a_q$, l'image de M dans $\mathscr{M}_q(\boldsymbol{Z}/p\boldsymbol{Z})$ y est inversible, et par suite il existe T tel que: $M^T \equiv I \bmod p$, où I est la matrice identité. De ceci se déduit: $\forall k \geqslant 1$, $M^{Tp^k} = I \bmod p^{k+1}$. Par suite, $\forall k \geqslant 1$, l'homomorphisme $\boldsymbol{N} \to \mathrm{GL}_q(\boldsymbol{Z}/p^k\boldsymbol{Z})$ qui a n associe M^{Tn} est continu quand $\boldsymbol{N}$ est muni de la topologie p-adique et $\boldsymbol{Z}/p^k\boldsymbol{Z}$ de la topologie discrète.

Donc l'homomorphisme $\boldsymbol{N} \to \mathrm{GL}_q(\boldsymbol{Z})$, $n \mapsto M^{Tn}$ est continu pour la topologie p-adique et le lemme 5 s'en déduit. ∎

Preuve du théorème 2. (i) Nous dirons qu'une matrice M est *pseudo-régulière* s'il existe une matrice semblable à M, de la forme $\begin{pmatrix} M_1 & 0 \\ 0 & 0 \end{pmatrix}$ où M_1 est inversible. Le polynôme caractéristique de M est produit de celui de M_1 par une puissance de la variable; par suite $\det(M_1)$ ne dépend que de M et si $M \in \mathscr{M}_r(\boldsymbol{Z})$, $\det(M_1)$ est entier. Nous poserons: $d(M) = \det(M_1)$.

(ii) Soit $\mu: X^* \to \mathscr{M}_r(\boldsymbol{Q})$ un homomorphisme. G. Jacob a montré qu'il existe une constante $N \in \boldsymbol{N}$ telle que pour tout élément w de X^* vérifiant $|w| \geqslant N$, il existe une factorisation $w = w_1 w_2 w_3$ telle que $0 < |w_2| \leqslant N$ et μw_2 est une matrice pseudo-régulière ([6] ou [7], chapitre VII, th. 19).

(iii) Grâce au lemme 4, nous pouvons supposer que S est $\boldsymbol{Z}$-rationnelle. Soit donc (λ, μ, γ) une représentation de S avec: $\lambda \in \mathscr{M}_{1,r}(\boldsymbol{Z})$, $\mu X^* \subset \mathscr{M}_r(\boldsymbol{Z})$ et $\gamma \in \mathscr{M}_{r,1}(\boldsymbol{Z})$.

Soit Q_1 l'ensemble fini des nombres premiers où p divise $d(\mu w)$, $|w| \leqslant N$ et μw pseudo-régulière.

(iv) Soit $w \in X^*$ tel que $|w| \geqslant N$. D'après (ii) il existe une factorisation $w = w_1 w_2 w_3$ où w_2 vérifie: $0 < |w_2| \leqslant N$, w_2 est pseudo-régulière. Donc μw_2 est semblable à une matrice de la forme $\begin{pmatrix} M_1 & 0 \\ 0 & 0 \end{pmatrix}$ où M_1 est inversible. Il existe donc une matrice ligne λ_1 et une matrice colonne γ_1 telles que:

$$\forall n \geqslant 1, \quad S(w_1 w_2^n w_3) = \lambda \mu w_1 \mu w_2^n \mu w_3 \gamma = \lambda_1 M_1^n \gamma_1.$$

D'après (i), le polynôme caractéristique $t^q - a_1 t^{q-1} - \ldots - a_q$ de M_1 est à coefficients entiers et $a_q = \pm\det(M_1) = \pm d(\mu w_2)$.

La suite $u_n = S(w_1 w_2^n w_3)$ vérifie donc:

$$\forall n \geqslant 1, \quad u_{n+q} = a_1 u_{n+q-1} + \ldots + a_q u_n.$$

(v) Soit $p \notin Q_1$. Comme p ne divise pas a_q, il existe d'après le lemme 5 un entier $T \geqslant 1$ tel que l'application $n \mapsto u_{1+Tn} = S(w_1 w_2^{1+Tn} w_3)$ soit continue pour la topologie p-adique. Or l'application $n \mapsto 1 + |w| + nT|w_2|$ $= 1 + |w_1 w_2^{1+Tn} w_3|$ est continue; donc l'application $f: n \mapsto \dfrac{u_{1+Tn}}{|1 + w_1 w_2^{1+Tn} w_3|}$ est continue $\boldsymbol{N} \to \boldsymbol{Q}$.

D'après le lemme 1 et l'hypothèse, $f(n)$ est entier quand n parcourt une partie dense de $\boldsymbol{N}$, donc dense pour la topologie p-adique. Par suite, $f(\boldsymbol{N})$ est contenu dans l'adhérence de $\boldsymbol{N}$ dans $\boldsymbol{Q}$, i.e. $\{x \in \boldsymbol{Q} \mid v_p(x) \geqslant 0\}$, où v_p désigne la valuation p-adique. En particulier: $v_p\big(S(w)/(|w|+1)\big)$ $= v_p\big(f(0)\big) \geqslant 0$.

(vi) On obtient ainsi: $\forall p \in Q_1$, $\forall w$ tel que $|w| \geqslant N$, $v_p\big(S(w)/(|w|+1)\big)$ $\geqslant 0$. Soit Q_2 l'ensemble fini des nombres premiers qui interviennent dans les dénominateurs des $S(w)/(1+|w|)$ où $|w| < N$; soit $Q = Q_1 \cup Q_2$. On peut alors appliquer la proposition 1. ∎

5. Sur l'image d'une série rationnelle. Nous présentons dans ce paragraphe quelques résultats donnant des conditions suffisantes pour qu'une série rationnelle n'ait qu'un nombre fini de coefficients distincts. La plupart d'entre'eux ont déjà été établi dans le cas d'une variable par J. Berstel [1].

Auparavant, énonçons un résultat qui caractérise les séries rationnelles d'image finie, et que nous avons démontré en [13].

Proposition 3. *Soit S une série rationnelle. Les deux conditions suivantes sont équivalentes:*

(i) $\{S(w) |\ w \in X^*\}$ *est fini.*

(ii) *Pour tout rayon* R, $\{S(w) |\ w \in R\}$ *est fini.*

Nous allons démontrer la

PROPOSITION 4. *Soit* S *une série* $\mathbf{Z}$*-rationnelle et* A *dense dans* X^*.

(i) *Si* $S(A)$ *est fini,* S *est d'image finie.*

(ii) *S'il existe* $d \in \mathbf{N}$ *tel que pour tout* $w \in X^*$, $S(w)$ *est nul ou n'a pas plus de* d *diviseurs,* S *est d'image finie.*

Preuve. D'après la proposition 3, il suffit de montrer que pour tout rayon R, $S(R) = \{S(w) |\ w \in R\}$ est fini. Soit uv^*w un rayon; la série en la variable t, $\sum S(uv^n w)t^n$ est $\mathbf{Z}$-rationnelle. De plus, d'après le lemme 1, l'ensemble $B = \{n \in \mathbf{N} |\ uv^n w \in A\}$ est dense dans $\mathbf{N}$.

On est donc ramené à démontrer la proposition dans le cas d'une variable. Pour (ii), c'est un résultat de J. Berstel [1] (corollaire 3.1). Pour (i): soit $\sum u_n t^n$ une série $\mathbf{Z}$-rationnelle d'une variable.

Elle vérifie une relation de récurrence linéaire à coefficients entiers: $\forall n \geqslant 0$, $u_{n+q} = a_1 u_{n+q-1} + \ldots + a_q u_n$ $(a_i \in \mathbf{Z})$. En supprimant un nombre fini de termes de (u_n), on est ramené à: $a_q \neq 0$. Soit p un nombre premier ne divisant pas a_q: d'après le lemme 5, il existe T tel que les T fonctions f_i $(0 \leqslant i \leqslant T-1)$ définies par: $f_i(n) = u_{i+Tn}$ soient continues pour la topologie p-adique.

Pour tout i, l'ensemble A_i des n tels que $i+Tn \in A$ est dense dans $\mathbf{N}$ (lemme 1) et l'on a: $f_i(A_i)$ est fini. Par suite $f_i(\mathbf{N}) = f_i(A_i)$ est fini, et les u_n sont en nombre fini. ■

COROLLAIRE 1. *Soit* S *une série* $\mathbf{Z}$*-rationnelle et* A *dense dans* X^* *tel que* $S(A) = 0$. S *est un polynôme.*

Preuve. D'après la proposition 2, S est d'image finie. Il existe donc un entier $d \geqslant 1$ tel que: $S(w) = 0 \Leftrightarrow d$ divise $S(w)$.

D'après le lemme 3 et l'hypothèse $S(A) = 0$, les $d-1$ ensembles $\{w |\ S(w) \equiv a \bmod d\}$, $0 \leqslant a \leqslant d-1$, sont finis; leur réunion étant précisément le support de S, celui-ci est fini et S est un polynôme. ■

COROLLAIRE 2. *Soit* S *une série* $\mathbf{Z}$*-rationnelle et* A *dense dans* X^*. *Si* $\forall w \in A$, $S(w)$ *est nul ou un nombre premier,* S *est d'image finie.*

Ce corollaire découle de la proposition 2 (ii). ■

Soit P un polynôme d'une variable tel que: $P(n) \in \mathbf{Z}, \forall n \in \mathbf{N}$. Il est bien connu [11] que si $P(\mathbf{N})$ est infini, i.e. P non constant, l'ensemble des nombres premiers p qui divisent l'un des $P(n)$ est infini. On obtient un résultat analogue pour les séries rationnelles, en se restreignant aux séries à *croissance polynômiale*; une série S est dite à croissance polynômiale s'il existe des entiers C et s tels que:

$$\forall w \in X^*, \quad |(S, w)| \leqslant C|w|^s.$$

(Rappelons que $|w|$ désigne la longueur de w.)

PROPOSITION 3. *Soit* S *une série* $\mathbf{Z}$*-rationnelle à croissance polynômiale,* A *dense dans* X^* *et* d *un entier* $\geqslant 1$. *Si pour tout* $w \in A$, $S(w)$ *est nul ou n'admet pas plus de* d *diviseurs premiers, alors* S *est d'image finie.*

Preuve. Comme pour la preuve de la proposition 4, on est ramené au cas où S est une série d'une variable. Mais dans ce cas, la proposition découle d'un résultat de J. Berstel ([1], théorème I). ■

Nous dirons qu'un ensemble E de nombres entiers est un *ensemble de Pólya* si l'ensemble des nombres premiers p où p divise l'un des $x \in E$, $x \neq 0$, est fini.

PROPOSITION 4. *Soit* S *une série* $\mathbf{Z}$*-rationnelle et* A *dense dans* X^*. *Si* $S(A)$ *est un ensemble de Pólya, l'ensemble des coefficients de* S *est un ensemble de Pólya.*

Preuve. Soit Q_1' l'ensemble des nombres premiers p où p divise l'un des $x \in S(A)$, $x \neq 0$. Q_1' est fini par hypothèse. Reprenons les points (i), (ii), (iii), et (iv) de la démonstration du théorème 2.

Soit p un nombre premier $\notin Q_1 \cup Q_1'$. D'après le lemme 5, l'application $n \mapsto u_{1+Tn} = S(w_1 w_2 w_2^{Tn} w_3)$ est continue pour la topologie p-adique. D'après le lemme 1, l'ensemble B des n tels que $w_1 w_2 w_2^{Tn} w_3 \in A$ est dense dans $\mathbf{N}$, donc dense pour la topologie p-adique. Or, $n \in B$ implique que $u_{1+Tn} = 0$ ou p ne divise pas u_{1+Tn}, i.e.: $|u_{1+Tn}|_p = 0$ ou 1. ($|\ |_p$ désigne la norme p-adique.)

Par suite: $\forall n$, $|u_{1+Tn}|_p = 0$ ou 1, et en particulier: $|u_1|_p = \big|(S(w))\big|_p = 0$ ou 1.

D'où: $\forall p \notin Q_1 \cup Q_1'$, $\forall w$ tel que $|w| \geqslant N$, $|S(w)|_p = 0$ ou 1.

Soit Q_2 l'ensemble fini des facteurs premiers des $S(w)$ avec $|w| < N$ et $Q = Q_1 \cup Q_1' \cup Q_2$.

Alors $\forall p \notin Q$, $\forall w \in X^*$, $S(w)$ est nul ou p ne divise pas $S(w)$ et la proposition en découle. ■

Tous mes remerciements vont à J. Berstel pour son aide et ses conseils pendant la rédaction de cet article, et pour avoir bien voulu lire le manuscrit.

Ajouté sur épreuves: la démonstration de la proposition 1 peut-être simplifiée par l'utilisation d'un théorème de Shirshov (voir th. 4.2.8 dans L. H. Rowen: *Polynomials identities in ring theory*, Acad. Press 1980).

Bibliographie

[1] J. Berstel, *Factorisation de fractions rationnelles et de suites récurrentes*, Acta Arith. 30 (1976), p. 5–17.

[2] N. Bourbaki, *Algèbre*, chapitre 9, Hermann, Paris.

[3] S. Eilenberg, *Automata, languages and machines*, vol. A, Acad. Press, New York 1974.

[4] M. Fliess, *Matrices de Hankel*, J. Maths. Pures Appl. 53 (1974), p. 197–222.

[5] M. Hall, Jr., *A topology for free groups and related groups*, Ann. of Math. 52 (1950), p. 127–139.

[6] G. Jacob, Thèse Sci. Maths., Univ. Paris 7 (1975).
[7] — *Un théorème de factorization des produits d'endomorphismes de K^n*, J. Algèbra 63 (1980), p. 389–412.
[8] K. Lamèche, *Quelques propriétés des séries rationnelles en variables non commutatives*, J. Combinatorial Theory (A) 14 (1973), p. 128–135.
[9] K. Mahler, *On the Taylor coefficients of rational functions*, Proc. Cambridge Phil. Soc. 52 (1956), p. 39–48.
[10] G. Pólya, *Arithmetische Eigenschaften der Reihenentwicklungen rationaler Funktionen*, J. Reine Angew. Math. 151 (1928), p. 687–706.
[11] G. Pólya et G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, 2. Band 8. Abschnitt, Springer Verlag, Berlin–Heidelberg–New York 1971.
[12] G. Rauzy, *Ensembles arithmétiquement denses*, C. R. Acad. Sci. Paris Sér. A 265 (1967), p. 37–38.
[13] C. Reutenauer, *Une caractérisation de la finitude de l'ensemble des coefficients d'une série rationnelle en variables non commutatives*, ibid. 284 (1977), p. 1159–1162.
[14] — *Une topologie sur le monoïde libre*, Semigroup Forum 18 (1979), p. 33–49.
[15] H. Davenport, D. J. Lewis and A. Schinzel, *Polynomials of certain special types*, Acta Arith. 9 (1964), p. 107–116.
[16] M. P. Schützenberger, *On the definition of a family of automata*, Information and Control 4 (1961), p. 245–270.

Reçu le 11.5.1978 (1070)

ACTA ARITHMETICA
XXXIX (1981)

A problem of Erdös on sums of two squarefull numbers

by

R. W. K. Odoni (Exeter)

0. Introduction. In a recent list [6] of solved and unsolved problems, P. Erdös notes that many interesting questions arise when one attempts to imitate the proofs of results on quadratic forms (and in particular sums of squares) when considering their apparent analogues for *squarefull numbers*, that is, positive integers n such that, when p is prime and $p|n$, then $p^2|n$. (Erdös calls these *powerful numbers*.)

Our concern in this paper is to answer, in the negative, Erdös's question as to whether the number of natural numbers $\leqslant x$ which are sums of two squarefull numbers $\sim Cx(\log x)^{-1/2}$ (which is the expected quantity, by analogy with Landau's well known result [10] for sums of two squares). We shall achieve this by proving

Theorem 1. *Let $\mathscr{U}$ denote the set of sums of two squarefull numbers. Then there exist positive constants α, β and γ such that*

$$\text{(I)} \qquad \operatorname{card}\mathscr{U}\cap[1,x] > \alpha x(\log x)^{-1/2}\exp(\beta\log\log x/\log\log\log x)$$

for all $x > \gamma$.

We remark that Theorem 1 is not necessarily so surprising as it seems at first glance, since A. O. L. Atkin [1] has shown how a slight "perturbation" of the sequence, S, of natural squares can yield a sequence S' for which $S' \dotplus S'$ has positive natural density. There is no relation between Atkin's arguments and our own, however.

The proof of Theorem 1 is rather complicated, and therefore requires some preliminary discussion. We view Erdös's problem as one on the representation of natural numbers by at least one of a large set of positive definite binary integral quadratic forms. We note that $\mathscr{U}$ is identical with the set of all integers represented by at least one of the quadratic forms

$$F_{mn} = F_{mn}(x,y) = m^3x^2 + n^3y^2 \quad \text{for} \quad m, n \geqslant 1,\ m \leqslant n \text{ and } (m,n) = 1.$$

Since we only require an Ω-result for $\mathscr{U}$, it will suffice to replace $\mathscr{U}$ in Theorem 1 by any subset $\mathscr{U}_1$ of $\mathscr{U}$. We take advantage of this in order to