Michigan Math. J. 47 (2000)

Propriétés Arithmétiques de Fractions Rationnelles à Coefficients Algébriques

Jean-Christophe Masseron

1. Introduction

La manière dont certaines propriétés imposées aux valeurs d'un polynôme détermine ce polynôme, a intéressé de nombreux auteurs. Le lecteur désirant avoir de plus amples informations et d'autres résultats que ceux présentés ici sur ce sujet pourra consulter les livres de Narkiewicz [4] et la Section 22 à partir du Théorème 33 du livre de Schinzel [5]. Notons qu'un problème voisin est de regarder à quelles conditions une fonction entière sur $\mathbb{C}$ prenant des valeurs entières est un polynôme (voir Waldschmidt [8] et références).

Si nous considérons une fraction rationnelle à une variable à coefficients dans $\mathbb{Q}$, on sait que si elle prend des valeurs entières sur un ensemble infini d'entiers, alors cette fraction rationnelle est un polynôme.

En dimension r, il convient de se poser la question suivante.

Question 1.1. Quelle condition mettre sur l'ensemble $E \subset \mathbb{Z}^r$ pour que f étant dans $\mathbb{Q}(X_1, \dots, X_r)$, si

$$\forall \vec{n} \in E, \quad f(\vec{n}) \in \mathbb{Z} \text{ ou } f(\vec{n}) \text{ n'est pas défini}$$

alors f est dans $\mathbb{Q}[X_1, \dots, X_r]$?

Remarque 1.1. Pour alléger les énoncés des théorèmes, dans la suite du texte, $f(E) \subset \mathbb{Z}$ signifie que pour tout $\vec{n} \in E$, $f(\vec{n}) \in \mathbb{Z}$, ou $f(\vec{n})$ n'est pas défini; nous vérifierons dans les preuves que cette convention ne pose pas de problèmes.

Yasumoto [9] dans son article est parti de cette idée en regardant les fractions rationnelles à un nombre r quelconque de variables à coefficients entiers algébriques prenant des valeurs entières algébriques.

La motivation du présent texte est née de la lecture de cet article de Yasumoto [9]. Ce dernier donne une condition sur E liée à la densité Banachique qui se définit comme suit.

Définition 1.1. Soient $r \geq 1$, $A \subset \mathbb{Z}^r$, et $k \in \mathbb{N}$, on pose

$$A_k = \left\{ \vec{n} = (n_1, \dots, n_r) \in A, \ \max_{1 \leq i \leq r} |n_i| \leq k \right\}.$$

Received December 22, 1998. Revision received January 5, 2000.

On définit alors la densité supérieure Banachique par

$$\mathrm{d}(A) = \limsup_{k\to\infty} \frac{\operatorname{card} A_k}{(2k+1)^r}.$$

THÉORÈME 1.1 (Yasumoto). *Soit $r \geq 1$. Soit $A \subset \mathbb{Z}^r$ tel que $\mathrm{d}(A) > 0$, et soit $f \in \bar{\mathbb{Q}}(X_1, \ldots, X_r)$. Si $f(\vec{n})$ est un entier algébrique pour tout $\vec{n} \in A$, alors f est un polynôme de $\bar{\mathbb{Q}}[X_1, \ldots, X_r]$.*

Dans la suite de son article, Yasumoto [9] étend son résultat aux fonctions rationnelles des variétés affines lisses au-dessus de $\bar{\mathbb{Q}}$. Dans le présent texte, nous nous intéressons au cas des fractions rationnelles à deux variables sur $\mathbb{Q}$, et les résultats ainsi donnés peuvent s'étendre facilement aux entiers algébriques; ce qui est montré à la fin de la Partie 2.

Le résultat que nous allons démontrer améliore celui de Yasumoto pour $r = 2$.

THÉORÈME 1.2. *Soit $\varepsilon > 0$. Soit $E \subset \mathbb{Z}^2$, tel que*

$$\limsup_{k\to\infty} \frac{\operatorname{card} E \cap \{(m,n) \in \mathbb{Z}^2,\ -k \leq m, n \leq k\}}{k^{3/2+\varepsilon}} > 0.$$

Soit $f \in \mathbb{Q}(X, Y)$. Si

$$f(\vec{n}) \in \mathbb{Z} \quad \forall \vec{n} \in E,$$

alors

$$f \in \mathbb{Q}[X, Y].$$

Dans la Partie 2, nous prouvons que si une fraction rationnelle f en une variable prend plus de $c(f)$ valeurs entières (où $c(f)$ se calcule en fonction des coefficients et des degrés d'un numérateur et d'un dénominateur de f), alors f est un polynôme.

Dans la Partie 3.1, nous donnons un critère suffisant pour que les ensembles E répondent affirmativement à la Question 1.1 dans le cas $r = 2$. On se ramène au cas des fractions rationnelles à une indéterminée par la spécialisation $Y = aX + b$. Dans la Partie 3.2 nous démontrons à l'aide de ce critère le Théorème 1.2. De plus, contrairement à Yasumoto [9], cette démonstration n'utilise pas la construction des hyperrationnels, et par conséquent ne fait pas appel à l'axiome du choix. En effet, Yasumoto introduit la notion d' "hyper-entiers arithmétiquement indépendants" et démontre qu'ils le sont presque tous pour établir son résultat.

Enfin, la Partie 3.3 est l'occasion de rechercher le meilleur exposant de k qu'on peut atteindre par cette méthode. Dans cet esprit, on peut poser la question suivante.

CONJECTURE 1.1. Soit $A \subset \mathbb{Z}^2$ et $\varepsilon > 0$ tels que

$$\limsup_{k\to\infty} \frac{\operatorname{card} A_k}{k^{1+\varepsilon}} > 0.$$

Pour $f \in \mathbb{Q}(X, Y)$, si $f(A) \subset \mathbb{Z}$ a-t-on nécessairement f polynôme de $\mathbb{Q}[X, Y]$?

On remarquera d'ailleurs à la Section 3.3.4 que la quantité $k^{1+\varepsilon}$ ne peut pas être remplacée par $k \log k$.

2. Cas des Fractions Rationnelles à une Indéterminée

2.1. Fractions Rationnelles de $\mathbb{Q}(X)$

Nous allons avoir besoin pour la suite de deux types de mesures sur les polynômes, la première se trouve dans le livre de Lang [1] au Chapitre 3, début du paragraphe 2 ("Gauss' Lemma") et la seconde dans l'article de Mahler [3], cette dernière définition se retrouvant aussi dans le livre de Waldschmidt [7]. Dans les deux définitions qui viennent, on considère $P \in \mathbb{Z}[X]$ avec

$$P(X) = \sum_{i=0}^{\deg P} P_i X^i.$$

Définition 2.1. On appelle hauteur du polynôme P, le nombre

$$|P| = \sup_i |P_i|.$$

Définition 2.2. On appelle mesure de Mahler du polynôme P, le nombre

$$\mathrm{M}(P) = \begin{cases} \exp\left(\int_0^1 \log|P(e^{2i\pi t})|\, dt\right) & \text{si } P \neq 0, \\ 0 & \text{si } P = 0. \end{cases}$$

Nous allons aussi utiliser le résultat suivant, qui est implicite dans l'article de Mahler [3] à l'équation II.

Lemme 2.1. *Soient* P, Q *dans* $\mathbb{Z}[X]$, *on a*

$$|P||Q| \leq 2^{\deg P + \deg Q} (\deg P + \deg Q + 1)^{1/2} |PQ|.$$

Preuve. Ce résultat est directement issu des suivants, pour P et Q dans $\mathbb{Z}[X]$:

(i) $|P| \leq 2^{\deg(P)} \mathrm{M}(P)$;
(ii) $\mathrm{M}(P) \leq (\deg(P) + 1)^{1/2} |P|$;
(iii) $\mathrm{M}(PQ) = \mathrm{M}(P)\mathrm{M}(Q)$.

D'où $|P||Q| \leq 2^{\deg P} 2^{\deg Q} \mathrm{M}(P)\mathrm{M}(Q) \leq 2^{\deg P + \deg Q} \mathrm{M}(PQ)$ or comme

$$\mathrm{M}(PQ) \leq (\deg PQ + 1)^{1/2} |PQ|,$$

on obtient

$$|P||Q| \leq 2^{\deg P + \deg Q} (\deg P + \deg Q + 1)^{1/2} |PQ|. \qquad \square$$

Définissons les ensembles suivants, pour P_1 et P_2 dans $\mathbb{Z}[X] \backslash \{0\}$,

$$E(P_1, P_2) = \left\{ n \in \mathbb{Z},\ \frac{P_1(n)}{P_2(n)} \in \mathbb{Z} \text{ ou } P_2(n) = 0 \right\}.$$

Il est clair que:

LEMME 2.2. *Soient P, P_1, et P_2 trois polynômes de $\mathbb{Z}[X]$ non nuls. Nous avons*:
(i) $E(P_1, P_2) \subset E(P_1 + PP_2, P_2)$;
(ii) $E(P_1, P_2) \subset E(P_1 P, P_2)$;
(iii) $\operatorname{card} E(P_1 P, P_2 P) \leq \operatorname{card} E(P_1, P_2) + \deg P$.

Dans toute la suite de cette partie, on considère $g/h \in \mathbb{Q}(X)$ avec:
(a) g, h dans $\mathbb{Z}[X]\backslash\{0\}$;
(b) $\tilde{g}, \tilde{h}$ dans $\mathbb{Z}[X]$, premiers entre eux sur $\mathbb{Z}[X]$ tels que

$$g = \Delta\tilde{g} \quad \text{et} \quad h = \Delta\tilde{h}$$

(i.e., $g/h = \tilde{g}/\tilde{h}$) où $\Delta = \operatorname{pgcd}(g, h)$ sur $\mathbb{Z}[X]$.

Déterminons maintenant un majorant du nombre de points entiers atteints par la fraction rationnelle g/h.

Supposons pour la suite de cette partie que $\tilde{h} \notin \mathbb{Z}$ (i.e., $g/h \notin \mathbb{Q}[X]$). Soit $R \in \mathbb{Z}$, le résultant de $\tilde{g}$ et $\tilde{h}$. Il existe $(u, v) \in \mathbb{Z}[X]^2$ tel que

$$\begin{cases} \deg u < \deg \tilde{h} \\ \deg v < \deg \tilde{g} \end{cases} \quad \text{et} \quad R = u\tilde{g} + v\tilde{h}.$$

Grâce au Lemme 2.2, il suffit de majorer le nombre de points entiers de $\tilde{g}/\tilde{h}$ (car $g/h = \Delta\tilde{g}/\Delta\tilde{h}$), et on a

$$E(\tilde{g}, \tilde{h}) \subset E(u\tilde{g} + v\tilde{h}, \tilde{h}) = E(R, \tilde{h}).$$

Ainsi le nombre maximal de points entiers que peut avoir la fraction rationnelle $\tilde{g}/\tilde{h}$ est au plus le nombre de points dont l'image par $\tilde{h}$ est un diviseur de R.

On va donc maintenant chercher à majorer le nombre de diviseurs de R. On notera pour la suite, pour un entier $n \in \mathbb{N}$,

$$\operatorname{div}(n) = \operatorname{card}\left\{k \in \mathbb{Z},\ k\big|_{\mathbb{Z}} n\right\}.$$

Le Théorème 1.5.4 du livre de Tenenbaum [6] donne la première partie du résultat suivant.

LEMME 2.3. *Pour tout ε réel positif strict, il existe un entier $N_0 \geq 16$ tel que l'on ait pour $n \geq N_0$, d'une part*

$$\operatorname{div}(n) \leq 2n^{\frac{\log 2+\varepsilon}{\log\log n}}$$

et d'autre part

$$n'^{\frac{\log 2+\varepsilon}{\log\log n}} > n^{\frac{\log 2+\varepsilon}{\log\log n}} \quad \forall n' > n.$$

Posons:
(i) $\varepsilon = 10 - \log 2$;
(ii) $\sigma : \mathbb{N}\backslash\{0, 1\} \to \mathbb{R}_+$ et $n \mapsto \sigma(n) = 2n^{\frac{10}{\log\log n}}$;
(iii) $N_0 = 16$.

En effet, pour tout $n \geq 3$, $\operatorname{div}(n) \leq 2n^{\frac{10}{\log\log n}}$ (cf. [6]).

On a $|R| \leq |\tilde{g}|^{\deg \tilde{h}} |\tilde{h}|^{\deg \tilde{g}} (\deg \tilde{g} + \deg \tilde{h})!$ par majoration de chaque coefficient des polynômes par leur hauteur.

En appliquant le Lemme 2.1 à Δ, $\tilde{g}$, $\tilde{h}$, nous avons les majorations suivantes:

$$\begin{cases} |\Delta||\tilde{g}| \leq 2^{\deg g} (\deg g + 1)^{1/2} |g|, \\ |\Delta||\tilde{h}| \leq 2^{\deg h} (\deg h + 1)^{1/2} |h| \end{cases}$$

d'où

$$\begin{cases} |\tilde{g}| \leq 2^{\deg g} (\deg g + 1)^{1/2} |g|, \\ |\tilde{h}| \leq 2^{\deg h} (\deg h + 1)^{1/2} |h|. \end{cases}$$

Il s'ensuit que

$$|R| \leq N(g, h)$$

où

$$N(g,h) = 16 + 4^{\deg g \times \deg h} (\deg g + 1)^{(\deg h)/2} (\deg h + 1)^{(\deg g)/2} \times |g|^{\deg h} |h|^{\deg g} (\deg g + \deg h)!.$$

On a alors $N(g,h) \geq |R|$ et $N(g,h) \geq 16$, et comme σ est croissante au-dessus de 16, on obtient

$$\operatorname{div}(R) \leq \sigma(N(g,h)).$$

Donc, avec le Lemme 2.2,

$$\operatorname{card} E(g,h) \leq \deg h + \operatorname{card} E(\tilde{g}, \tilde{h}) \leq (\sigma(N(g,h)) + 1) \deg h.$$

Si on pose

$$M(g,h) = (\sigma(N(g,h)) + 1) \deg h + 1,$$

on peut alors affirmer:

THÉORÈME 2.1. *Soit $g/h \in \mathbb{Q}(X)$ avec g et h dans $\mathbb{Z}[X]$ et $h \neq 0$. Soit $E(g,h) = \{n \in \mathbb{Z},\ g(n)/h(n) \in \mathbb{Z}$ ou $h(n) = 0\}$. Si*

$$\operatorname{card} E(g,h) \geq M(g,h)$$

alors

$$\frac{g}{h} \in \mathbb{Q}[X].$$

2.2. Fractions Rationnelles de $\bar{\mathbb{Q}}(X)$

On va maintenant introduire un argument Galoisien qui va nous permettre d'étendre le résultat du Théorème 2.1 aux fractions rationnelles à coefficients algébriques.

Soit $g/h \in \bar{\mathbb{Q}}(X)$, avec $g, h \in \bar{\mathbb{Z}}[X]$, anneau des polynômes à coefficients entiers algébriques. Soit $\mathbb{K}(g,h)$, la clôture galoisienne du corps de nombres engendré par les coefficients de g et h. Posons

$$\mathbb{G}(g,h) = \operatorname{Gal}(\mathbb{K}(g,h), \mathbb{Q}) = \{\sigma_1, \ldots, \sigma_t\}.$$

Ecrivons les fonctions symétriques élémentaires en les $(g/h)^\sigma$, $\sigma \in \mathbb{G}(g,h)$, sous la forme $\bar{g}_j/H$ $(1 \le j \le t)$; où

$$H = \prod_\sigma h^\sigma.$$

On a, pour tout j, $\bar{g}_j/H \in \mathbb{Q}(X)$, ce qui va permettre de nous ramener au cas précédent.

THÉORÈME 2.2. *Si*

$$\mathrm{card}\left\{n \in \mathbb{Z},\ \frac{g}{h}(n) \in \bar{\mathbb{Z}} \text{ ou } h(n) = 0\right\} \ge \max_j M(\bar{g}_j, H)$$

alors

$$\frac{g}{h} \in \bar{\mathbb{Q}}[X].$$

Preuve. Remarquons d'abord que, pour tout $1 \le j \le t$,

$$\mathrm{card}\, E(\bar{g}_j, H) \ge \mathrm{card}\left\{n \in \mathbb{Z},\ \frac{g}{h}(n) \in \bar{\mathbb{Z}} \text{ ou } h(n) = 0\right\}.$$

On applique alors le Théorème 2.1 à $\bar{g}_j/H$, pour $1 \le j \le t$. Comme $M(\bar{g}_j, H)$ ne dépend que de $[\mathbb{K}(g,h) : \mathbb{Q}]$ et de la hauteur des coefficients, $\bar{g}_j/H$ est dans $\bar{\mathbb{Q}}[X]$ pour tout j.

Ainsi, g/h est racine de

$$P(Y) = \prod_\sigma \left(Y - \left(\frac{g}{h}\right)^\sigma\right)$$

polynôme unitaire de $(\bar{\mathbb{Q}}[X])[Y]$. Donc g/h est entier sur l'anneau $\bar{\mathbb{Q}}[X]$ et comme g/h est dans $\bar{\mathbb{Q}}(X)$, on a $g/h \in \bar{\mathbb{Q}}[X]$. □

3. Fractions Rationnelles à Deux Indéterminées

3.1. Majoration Effective du Nombre de Points Entiers

3.1.1. Fractions Rationnelles de $\mathbb{Q}(X, Y)$

Dans cette partie, on va majorer le nombre de points entiers que peut prendre une fraction rationnelle donnée à deux indéterminées. Le principe est de compter les points entiers atteints sur les droites de la forme $Y = aX + b$ où $(a,b) \in \mathbb{Z}^2$. Dans cette partie, on considère les fractions rationnelles p/q de $\mathbb{Q}(X,Y)$ avec p et q dans $\mathbb{Z}[X,Y]$ sans facteur commun, $q \notin \mathbb{Z}[X]$ et $p \ne 0$.

NOTATION 3.1. Dans toute la Partie 3, la notation "deg" sans précision de variable désignera le degré total des polynômes à 2 variables.

On pose formellement, pour tout $(a,b) \in \mathbb{Z}^2$,

$$p_{a,b}(X) = p(X, aX + b).$$

On a donc $p_{a,b} \in \mathbb{Q}[X]$.

Nous aurons tout d'abord besoin des résultats suivants.

LEMME 3.1. *Pour $p/q \in \mathbb{Q}(X, Y)$, l'écriture formelle $p_{a,b}/q_{a,b}$ définit une fraction rationnelle de $\mathbb{Q}(X)$ pour tous les couples $(a, b) \in \mathbb{Z}^2$ sauf au plus* $\deg q$ *couples.*

Preuve. Soit $p/q \in \mathbb{Q}(X, Y)$. Il suffit d'éviter tous les couples $(a, b) \in \mathbb{Z}^2$ tels que $q_{a,b} = 0$. Cela revient à considérer les couples $(a, b) \in \mathbb{Z}^2$ tels que

$$Y - (aX + b)\big|_{\mathbb{Q}[X,Y]}q(X, Y).$$

Pour des couples (a, b) distincts, les $Y - (aX + b)$ sont deux à deux premiers; d'où $p_{a,b}/q_{a,b}$ est définie sur tout $\mathbb{Z}^2$ sauf au plus $\deg q$ couples d'entiers. □

REMARQUE 3.1. D'après le Lemme 3.1, pour tout entier b il existe au plus $\deg q$ entiers a tels que $q_{a,b} = 0$.

Dans la suite du texte, nous utiliserons sans autre précision des couples d'entiers (a, b) tels que les fractions rationnelles du type $p_{a,b}/q_{a,b}$ soient définies dans $\mathbb{Q}(X)$.

Etablissons une notation particulière des polynômes $p_{a,b}$.

NOTATION 3.2. Posons, pour $p \in \mathbb{Z}[X, Y]$,

$$p(X, Y) = \sum_{0 \le i+j \le \deg p} P_{i,j} X^i Y^j.$$

On a donc pour tout $(i, j) \in \{1, \dots, \deg p\}^2$, $P_{i,j} \in \mathbb{Z}$. Alors

$$p_{a,b}(X) = \sum_{0 \le i+j \le \deg p} P_{i,j} X^i (aX + b)^j;$$

soit

$$p_{a,b}(X) = \sum_{0 \le i \le \deg p} p_{(i)}(a, b) X^i$$

avec $p_{(i)} \in \mathbb{Z}[X, Y]$.

Comptons à $b \in \mathbb{Z}$ fixé le nombre de coefficients $a \in \mathbb{Z}$ tels que $q_{a,b} \in \mathbb{Z}$.

LEMME 3.2. *Soit $b \in \mathbb{Z}$. On a*

$$\operatorname{card}\{a \in \mathbb{Z},\ q_{a,b} \in \mathbb{Z}\} \le \deg q.$$

Preuve. On sait que pour tout $(a, b) \in \mathbb{Z}^2$, $q_{a,b} \in \mathbb{Z}[X]$; donc, avec la Notation 3.2, si $q_{a,b} \in \mathbb{Z}$ on peut écrire ce polynôme sous la forme

$$q_{a,b}(X) = q_{(0)}(a, b) = \sum_{j=0}^{\deg q} Q_{0,j} b^j$$

où pour tout entier $j \in [0, \deg q]$, on a $Q_{0,j} \in \mathbb{Z}$. Donc,

$$Y-(aX+b)\big|_{\mathbb{Z}[X,Y]}q(X,Y)-\sum_{j=0}^{\deg q}Q_{0,j}b^j.$$

Or, à b fixé, les polynômes $Y-(aX+b)$ sont premiers entre eux. Donc, ils sont au plus au nombre des $\deg q$ facteurs irréductibles de

$$q-\sum_{j=0}^{\deg q}Q_{0,j}b^j,$$

qui ne peut être nul, q n'étant pas dans $\mathbb{Z}$. □

REMARQUE 3.2. On enlèvera pour tout b les entiers a tels que $q_{a,b}\in\mathbb{Z}$, donc y compris ceux tels que $q_{a,b}=0$.

Voyons maintenant pour un $b\in\mathbb{Z}$ et un $a_0\in\mathbb{Z}$ fixés tels que $q_{a_0,b}\notin\mathbb{Z}$, combien de coefficients $a\in\mathbb{Z}$ répondent à la condition $q_{a,b}=q_{a_0,b}$.

LEMME 3.3. *Soit $b\in\mathbb{Z}$, et soit $a_0\in\mathbb{Z}$ tel que $q_{a_0,b}\notin\mathbb{Z}$. Alors, si on pose*

$$Q(a_0)=\{a\in\mathbb{Z},\ q_{a,b}=q_{a_0,b}\},$$

on a

$$\operatorname{card}Q(a_0)\le\deg q.$$

Preuve. Si $Q(a_0)=\{a_0\}$, il n'y a rien à démontrer. Sinon, il existe $a\in Q(a_0)\backslash\{a_0\}$. Alors, $q_{(i)}(a,b)=q_{(i)}(a_0,b)$ pour tout $0\le i\le\deg q$. De plus comme $q_{a,b}=q_{a_0,b}\notin\mathbb{Z}$, il existe $i_0>0$ tel que $q_{(i_0)}\neq 0$.

(i) Si pour tout entier $i\in[0,\deg q]$ tel que $\deg q_{(i)}>0$, on a $\deg_X q_{(i)}\le 0$ alors

$$q_{a,b}(X)=\sum_{j=0}^{\deg q}q_{(j)}(a,b)X^j=k(X)\in\mathbb{Z}[X]$$

avec k ne dépendant pas de a. Donc, pour tout $a\in Q(a_0)$,

$$Y-(aX+b)\big|_{\mathbb{Z}[X,Y]}(q(X,Y)-k(X)).$$

Par un raisonnement analogue à celui de la démonstration du Lemme 3.2, il ne peut y avoir plus de $\deg q$ éléments dans $Q(a_0)$.

(ii) Sinon, $\deg_X q_{(i_0)}>0$ et alors a est racine du polynôme $q_{(i)}(X,b)-q_{(i)}(a_0,b)$; ce qui entraîne évidemment que le nombre d'éléments de $Q(a_0)$ est inférieur à $\deg q_{(i_0)}$.

Dans tous les cas, $\operatorname{card}Q(a_0)\le\deg q$. □

Introduisons les ensembles $E(p,q,2)$ qui seront les analogues des $E(p,q)$ de la Partie 2. Pour tout $p\in\mathbb{Z}[X]$, posons $M(p,0)=0$ et $E(p,0)=\mathbb{Z}$. Soit, pour $q\neq 0$,

$$E(p,q,2)=\big\{b\in\mathbb{Z},\ \operatorname{card}\{a\in\mathbb{Z},\ \operatorname{card}E(p_{a,b},q_{a,b})>M(p_{a,b},q_{a,b})\}>1+\deg q(1+2^{2\deg p\deg q})\big\};$$

où on définit, pour $q_{a,b} \neq 0$,

$$M(p_{a,b}, q_{a,b}) = 1 + \deg q\Big(1 + 2N(p_{a,b}, q_{a,b})^{\frac{10}{\log\log N(p_{a,b}, q_{a,b})}}\Big).$$

Pour simplifier les notations, on notera $\mathrm{C}(x, y)$, la condition $\operatorname{card} E(x, y) > M(x, y)$.

On va maintenant adapter les constantes de la Partie 2 aux polynômes à deux indéterminées; en effet, on a

$$p_{a,b}(X) = p(X, aX + b) = \sum_{i=0}^{\deg p} X^i \sum_{j=0}^{\deg p-i} P_{i,j}(aX + b)^j.$$

Soit

$$p_{a,b}(X) = \sum_{i=0}^{\deg p} X^i \sum_{j=0}^{\deg p-i} P_{i,j} \sum_{k=0}^{j} \mathrm{C}_j^k a^k b^{j-k} X^k = \sum_{i=0}^{\deg p} \sum_{k=0}^{\deg p-i} \alpha_k X^{i+k}$$

avec

$$\alpha_k = a^k \sum_{j=k}^{\deg p-i} \mathrm{C}_j^k P_{i,j} b^{j-k}.$$

En remarquant que pour tout entier $k \in [0, \deg p]$

$$\sum_{j=k}^{\deg p-i} \mathrm{C}_j^k = \mathrm{C}_{\deg p-i+1}^{k+1},$$

on a

$$|\alpha_k| \leq |p|(|a| + |b|)^{\deg p+1} \leq |p|(2\max(|a|, |b|))^{\deg p+1}.$$

Donc, comme

$$p_{a,b}(X) = \sum_{l=0}^{\deg p} X^l \sum_{i=0}^{l} \alpha_i,$$

on a

$$|p_{a,b}| \leq |p|(\deg p + 1)(2\max(|a|, |b|))^{\deg p+1}.$$

On va donc poser, pour $q_{a,b} \neq 0$,

$$\begin{aligned} &N(p_{a,b}, q_{a,b}) \\ &\quad= 16 + 4^{(\deg p+\deg q)^2}(\deg p + \deg q)!|p|^{\deg q}|q|^{\deg p} \\ &\qquad\times (\deg p + 1)^{(3\deg q)/2}(\deg q + 1)^{(3\deg p)/2}\max(|a|, |b|)^{(\deg p+\deg q)^2} \end{aligned}$$

Notons $R_Y(p, q)$ le résultant de p et q en la variable Y dans $\mathbb{Z}[X]$. Si $p \in \mathbb{Z}[X]$, on prend $R_Y(p, q) = p$. Le lemme suivant fait le lien avec la Partie 2, puisque les polynômes considérés ici sont à une indéterminée:

LEMME 3.4. *Soient p, q deux polynômes à deux variables sans facteur commun. Soit $(a, b) \in \mathbb{Z}^2$ tel que $\mathrm{C}(p_{a,b}, q_{a,b})$ et $q_{a,b} \neq 0$. On a alors*

$$q_{a,b}\big|_{\mathbb{Q}[X]} R_Y(p, q).$$

Preuve. Puisque p et q sont sans facteur commun, et $q_{a,b} \notin \mathbb{Z}$, donc d'après le Théorème 2.1 si $\mathrm{C}(p_{a,b}, q_{a,b})$, alors on a $p_{a,b}/q_{a,b} \in \mathbb{Q}[X]$. Comme $R_Y(p,q) = up + vq$ avec u et v dans $\mathbb{Z}[X,Y]$, on a

$$\frac{p_{a,b}}{q_{a,b}} u_{a,b} + v_{a,b} \in \mathbb{Q}[X].$$

Donc

$$\frac{R_Y(p,q)}{q_{a,b}} \in \mathbb{Q}[X]. \qquad \square$$

On va ici compter le nombre de polynômes distincts du type $q_{a,b}$ qu'on obtient à b fixé.

LEMME 3.5. *Soit $b \in E(p,q,2)$. On a*

$$\operatorname{card}\big\{a \in \mathbb{Z},\ \mathrm{C}(p_{a,b}, q_{a,b}),\ q_{a,b} \notin \mathbb{Z} \text{ et } \forall a' < a,\ \text{si } q_{a',b} \notin \mathbb{Z} \text{ alors } a \notin Q(a')\big\} \leq 2^{2\deg p \deg q}.$$

Preuve. D'après le Lemme 3.4, $q_{a,b}\big|_{\mathbb{Z}[Q]} R_Y(p,q)$. Donc $q_{a,b}$ prend ses au plus $\deg q$ facteurs irréductibles parmi les au plus $2\deg p \deg q$ facteurs irréductibles de $R_Y(p,q)$ comptés avec leurs multiplicités. Donc les polynômes de la forme $q_{a,b}$ parmi les diviseurs éventuels de $R_Y(p,q)$ sont aux constantes près au plus au nombre de $2^{2\deg p \deg q}$. $\square$

REMARQUE 3.3. On peut aussi voir dans le Lemme 3.5 une relation d'équivalence sur $\mathbb{Z}$,

$$a \Re a' \iff Q(a) = Q(a'),$$

et démontrer que

$$\operatorname{card}\big(\{a \in \mathbb{Z},\ \mathrm{C}(p_{a,b}, q_{a,b}),\ q_{a,b} \notin \mathbb{Z}\}/\Re\big) \leq 2^{2\deg p \deg q}.$$

Reprenons le comptage avec le résultat que nous apporte le lemme précédent:

$$\begin{aligned}
&\operatorname{card}\big\{a \in \mathbb{Z},\ \mathrm{C}(p_{a,b}, q_{a,b})\big\} \\
&\quad = \operatorname{card}\Big(\big\{a \in \mathbb{Z},\ \mathrm{C}(p_{a,b}, q_{a,b}),\ q_{a,b} \notin \mathbb{Z}\big\} \cup \big\{a \in \mathbb{Z},\ \mathrm{C}(p_{a,b}, q_{a,b}),\ q_{a,b} \in \mathbb{Z}\big\}\Big) \\
&\quad \leq \operatorname{card}\Big(\big\{a \in \mathbb{Z},\ \mathrm{C}(p_{a,b}, q_{a,b}),\ q_{a,b} \notin \mathbb{Z}\big\}/\Re\Big) \operatorname{card}\Big(\max_{a \in \mathbb{Z}} Q(a)\Big) + \deg q \\
&\quad \leq \deg q\,(1 + 2^{2\deg p \deg q}).
\end{aligned}$$

Introduisons maintenant les notations et hypothèses propres au théorème que nous allons démontrer.

1. Soit $g/h \in \mathbb{Q}(X,Y)$, avec g et h dans $\mathbb{Z}[X,Y]$. Considérons $\tilde{g}$ et $\tilde{h}$ dans $\mathbb{Z}[X,Y]$ sans facteurs communs tels que $g/h = \tilde{g}/\tilde{h}$. On a alors $\deg \tilde{g} \leq \deg g$ et $\deg \tilde{h} \leq \deg h$.

2. On suppose que $h \notin \mathbb{Z}[X]$, c'est-à-dire que le degré en Y du polynôme h n'est pas négatif ou nul.

3. D'une part, on a $R_Y(\tilde{g}, \tilde{h}) \neq 0$, car $\tilde{g}$ et $\tilde{h}$ sont sans facteur commun. D'autre part, il existe un couple de polynômes $(u, v) \in \mathbb{Z}[X, Y]$ tels que:

(a) $\tilde{g}u + \tilde{h}v = R_Y(\tilde{g}, \tilde{h})$;
(b) $\deg_Y u < \deg_Y \tilde{h} \leq \deg_Y h$;
(c) $\deg_Y v < \deg_Y \tilde{g} \leq \deg_Y g$;
(d) si $\tilde{g} \in \mathbb{Z}[X]$, on pose bien sûr, $v = 0$ et $u = 1$.

PROPOSITION 3.1. *Soit $g/h \in \mathbb{Q}(X, Y)$ avec $h \notin \mathbb{Z}[X]$. Si*

$$\operatorname{card} E(g, h, 2) > \deg h,$$

alors

$$\frac{g}{h} \in \mathbb{Q}[X, Y].$$

Preuve. Nous allons montrer ce résultat par l'absurde. Posons $\tilde{g}/\tilde{h} = g/h$ où $\tilde{g}$ et $\tilde{h}$ sont sans facteur commun. Supposons

$$\operatorname{card} E(g, h, 2) > \deg h$$

et

$$\frac{\tilde{g}}{\tilde{h}} \in \mathbb{Q}(X, Y)\backslash\mathbb{Q}[X, Y].$$

Dans la suite de la démonstration de la Proposition 3.1, nous allons nous efforcer de trouver une contradiction à $\tilde{h} \notin \mathbb{Z}$. Nous aurons alors terminé notre travail concernant la démonstration par l'absurde.

A b fixé, nous pouvons grâce au Lemme 3.3 majorer le nombre d'entiers a tel que $\tilde{h}_{a,b} = \tilde{h}_{a_0,b}$ pour un entier a_0 fixé. Nous devons maintenant majorer le nombre d'ensemble $\tilde{H}(a_0)$ ainsi obtenus, c'est le but du Lemme 3.5. Mais comme pour tout entier b de $E(g, h, 2)$, on a

$$\operatorname{card}\{a \in \mathbb{Z},\ \mathrm{C}(g_{a,b}, h_{a,b})\} \geq 1 + \deg h(1 + 2^{2 \deg g \deg h}),$$

il existe des polynômes $\tilde{h}_{a,b}$ diviseurs de $R_Y(g, h)$, égaux à une constante multiplicative près.

Donc il existe un entier $a \in \mathbb{Z}$ tel que

(i) $\mathrm{C}(g_{a,b}, h_{a,b})$;
(ii) il existe $a' \in \mathbb{Z}\backslash\{a\}$ et $\alpha \in \mathbb{Q}\backslash\{0, 1\}$ tels que $\mathrm{C}(g_{a',b}, h_{a',b})$ et $\tilde{h}_{a,b} = \alpha\tilde{h}_{a',b}$ avec $\tilde{h}_{a,b} \notin \mathbb{Z}$ d'après le Lemme 3.2.

Alors, pour un tel entier a,

$$\tilde{h}_{a,b}(X) = \sum_{i=0}^{\deg \tilde{h}} \tilde{h}_{(i)}(a, b)X^i = \alpha \sum_{i=0}^{\deg \tilde{h}} \tilde{h}_{(i)}(a', b)X^i.$$

Le lemme suivant nous conduira à la contradiction recherchée, car un tel polynôme $\tilde{h}$, avec les contraintes ci-dessus, ne peut être que nul.

LEMME 3.6. *Sous les hypothèses précédentes,* $\tilde{h} = 0$.

Preuve. Soit $b \in E(g, h, 2)$. Soient $(a, a') \in \mathbb{Z}^2$, distincts tels que $\mathrm{C}(g_{a,b}, h_{a,b})$, $\mathrm{C}(g_{a',b}, h_{a',b})$, et il existe $\alpha \in \mathbb{Q}\backslash\{0, 1\}$ tel que $\tilde{h}_{a,b} = \alpha \tilde{h}_{a',b}$. On a

$$\tilde{h}_{a,b} = \sum_{l=0}^{\deg \tilde{h}} \tilde{h}_{(l)}(a, b) X^l = \sum_{l=0}^{\deg \tilde{h}} \left(\sum_{i=0}^{l} \sum_{j \geq i} \tilde{H}_{l-i,j} a^i b^{j-i} C_j^{j-i} \right) X^l.$$

Montrons par récurrence que pour $l \leq \deg \tilde{h}$, on a

$$\forall i \in [0, l], \ \forall j \in [0, \deg \tilde{h} - l], \quad \tilde{H}_{i,j} = 0.$$

Comme pour $i + j > \deg \tilde{h}$, $\tilde{H}_{i,j} = 0$, on prend j dans $[0, \deg \tilde{h}]$.

(1) Pour $l = 0$,

$$\tilde{h}_{(0)}(a, b) = \alpha \tilde{h}_{(0)}(a', b).$$

D'où

$$\sum_{j \geq 0} \tilde{H}_{0,j} b^j = \alpha \sum_{j \geq 0} \tilde{H}_{0,j} b^j.$$

Donc

$$\sum_{j \geq 0} \tilde{H}_{0,j} b^j = 0$$

car $\alpha \neq 1$. Donc pour tout $b \in E(g, h, 2)$, on a

$$\sum_{j \geq 0} \tilde{H}_{0,j} b^j = 0$$

avec $\operatorname{card} E(g, h, 2) > \deg h \geq \deg \tilde{h}$, d'où

$$\forall j \in [0, \deg \tilde{h}], \quad \tilde{H}_{0,j} = 0.$$

(2) Supposons maintenant que pour $l < \deg \tilde{h}$ et pour tout entier $i \in [0, l]$, on ait pour tout entier j de $[0, \deg \tilde{h}]$, $\tilde{H}_{l-i,j} = 0$. On a

$$\tilde{h}_{(l+1)}(a, b) = \sum_{j \geq 0} \tilde{H}_{l+1,j} b^j + \sum_{i=0}^{l} \sum_{j \geq i} \tilde{H}_{l-i,j} a^i b^{j-i} C_j^{j-i} = \sum_{j \geq 0} \tilde{H}_{l+1,j} b^j$$

par hypothèse de récurrence. Mais

$$\tilde{h}_{(l+1)}(a, b) = \alpha \tilde{h}_{(l+1)}(a', b),$$

d'où

$$\sum_{j \geq 0} \tilde{H}_{l+1,j} b^j = 0$$

car $\alpha \neq 1$.

Par un raisonnement analogue au cas $l = 0$, comme $\operatorname{card} E(g, h, 2) > \deg h \geq \deg \tilde{h}$, on a $\tilde{H}_{l+1,j} = 0$ pour tout entier $j \in [0, \deg \tilde{h}]$. Donc pour tout entier $i \in [0, \deg \tilde{h}]$, pour tout entier $j \in [0, \deg \tilde{h}]$, $\tilde{H}_{i,j} = 0$. D'où $\tilde{h} = 0$. □

Le Lemme 3.2 et le Lemme 3.6 permettent d'aboutir à une contradiction car à $b \in E(g,h,2)$ fixé, il y a plus de $\deg h$ entiers a tels que $\mathrm{C}(g_{a,b}, h_{a,b})$ et ainsi il y en a au moins un tel que $h_{a,b} \notin \mathbb{Z}$. Donc, si

$$\operatorname{card} E(g,h,2) > \deg h$$

alors

$$\frac{g}{h} \in \mathbb{Q}[X,Y]. \qquad \square$$

REMARQUE 3.4. Afin de s'affranchir de l'hypothèse 2: $h \notin \mathbb{Z}[X]$, il faut considérer

$$\frac{g_{a,b^1}}{h_{a,b^1}}(Y) = \frac{g}{h}(aY+b, Y),$$

$$\frac{g_{a,b^2}}{h_{a,b^2}}(Y) = \frac{g}{h}(X, aX+b),$$

et, pour $i = 1, 2$,

$$E(g,h,i,2) = \left\{ b \in \mathbb{Z},\ \operatorname{card}\{a \in \mathbb{Z},\ \mathrm{C}(g_{a,b^i}, h_{a,b^i})\} \geq 1 + \deg h (1 + 2^{2\deg g \deg h}) \right\}.$$

REMARQUE 3.5. Les couples (a,b) tels que $h_{a,b} = 0$ sont bel et bien pris en compte, puisque pour chaque entier $b \in E(g,h,i,2)$ il y a strictement plus de $\deg h$ valeurs de a correspondantes.

On peut alors affirmer:

THÉORÈME 3.1. *Soit $g/h \in \mathbb{Q}(X,Y)$, avec g et h dans $\mathbb{Z}[X,Y]$. Si*

$$\operatorname{card} E(g,h,i,2) > \deg h \quad \forall i \in \{1,2\},$$

alors

$$\frac{g}{h} \in \mathbb{Q}[X,Y].$$

Enonçons maintenant un corollaire qui nous sera utile dans la suite du texte:

COROLLAIRE 3.1. *Soit $g/h \in \mathbb{Q}(X,Y)$ avec $\deg h \geq 1$. Supposons que pour tout k suffisamment grand, il y ait plus de $\deg h$ entiers $b \in [-k^{3/2}, k^{3/2}]$, tels que pour chacun d'entre eux, il y ait plus de $1 + \deg h(1 + 2^{2\deg g \times \deg h})$ entiers $a \in [-k^{1/2}, k^{1/2}]$ tels que pour chaque couple (a,b), il y ait plus de $k^{\frac{20(\deg g + \deg h)^2}{\log\log k}}$ points de la forme $\vec{n} = (n, an+b)$ avec $n \in \mathbb{Z}$ tels que $g(\vec{n})/h(\vec{n}) \in \mathbb{Z}$. Supposons la même chose pour les points de la forme $(an+b, n)$. Alors $g/h \in \mathbb{Q}[X,Y]$.*

Preuve. Montrons que pour tout couple $(a,b) \in \mathbb{Z}^2$ tel que cela ait un sens,

$$k^{\frac{20(\deg g + \deg h)^2}{\log\log k}} > M(g_{a,b}, h_{a,b}).$$

Pour cela, posons

$$C = 4^{(\deg g + \deg h)^2} (\deg g + \deg h)! (\deg g + 1)^{(3/2)\deg h} \times (\deg h + 1)^{(3/2)\deg g} |g|^{\deg h} |h|^{\deg g}.$$

Par définition, pour tout $(a, b) \in \mathbb{Z}^2$ tel que cela ait un sens, on a

$$N(g_{a,b}, h_{a,b}) \leq 16 + Ck^{(3/2)d^2},$$

où $d = \deg g + \deg h$ car $\max(|a|, |b|) \leq k^{3/2}$.

Si k est très grand devant 16, on a

$$\sigma(N(g_{a,b}, h_{a,b})) < \sigma(2Ck^{(3/2)d^2})$$

De plus, si $k > 2C^{2/d^2}$, on a

$$\sigma(N(g_{a,b}, h_{a,b})) < \sigma(k^{2d^2}) < 2k^{\frac{2d^2 \times 10}{\log\log k}}.$$

D'où

$$1 + \deg h(1 + \sigma(N(g_{a,b}, h_{a,b}))) < 1 + \deg h\left(1 + 2k^{\frac{2d^2 \times 10}{\log\log k}}\right).$$

D'où le résultat. □

3.1.2. Fractions Rationnelles de $\bar{\mathbb{Q}}(X, Y)$

Le même type d'argument Galoisien que nous avons développé dans la Partie 2.2 nous permet ici d'étendre le résultat du Théorème 3.1 aux fractions rationnelles à deux indéterminées à coefficients algébriques sur $\mathbb{Q}$.

Nous allons utiliser ici les notations du Théorème 2.2 étendues au cas de deux variables, les fonctions symétriques élémentaires en les $(g/h)^\sigma$ où σ est un élément de $\mathbb{G}(g, h)$ seront prises sous la forme $\bar{g}_j/H$, $1 \leq j \leq t$; où

$$H = \prod_\sigma h^\sigma.$$

THÉORÈME 3.2. *Soit $g/h \in \bar{\mathbb{Q}}(X, Y)$. Si*

$$\forall i \in \{1, 2\},\ \forall (1 \leq j \leq t), \quad \operatorname{card} E(\bar{g}_j, H, i, 2) > \deg h,$$

alors $g/h \in \bar{\mathbb{Q}}[X, Y]$.

Preuve. La fraction rationnelle g/h est racine du polynôme,

$$\prod_\sigma \left(Z - \left(\frac{g}{h}\right)^\sigma\right),$$

qui est un polynôme unitaire de $(\bar{\mathbb{Q}}[X, Y])[Z]$. De plus g/h est dans $\bar{\mathbb{Q}}(X, Y)$. Donc $g/h \in \bar{\mathbb{Q}}[X, Y]$. □

De même, en remplaçant $\mathbb{Z}$ par $\bar{\mathbb{Z}}$ dans le Corollaire 3.1:

COROLLAIRE 3.2. *Soit $g/h \in \bar{\mathbb{Q}}(X, Y)$, et posons $\delta = [\mathbb{K}(g, h) : \mathbb{Q}]$. Supposons que pour tout k suffisamment grand devant les hauteurs de g et h, il y ait plus de $\delta \deg h$ entiers $b \in [-k^{3/2}, k^{3/2}]$, tels que pour chacun d'entre eux, il y ait plus de $1 + \delta \deg h(1 + 2^{2\delta \deg g \times \deg h})$ entiers $a \in [-k^{1/2}, k^{1/2}]$ tels que pour chaque couple (a, b), il y ait plus de $k^{\frac{20\delta^2(\deg g + \deg h)^2}{\log\log k}}$ points de la forme $\vec{n} = (n, an + b)$ avec*

$n \in \mathbb{Z}$ tels que $g(\vec{n})/h(\vec{n}) \in \bar{\mathbb{Z}}$. Supposons la même chose pour les points de la forme $(an+b, n)$. Alors $g/h \in \bar{\mathbb{Q}}[X, Y]$.

Preuve. Il suffit d'appliquer le Théorème 3.2 en ayant remarqué que

$$k^{\frac{20\delta^2(\deg g+\deg h)^2}{\log\log k}} > \max_j M(\bar{g}_{j_{a,b}}, H_{a,b}),$$

dès que $\bar{g}_{j_{a,b}}/H_{a,b}$ a un sens, car $\deg \bar{g}_{j_{a,b}} \leq \delta \deg g$ et $\deg H_{a,b} \leq \delta \deg h$. □

3.2. Amélioration du Critère de Yasumoto

Grâce aux majorations de la Partie 3.1, nous allons maintenant démontrer le résultat annoncé sur l'amélioration du texte de Yasumoto [9]. Nous aurons besoin de la notation suivante.

LEMME 3.7. *Soit $\eta > 1$. Soit E un sous-ensemble de $\mathbb{Z}^2$ tel que*

$$\limsup \frac{\operatorname{card} E_k}{k^\eta} > 0.$$

Soit $t \geq 1$, un entier. Notons $\tilde{E}(t)$ un ensemble formé de E auquel on enlève les points placés sur t droites. Alors

$$\limsup \frac{\operatorname{card} \tilde{E}(t)_k}{k^\eta} = \limsup \frac{\operatorname{card} E_k}{k^\eta}.$$

Preuve. Pour chaque k, on enlève au plus $t(2k+1)$ points. Le nombre de points enlevés devient négligeable devant le nombre de points restants. D'où le résultat. □

La démonstration du Théorème 1.2 repose en majeure partie sur les démonstrations des Lemmes 3.7 et 3.8, qui vont montrer que pour tout k suffisamment grand, toute fraction rationnelle à coefficients rationnels prenant des valeurs entières sur tout E vérifie les conditions imposées par le Corollaire 3.1 avec un $\varepsilon > \frac{20(\deg g+\deg h)^2}{\log\log k}$. Soit un réel $\varepsilon > 0$.

LEMME 3.8. *Soit g la fonction de variable entière positive à valeurs entières positives définie par*

$$g\colon \mathbb{N} \to \mathbb{N} \quad et \quad k \mapsto g(k) = 12[k^{1/2+\varepsilon}].$$

Si pour une infinité de valeurs de k, $\operatorname{card} E_k \geq kg(k)$, alors pour tout $(t,u) \in \mathbb{N}^2$ non nuls et pour tout k suffisamment grand tel que $\operatorname{card} E_k \geq kg(k)$, il y a plus de t valeurs d'entiers b telles qu'il y ait pour chacune d'entre elles plus de u valeurs d'entiers a telles que pour tout couple (a,b) il y ait plus de k^ε points de la forme $\vec{n} = (n, an+b)$ dans E.

Preuve. Soit $k \in \mathbb{N}$ tel que $\operatorname{card} E_k \geq kg(k)$, et soit un entier $a \in [1, k^{1/2}]$. Donc E_k est recouvert par les droites d'équation $Y = aX + b$ où $-(a+1)k \leq b \leq (a+1)k$. Chacune de ces droites contient au plus $(2k+a)/a$ points de coordonnées inférieures à k.

Soit l'application $h\colon \mathbb{N} \to \mathbb{N}$ arbitraire pour l'instant. Notons $N_a(k)$ le nombre de droites de la forme $Y = aX + b$ contenant plus de $h(k)$ points de E_k. On a donc

$$\operatorname{card} E_k \leq N_a(k)\frac{2k+a}{a} + h(k)(2(a+1)k+1)$$

d'où

$$kg(k) \leq N_a(k)\frac{2k+a}{a} + h(k)(2(a+1)k+1).$$

Supposons $g(k) \geq 2h(k)(2(a+1) + 1/k)$. On a alors

$$kg(k) \geq 2h(k)(2(a+1)k+1).$$

D'où

$$\begin{aligned} N_a(k) &\geq \frac{a}{2k+a}h(k)(2(a+1)k+1) \\ &\geq \frac{a}{2k+a}h(k)2ak + ah(k) \geq a^2h(k)\frac{2k}{2k+k^{1/2}} \\ &\geq a^2h(k) \end{aligned}$$

cela pour tout entier $a \in [1, k^{1/2}]$.

Soit $N(k)$ le nombre de droites de la forme $Y = aX + b$, a variant dans $[1, k^{1/2}]$, contenant plus de $h(k)$ points de E_k; alors

$$N(k) \geq h(k)\sum_{j=1}^{[k^{1/2}]} j^2$$

d'où

$$N(k) \geq h(k)\frac{[k^{1/2}]([k^{1/2}]+1)(2[k^{1/2}]+1)}{6} \geq h(k)\frac{k^{3/2}}{4}.$$

Mais pour toutes les droites de la forme $Y = aX + b$ avec a entier dans $[1, k^{1/2}]$, il y a au plus $2([k^{1/2}]+1)k+1$ valeurs distinctes de b.

Soit un couple d'entiers $(t, u) \in (\mathbb{N}\setminus\{0\})^2$. On prend $h(k) = k^\varepsilon$, on vérifie que

$$12[k^{1/2+\varepsilon}] \geq 2k^\varepsilon\left(2(a+1) + \frac{1}{k}\right).$$

Mais dès que $k^\varepsilon > (4u+1)$, il existe $b_0 \in \mathbb{Z}$ tel que l'on ait plus de u entiers a tels qu'il y ait plus de k^ε points sur la droite $Y = aX + b_0$. Sinon pour tout entier b il y aurait moins de u valeurs de a et alors $N(k) < k^{3/2}u$, d'où la contradiction.

Considérons maintenant $\tilde{E}(u)$ l'ensemble formé de E privé de u droites parmi celles définies ci-dessus pour le même entier b_0; $\tilde{E}(u)$ vérifie les mêmes hypothèses que E d'après le Lemme 3.7. On peut donc répéter le même raisonnement que ci-dessus en remplaçant E par $\tilde{E}(u)$, on obtient alors un nouvel entier b_1 pour lequel on a le même résultat. En renouvelant l'opération t fois, il y a plus de t valeurs de d'entier b telles qu'il y ait plus de u valeurs d'entiers a telles que pour tout couple (a, b) il y ait plus de k^ε valeurs d'entiers n tels que $(n, an+b) \in E$ ce pour tout couple (t, u). $\square$

Il ne nous reste plus qu'à terminer la démonstration du Théorème 1.2.

Preuve. L'hypothèse

$$\limsup_{k\to\infty} \frac{\operatorname{card} E \cap \{(m,n) \in \mathbb{Z}^2,\ -k \le m, n \le k\}}{k^{3/2+\varepsilon}} > 0$$

entraîne, grâce au Lemme 3.8, que les fractions rationnelles à coefficients entiers qui prennent des valeurs entières sur tout E vérifient les conditions du Corollaire 3.1 et sont en fait des polynômes. □

On a donc démontré le résultat de l'article de Yasumoto [9] avec k^2 remplacé par $k^{3/2+\varepsilon}$ dans le cas des fractions rationnelles à deux variables. On essaiera par la suite de revenir aux cas des dimensions supérieures en utilisant la même méthode, et d'affiner le résultat de l'article de Yasumoto [9].

3.3. Ensembles de Densité Suffisante ou Non

Cette dernière partie va tenter de donner une idée plus précise des réponses à apporter à la Question 1.1, en donnant quelques sous-ensembles de $\mathbb{Z}^2$ sur lesquels une fraction rationnelle ne peut pas prendre que des valeurs entières sans être un polynôme. Nous donnerons aussi quelques exemples à la limite du résultat pour, en quelque sorte, minorer la taille de ces ensembles idéaux qui restent à définir. Nous allons, tout d'abord donner un corollaire au Corollaire 3.1.

COROLLAIRE 3.3. *Soit $E \subset \mathbb{Z}^2$, contenant des points de la forme $(n, an+b)$ et $(an+b, n)$ avec a, b, n dans $\mathbb{Z}$, où pour tout couple $(t, u) \in \mathbb{Z}^2$, il y a plus de t valeurs de b pour lesquelles il y a plus de u valeurs de a telles que pour tout couple (a, b) il y a une infinité de points $(n, an+b)$ et $(an+b, n)$ dans E. Alors, pour toute $f \in \mathbb{Q}(X, Y)$,*

$$\forall \vec{n} \in E, \quad f(\vec{n}) \in \mathbb{Z} \Rightarrow f \in \mathbb{Q}[X, Y].$$

Preuve. Soit $f \in \mathbb{Q}(X, Y)$, avec $f = g/h$ et g et h sans facteur commun, telle que $f(\vec{x}) \in \mathbb{Z}$ pour tout $\vec{x} \in E$. Considérons $b_0, \ldots, b_{\deg h}$ des entiers tels que pour chacun d'entre eux il existe plus de $1 + \deg h(1 + 2^{2\deg g \deg h})$ entiers a_{b_i} tels que pour chaque couple (a_{b_i}, b_i) il y ait une infinité de points du type $(n, a_{b_i}n + b_i)$ et $(a_{b_i}n + b_i, n)$ dans E. Alors,

$$\forall j \in \{1, 2\},\ \forall b_i,\ \forall a_{b_i},$$
$$\operatorname{card}\{n \in \mathbb{Z},\ f_{(a_{b_i}, b_i)^j}(n) \in \mathbb{Z}\} \ge M(g_{(a_{b_i}, b_i)^j}, h_{(a_{b_i}, b_i)^j})$$

d'où card $E(g, h, j, 2) \ge \deg h + 1 > \deg h$ pour $j \in \{1, 2\}$ et donc $f \in \mathbb{Q}[X, Y]$ d'après le Théorème 3.1. □

Nous appelerons $\mathbb{E}$ l'ensemble des ensembles $E \subset \mathbb{Z}^2$ qui vérifient les conditions du Corollaire 3.3.

3.3.1. Cas des Progressions Arithmétiques

PROPOSITION 3.2. *Soit $E \subset \mathbb{Z}^2$, un ensemble rencontrant toute progression arithmétique, alors $E \in \mathbb{E}$.*

Preuve. Par hypothèse, on a

$$\forall (a_1, a_2, b_1, b_2) \in \mathbb{Z}^4, \quad \exists n \in \mathbb{Z} \text{ tel que } (a_1 n + b_1, a_2 n + b_2) \in E.$$

Soit $(a, b) \in \mathbb{Z}^2$. Il existe m et n dans $\mathbb{Z}$ tels que $(m, am + b)$ et $(an + b, n)$ soient dans E. Avec

$$(a_1, a_2, b_1, b_2) = \begin{cases} (1, m, a, b + ma), \\ (a, b + na, 1, n), \end{cases}$$

on a l'existence de m' et n' tels que $(m+m', a(m+m')+b)$ et $(a(n+n')+b, n+n')$ soient dans E. Donc, il existe une infinité d'entiers $m \in \mathbb{Z}$ et une infinité d'entiers $n \in \mathbb{Z}$ tels que

$$(m, am + b) \in E \quad \text{et} \quad (an + b, n) \in E.$$

Donc $E \in \mathbb{E}$. □

3.3.2. Ensembles de Densité Banachique Nulle

PROPOSITION 3.3. *Il existe des sous-ensembles $E \subset \mathbb{Z}^2$ tels que*

(i) $\mathrm{d}(E) = 0$ *et*
(ii) *E contient un élément de $\mathbb{E}$.*

Preuve. Considérons

$$E = \{(2^a, 3^b 2^a + 5^c),\ (a, b, c) \in \mathbb{N}^3\} \cup \{(3^b 2^a + 5^c, 2^a),\ (a, b, c) \in \mathbb{N}^3\}.$$

On a

$$\operatorname{card}(E \cap \{(m, n) \in \mathbb{Z}^2,\ -k \le m, n \le k\}) = \mathrm{O}((\log k)^3);$$

donc $\mathrm{d}(E) = 0$ et pourtant E contient un élément de $\mathbb{E}$ et vérifie ainsi les conditions du Corollaire 3.3. □

REMARQUE 3.6. En prenant $2^{2^{\cdot^{\cdot^{2^a}}}}$ (w fois) à la place de 2^a, on arrive même à:

$$\operatorname{card}(E \cap \{(m, n) \in \mathbb{Z}^2,\ -k \le m, n \le k\}) = \mathrm{O}((\log \ldots \log k)^3) \quad (w - 1 \text{ fois})$$

REMARQUE 3.7. Cet exemple est inspiré d'un résultat de Lewis et Morton [2], résultat que l'on peut retrouver aussi dans le livre de Narkiewicz [4] sur les fractions rationnelles à plusieurs variables à la Remarque 3 du Chapitre VIII. Ce résultat s'écrit en deux variables de la façon suivante:

> Soit m, n deux entiers premiers entre eux sur $\mathbb{Z}$. Soit $f \in \mathbb{Q}(X, Y)$. Si pour toutes les valeurs de $k \in \mathbb{Z}$ telles que $f(m^k, n^k)$ existe, ce nombre est un entier de $\mathbb{Z}$ alors $f \in \mathbb{Q}[X, Y]$.

Mais la méthode utilisée dans le présent texte ne permet pas, a priori, de conduire à ce résultat.

3.3.3. Ensembles de Densité Banachique 1 sans Infinité de Points sur les Droites

Dans cette partie nous utiliserons les notations suivantes, qui définissent de nouveaux ensembles de droites et de points de $\mathbb{Z}^2$.

NOTATION 3.3. Nous considérons ici les ensembles $\mathbb{Z}_k^2$.

(i) Notons $\mathcal{D}_k$ l'ensemble des droites de $\mathbb{Z}^2$ qui joignent au moins deux points de $\mathbb{Z}_k^2$:

$$\mathcal{D}_k = \{\Delta : aX + bY + c = 0,\ (a, b, c) \in \mathbb{Z}^3,\ \mathrm{card}(\mathbb{Z}_k^2 \cap \Delta) \geq 2\}.$$

(ii) Posons, enfin, $\mathcal{P}_k$ l'ensemble des points de $\mathbb{Z}^2_{(k+1)^8-1} \backslash \mathbb{Z}^2_{k^8}$ qui se trouvent sur une droite de $\mathcal{D}_k$:

$$\mathcal{P}_k = \{\vec{n} \in \mathbb{Z}^2_{(k+1)^8-1} \backslash \mathbb{Z}^2_{k^8},\ \exists(\Delta \in \mathcal{D}_k,\ \vec{n} \in \Delta)\}.$$

Par construction, si une droite Δ est dans $\mathcal{D}_k$, elle est dans $\mathcal{D}_i$ pour tout $i \geq k$. Donc, pour tout $i \geq k$, $\Delta \cap (\mathbb{Z}^2_{(i+1)^8-1} \backslash \mathbb{Z}^2_{i^8}) \subset \mathcal{P}_i$.

LEMME 3.9.

$$\begin{aligned}\mathrm{card}\, \mathcal{D}_k &= 12k + 4 \sum_{i=2}^{k} \sum_{\substack{j<i \\ j \wedge i = 1}} [(2k+1-j)i + (2k+1-2i)j] \\ &\quad + 4 \sum_{i=k+1}^{2k} \sum_{\substack{j<i \\ j \wedge i = 1}} (2k+1-j)(2k+1-i) \\ &= \mathrm{O}(k^4).\end{aligned}$$

Preuve. Soit i, j dans $\mathbb{Z}$, et soit $jY = iX + c$ une droite de $\mathcal{D}_k$. Comme la pente de ces droites est fixée, ici i/j, il suffit pour les compter de compter les points les plus en bas à gauche par lesquels elles passent.

(1) Regardons d'abord ce qui se passe pour les points les plus bas du carré $\mathbb{Z}_k^2$. Une et une seule de chacune de ces droites passe par un point du type $(x, -k)$ où $-k \leq x \leq k - j$; cette même droite passe par $(x, -k + i)$, qui est le premier point au dessus de $(x, -k)$. Il y a donc $(2k+1-j)i$ droites distinctes si $i \leq k$ et $(2k+1-j)(2k+1-i)$ si $i \geq k+1$.

(2) Regardons maintenant les points les plus à gauche du carré $\mathbb{Z}_k^2$. Pour $i \geq k+1$, il n'y a plus aucun point à atteindre. D'autre part, pour $i \leq k$, une et une seule de ces droites passe par un point du type $(-k, y)$ où $-k \leq y \leq k - i$. Or pour ne pas recompter les droites déjà considérées, il convient de prendre $-k+i \leq y \leq k - i$. D'autre part ces droites passent aussi par les points $(-k + j, y)$; il y en donc au total $(2k+1-2i)j$.

Montrons maintenant que card $\mathcal{D}_k = \mathrm{O}(k^4)$. On a

$$\begin{aligned}\operatorname{card}\mathcal{D}_k &= 12k + 4\sum_{i=2}^{k}\sum_{\substack{j<i\\ j\wedge i=1}}((2k+1)(j+i)-3ij)\\ &\quad + 4\sum_{i=2}^{k}\sum_{\substack{j<i\\ j\wedge i=1}}((2k+1)^2-(2k+1)(i+j)+ij)\\ &\le 12k + 4(k-1)(k-1)(2k+1)(k-1+k)\\ &\quad + 4k\times 2k[(2k+1)^2+(2k-1)\times 2k]\\ &= 80k^4 - 16k^3 + 20k^2 + 20k - 4.\end{aligned}$$

Donc, pour $k \ge 2$, card $\mathcal{D}_k \le 80k^4 = \mathrm{O}(k^4)$. D'où le résultat. □

La Proposition 3.3 montre que les sous-ensembles de $\mathbb{Z}^2$ qui remplissent les conditions du Corollaire 3.3 ne sont pas nécessairement de densité Banachique positive stricte; le résultat suivant va établir que les ensembles de densité Banachique positive stricte ne remplissent pas nécessairement les conditions du Corollaire 3.3.

PROPOSITION 3.4. *Il existe des sous-ensembles $E \subset \mathbb{Z}^2$ tels que*

(i) $\mathrm{d}(E) = 1$ *et*
(ii) $E \notin \mathbb{E}$.

L'idée de l'exemple détaillé dans la démonstration suivante a été donnée par Omer Adelman.

Preuve. Posons

$$E = \bigcup_{k\in\mathbb{N}} \mathbb{Z}_k^2 \backslash \mathcal{P}_{[k^{1/8}]}.$$

La démonstration de la Proposition 3.4 consiste à vérifier que E est un sous-ensemble de $\mathbb{Z}^2$ tel que:

(a) $\mathrm{d}(E) = 1$;
(b) sur chacune des droites passant par deux points distincts de E, on ne trouve qu'un nombre fini de points de $\mathbb{Z}^2$, donc de E;
(c) montrons que la deuxième condition est réalisée.

Soient $M_1 = (x_1, y_1)$ et $M_2 = (x_2, y_2)$ dans E. Regardons les points qui se trouvent sur la droite (M_1, M_2). Il existe k tel que M_1, M_2 soient dans $\mathbb{Z}_k^2$, donc (M_1, M_2) est dans $\mathcal{D}_i$ pour tout $i \ge k$; ainsi les points de (M_1, M_2) sont dans $\mathcal{P}_i$ pour $i \ge k$. Donc,

$$E \cap (M_1, M_2) \subset \mathbb{Z}_{k^8}^2;$$

la deuxième condition est bien réalisée.

Regardons maintenant $\mathrm{d}(E)$, on a

$$E_k = \mathbb{Z}_k^2 \setminus \Big(\bigcup_{j \le k} \mathcal{P}_{[j^{1/8}]} \Big).$$

Or il y a, au plus $2k+1$ points de $\mathbb{Z}_k^2$ sur chacune des droites de $\mathcal{D}_{[k^{1/8}]}$. Donc

$$\operatorname{card} \bigcup_{j \le k} \mathcal{P}_{[j^{1/8}]} \le (2k+1) \operatorname{card} \mathcal{D}_{[k^{1/8}]} = \mathrm{O}(kk^{1/2}).$$

Donc

$$\frac{\operatorname{card} E_k}{(2k+1)^2} = \frac{(2k+1)^2 - \mathrm{O}(kk^{1/2})}{(2k+1)^2} = 1 - \mathrm{o}(k^{-1/2}).$$

D'où $\mathrm{d}(E) = 1$.

Donc E répond bien aux deux conditions, il s'agit d'un ensemble de densité Banachique égale à 1, qui n'a sur aucune droite une infinité de points. □

3.3.4. Critères sur la Densité Banachique: Amélioration de l'Exposant de k

L'exemple suivant indique qu'on ne peut pas remplacer l'exposant $\frac{3}{2} + \varepsilon$ par 1 dans le Théorème 1.2.

Proposition 3.5. *Il existe $f \in \mathbb{Q}(X, Y)$ telle que*:

(i) *pour* $A = \{\vec{n} \in \mathbb{Z}^2,\ f(\vec{n}) \in \mathbb{Z}\}$, $\operatorname{card} A_k \sim k \log k$;

(ii) $f \notin \mathbb{Q}[X, Y]$.

Preuve. Considérons $f(X, Y) = X/Y$. Soit

$$A = \bigcup_{(\alpha, m) \in \mathbb{Z}^2} \{(\alpha m, m)\};$$

alors

$$A_k = \bigcup_{|m| \le k,\ 0 \le |\alpha| \le [k/|m|]} \{(\alpha m, m)\}.$$

On a donc

$$\operatorname{card} A_k \sim (2k+1)\Big(2 \sum_{i=1}^{k} \frac{1}{i}\Big) \sim 2(2k+1) \log k.$$

On a bien pour tout $(m, n) \in A$, $f(m, n) \in \mathbb{Z}$ mais pour autant $f \notin \mathbb{Q}[X, Y]$. □

Ceci montre bien que la quantité d'entiers, sur lesquels une fraction rationnelle prend tellement de valeurs entières qu'elle est nécessairement un polynôme, doit être plus importante que $\mathrm{O}(k \log k)$.

Références

[1] S. Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, New York, 1983.

[2] D. J. Lewis and P. Morton, *Quotients of polynomials and a theorem of Pisot and Cantor*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28 (1982), 813–822.

[3] K. Mahler, *On some inequalities for polynomials in several variables,* J. London Math. Soc. (2) 37 (1962), 341–344.
[4] W. Narkiewicz, *Polynomial mappings,* Lecture Notes in Math., 1600, pp. 61–66, Springer-Verlag, Berlin, 1995.
[5] A. Schinzel, *Selected topics on polynomials,* University of Michigan Press, Ann Arbor, 1982.
[6] G. Tenenbaum, *Cours de théorie analytique des nombres,* Université de Bordeaux I, U.E.R. de Mathématiques et d'Informatique, Laboratoire de Théorie des Nombres, Talence, 1979.
[7] M. Waldschmidt, *Nombres transcendants,* Lecture Notes in Math., 402, Springer-Verlag, Berlin, 1974.
[8] ———, *Integer valued entire functions on Cartesian products,* Number theory in progress, vol. I (Zakopane-Kościelisko, 1997), pp. 553–576, de Gruyter, Berlin, 1999.
[9] M. Yasumoto, *Arithmetically independent integers and values of rational functions,* Manuscripta Math. 85 (1994), 1–10.

Institut de Mathématiques
Équipe de Théorie des Nombres
4 place Jussieu, case 247
75252 Paris Cedex 05
France

masseron@math.jussieu.fr