Université Paris 7 – Denis Diderot
UFR de Mathématiques

Mémoire de Master 2

Sous la direction de Marc Hindry

Un exemple d'application de techniques d'approximation diophantienne :

l'équation $ax^n - by^n = 1$

Lionel Ponton
lionel.ponton@gmail.com

Janvier 2013

Table des matières

Préambule

Ce mémoire a été rédigé dans le cadre du Master 2 de mathématiques parcours « Enseignants » proposé par l'Université Paris 7 – Denis Diderot.

Lorsque j'ai contacté le professeur Marc Hindry pour lui faire part de mon souhait de travailler sur un sujet d'arithmétique, il m'a immédiatement répondu de façon positive. Il m'a laissé une grande liberté dans le choix de mon sujet et, suite à notre discussion, m'a proposé d'étudier l'article de Bennett [5] qui fait l'objet du chapitre 5 de ce mémoire. Quand je lui ai proposé d'élargir le sujet au-delà des cas traités par Bennett, Marc m'a soutenu et encouragé dans cette voie.

Pour son accueil et sa disponibilité, je tenais à le remercier très sincèrement.

Au final, le présent travail tente de faire la synthèse des principaux travaux utilisant des techniques d'approximation diophantienne et qui ont conduit à montrer que l'équation donnée en titre admet au plus une solution non triviale pour $n \geq 3$. Pour l'essentiel, il s'agit des articles d'Evertse [13], Bennett et de Weger [6] et, bien sûr, l'article [5] de Bennett. Certains cas ne sont pas étudiés ici car ils s'appuient sur des techniques algébriques. Nous les abordons en quelques mots dans l'introduction.

Ce mémoire ne contient pas de résultats fondamentalement nouveaux mais il propose, cependant, quelques améliorations à certaines propriétés déjà établies. En particulier,

- dans le chapitre 1, une étude complète de l'équation $ax^2 - by^2 = 1$ est proposée avec notamment un algorithme permettant d'étudier l'existence de solutions et, le cas échéant, de déterminer les premières solutions (théorème 1.3.14) [(1)]
- les constantes proposées par Evertse ([13], théorème 2.1) ont été améliorées (de façon très nette dans les cas $n = 3$ et $n = 4$) lorsque $c = 1$ (théorème 3.1.1) ;
- quelques résultats élémentaires du chapitre 4 permettent d'intégrer le cas $b = 1$ ainsi que le cas $n = 347$ à l'étude proposée par Bennett et de Weger ([6], théorème 4.1.2), ce qui n'était pas le cas dans l'article original. De plus, l'amélioration des constantes d'Evertse permet d'utiliser directement la méthode décrite par Bennett et de Weger sans avoir à faire appel à d'autres résultats d'approximation diophantienne sauf pour quelques valeurs de b et de n.

Lionel Ponton
Janvier 2013

(1). Si les équations de Pell-Fermat sont largement étudiées dans la plupart des ouvrages de théorie des nombres, l'équation $ax^2 - by^2 = 1$ n'est que très rarement abordée et je n'ai trouvé aucune référence en proposant la résolution complète. Si les résultats proposés n'ont nullement la prétention d'être originaux, ils sont, en tout cas, le fruit d'une recherche personnelle.

Notations

- (E_n) désigne l'équation $ax^n - by^n = 1$ où a, b et n sont des entiers naturels non nuls.
- (F_n) désigne l'équation $(b+1)x^n - by^n = 1$ où b et n sont des entiers naturels non nuls.
- (PF_d) désigne l'équation de Pell-Fermat $x^2 - dy^2 = 1$ (avec d entier).
- $(PF_{d,m})$ désigne l'équation de Pell-Fermat généralisée $x^2 - dy^2 = m$ (avec d et m des entiers premiers entre eux).
- $\lfloor x \rfloor$ désigne la partie entière d'un réel x i.e. l'unique entier k tel que $k \leq x < k+1$.
- $\{x\}$ désigne la partie fractionnaire d'un réel x i.e. $\{x\} := x - \lfloor x \rfloor$.
- $\alpha = [a_0, a_1, ..., a_n, ...]$ désigne le développement en fraction continuée d'un irrationnel α (voir la notation 1.1.6).
- $\alpha = [a_0, a_1, ..., a_{N-1}, \overline{a_N, a_{N+1}, ..., a_{N+T-1}}]$ désigne un développement en fraction continuée périodique à partir du rang N pour un irrationnel quadratique α (voir la notation 1.1.12).
- deg$P$ désigne le degré d'un polynôme P.
- ord(f) désigne l'ordre d'une fonction analytique en 0 (voir la notation 2.1.1).
- f_ω désigne la fonction définie pour tout $z \in]-\infty\,;1[$ par $f_\omega(z) = (1-z)^\omega$ où ω est un réel.
- $A_k\left(z \,\middle|\, \begin{matrix} \omega_1 & \cdots & \omega_m \\ \rho_1 & \cdots & \rho_m \end{matrix}\right)$ et $R\left(z \,\middle|\, \begin{matrix} \omega_1 & \cdots & \omega_m \\ \rho_1 & \cdots & \rho_m \end{matrix}\right)$ désignent respectivement le $k-$ième polynôme en z et la fonction reste associée à une famille de $[\rho_1 - 1, \rho_2 - 1, ..., \rho_m - 1]$ approximants de Padé d'un système de fonctions binomiales $(f_{\omega_k})_{k \in [\![1,m]\!]}$ où ω_1, ω_2, ..., ω_m sont des réels (voir (2.1)).
- $\mathcal{C} = \mathcal{C}(]-\infty\,;1[\,, \mathbb{R})$ est l'ensemble des fonctions continues définies sur $]-\infty\,;1[$ et à valeurs dans $\mathbb{R}$.
- J^n et J^ρ_α : voir la notation 2.2.1.
- Γ désigne la fonction Gamma d'Euler définie pour tout réel $x > 0$ par $\Gamma(x) = \displaystyle\int_0^{+\infty} t^{x-1}\mathrm{e}^{-t}\,\mathrm{d}t$ qu'on peut prolonger à $\mathbb{C}$ privé des entiers négatifs ou nuls par $\Gamma(z) = \displaystyle\lim_{n\to+\infty} \frac{n!n^z}{z(z+1)\cdots(z+n)}$. En particulier, $\Gamma(k) = (k-1)!$ pour tout $k \in \mathbb{N}^*$.
- $\binom{z}{k} = \dfrac{z(z-1)\cdots(z-k+1)}{k!} = \dfrac{\Gamma(z+1)}{\Gamma(k+1)\Gamma(z-k+1)}$ pour $z \in \mathbb{C} \setminus \mathbb{Z}$ et $k \in \mathbb{N}$.
- PGCD(r,t) désigne le plus grand diviseur commun des entiers non nuls r et t.
- δ_r est le nombre rationnel $(r+1)\binom{r+\frac{1}{n}}{r+1}\binom{r-\frac{1}{n}}{r} n^r \mathrm{PGCD}(n^r, r!)$ pour des entiers $r \geq 1$ et $n \geq 3$. (voir (3.4)).
- $v_p(x)$ est la *valuation $p-$adique* d'un rationnel x pour un nombre premier p i.e. $v_p(x)$ est la puissance de p dans la décomposition de x en produit de facteurs premiers si x est entier et, si r et t sont des entiers, on pose $v_p\left(\frac{r}{t}\right) = v_p(r) - v_p(t)$.

- $\Phi_{m,n,r} := \max\left\{\frac{n^2}{n-1}r^{\frac{1}{n}}, \frac{n^2}{(m-1)(n-m+1)}r^{\frac{m-1}{n}}\right\}$ où m, n et r sont des entiers tels que $n > m \geq 2$ et $r \geq 1$ (voir la proposition 5.3.3).
- $\Delta_{m,n,r}$ est le quotient du P.P.C.M. des dénominateurs des coefficients de tous les A_{ij} par le P.G.C.D. des numérateurs de ces mêmes coefficients (les polynômes A_{ij}, qui dépendent des entiers n, m et r, étant définis par (5.5) p. 81).
- $\Omega_{m,n,r} := \max\{\sqrt{nr+n+m}, 2n\}$ où m, n et r sont des entiers tels que $n > m \geq 2$ et $r \geq 1$ (voir (5.16)).
- $d_{a,\mu} := \min\limits_{1\leq k\leq m}(t_{k+\mu} - t_k)$ où les t_k sont définis par (5.17) (voir (5.33)).
- $\theta(x,n,a) = \sum\limits_{\substack{p\leq x\\ p\equiv a\ [n]}} \ln p$ où la somme porte sur les nombres premiers p congrus à a modulo n et inférieurs ou égaux à x (avec a et n entiers naturels non nuls).
- $\pi(x)$ désigne le nombre de nombres premiers inférieurs ou égaux au nombre réel x.
- $L(s,\chi) := \sum\limits_{u=1}^{+\infty}\frac{\chi(u)}{u^s}$ est la série de Dirichlet associée au caractère χ.
- $\pi(x,n,a)$ désigne le nombre de nombres premiers $p \equiv a\ [n]$ tels que $p \leq x$ ($x \in \mathbb{R}$).

Introduction

L'objet de ce mémoire est l'étude du nombre de solutions de l'équation diophantienne

$$(E_n) : ax^n - by^n = 1$$

où n, a et b sont des entiers naturels non nuls et les inconnues x et y sont des entiers naturels. Ainsi, dans toute la suite, « (x, y) est une solution de (E_n) » signifiera « (x, y) est un couple d'entiers naturels tels que $ax^n - by^n = 1$ ». Par ailleurs, il est immédiat qu'une condition nécessaire pour que (E_n) admette des solutions est que a et b soient premiers entre eux. On fera donc dans toute la suite cette hypothèse.

Lorsque $a = 1$, (E_n) admet une solution évidente qui est $(x, y) = (1, 0)$. Nous appellerons, dans ce cas, cette solution la solution triviale de (E_n)

On remarquera également que (x, y) est solution de $bx^n - ay^n = -1$ si et seulement si (y, x) est solution de (E_n) donc on peut généraliser sans difficulté les résultats obtenus pour (E_n) à l'équation $|ax^n - by^n| = 1$.

Si n est un entier composé et k est un diviseur strict de n i.e. si on peut écrire $n = kd$ avec k et d compris entre 2 et $n - 1$ et si (x, y) est une solution de (E_n) alors $a(x^d)^k - b(y^d)^k = ax^n - by^n = 1$ donc $\left(x^d, y^d\right)$ est une solution de (E_k). Ainsi, toute solution de (E_n) fournit une solution de (E_k) et donc le nombre de solutions de (E_n) est borné par le nombre de solutions de (E_k). En particulier, pour montrer que (E_n) n'a qu'une seule solution, il suffit de montrer que (E_k) n'a qu'une seule solution, ce qui permettra de se restreindre, lorsque ce sera nécessaire, aux cas où n est nombre premier impair ou $n = 4$. On ne peut pas cependant se restreindre aux seuls nombres premiers car on verra que le cas $n = 2$ est très différent des cas n premiers impairs.

Plus précisément, l'équation (E_1) admet toujours une infinité de solutions [(2)]. Sa résolution s'appuie sur l'algorithme d'Euclide, le théorème de Bézout et le lemme de Gauss [(3)]. Pour l'équation (E_2), les choses sont déjà un peu moins simples. Un cas particulier important et largement abordé dans la littérature est l'équation de Pell-Fermat qui correspond à $(a, b) = (1, d)$ où d est un entier non carré. Ces équations ont toujours une infinité de solutions. Il existe plusieurs façons de le voir dont deux sont classiques : utiliser le principe des tiroirs pour montrer le théorème de Dirichlet ou utiliser le développement en fraction continuée des nombres irrationnels quadratiques (i.e. les nombres irrationnels qui sont racines de trinômes du second degré à coefficients entiers). Cette deuxième méthode à l'avantage de s'étendre aux équations de Pell-Fermat généralisées et de donner un critère de résolution de l'équation (E_2) dont l'ensemble des solutions est soit vide soit infini. Les deux approches évoquées de l'équation de Pell-Fermat présentent une différence fondamentale : le théorème de Dirichlet est *non effectif* en ce sens qu'il permet d'assurer l'existence d'une solution fondamentale mais sans la donner explicitement (méthode *explicite*) ni même donner une algorithme permettant de la calculer (méthode *effective*) contrairement à l'utilisation des fractions continuées qui permet d'obtenir un résultat *effectif*.

Avec ces équations et cette double approche, on aborde les premiers aspects de l'approximation diophantienne.

(2). Avec, évidemment, l'hypothèse $\mathrm{PGCD}(a, b) = 1$.

(3). Nous donnons, dans le chapitre 1, une méthode de résolution qui s'appuie sur les fractions continuées mais qui fait appelle, à bien y regarder, aux mêmes « ingrédients ».

L'objet de l'approximation diophantienne est l'étude de l'approximation des nombres réels par les nombres rationnels. On sait évidemment que $\mathbb{Q}$ est dense dans $\mathbb{R}$ et qu'il est donc possible d'approcher tout réel x par un rationnel $r = \frac{p}{q}$ avec une précision arbitrairement petite. Cependant, cette précision a un « prix » qui est la taille des nombres entiers p et q. L'approximation diophantienne s'intéresse plus particulièrement au lien entre la précision $|x - r|$ de l'approximation et le dénominateur q du rationnel r. On considère traditionnellement que l'acte fondateur de l'approximation diophantienne est le théorème suivant dû à Liouville [4] :

Théorème de Liouville (1844). — Soit $\theta \in \mathbb{R}$ un nombre algébrique irrationnel. Alors, il existe une constante explicite K telle que, pour tout nombre rationnel $\frac{p}{q}$ tel que $q > 0$,

$$\left|\theta - \frac{p}{q}\right| \geq \frac{1}{Kq^n}.$$

La démonstration de ce théorème est très simple. Considérons un rationnel $r = \frac{p}{q}$ tel que $p \in \mathbb{Z}$ et $q \in \mathbb{N}^*$.

Si $\left|\theta - \frac{p}{q}\right| > 1$ alors évidemment $\left|\theta - \frac{p}{q}\right| > \frac{1}{q^n}$.

Sinon, notons P le polynôme minimal sur $\mathbb{Q}$ de θ. Comme θ est de degré n, P est un polynôme de degré n à coefficient rationnels. Soit k le P.P.C.M. des dénominateurs des coefficients de P et $\widetilde{P} := kP$. Alors, $\widetilde{P}$ est un polynôme de degré n de $\mathbb{Z}[X]$. Comme θ est irrationnel, $n \geq 2$ et comme P est irréductible sur $\mathbb{Q}$, $\frac{p}{q}$ n'est pas une racine de P et donc $\widetilde{P}\left(\frac{p}{q}\right) \neq 0$. Ainsi, $q^n\left(\widetilde{P}(\theta) - \widetilde{P}\left(\frac{p}{q}\right)\right)$ est un entier non nul donc

$$\left|q^n\left(\widetilde{P}(\theta) - \widetilde{P}\left(\frac{p}{q}\right)\right)\right| \geq 1 \quad i.e. \quad \left|\widetilde{P}(\theta) - \widetilde{P}\left(\frac{p}{q}\right)\right| \geq \frac{1}{q^n}.$$

Or, comme $\left|\theta - \frac{p}{q}\right| \leq 1$, par le théorème des accroissements finis, il existe un réel $c \in [\theta - 1\,;\theta + 1]$ tel que

$$\widetilde{P}(\theta) - \widetilde{P}\left(\frac{p}{q}\right) = \widetilde{P}'(c)\left(\theta - \frac{p}{q}\right)$$

et $\widetilde{P}'(c) \neq 0$ car $0 = \widetilde{P}(\theta) \neq \widetilde{P}\left(\frac{p}{q}\right)$. Ainsi, en posant $M := \max\limits_{x \in [\theta-1;\theta+1]} \left|\widetilde{P}'(x)\right|$, on en déduit que

$$\left|\theta - \frac{p}{q}\right| = \frac{\left|\widetilde{P}(\theta) - \widetilde{P}\left(\frac{p}{q}\right)\right|}{\left|\widetilde{P}'(c)\right|} \geq \frac{1}{Mq^n}.$$

Finalement, en posant $K := \max\{1, M\}$, on peut affirmer que, dans tous les cas,

$$\left|\theta - \frac{p}{q}\right| \geq \frac{1}{Kq^n}.$$

Cette démonstration est instructive à deux niveaux. D'abord, elle utilise un argument tout aussi trivial que central en approximation diophantienne : tout entier naturel non nul est au moins égal à 1. On verra que toutes les démonstrations, sans exception, des principaux théorèmes de ce mémoire utilisent ce résultat. Ensuite, ce théorème a l'avantage d'être explicite i.e. de donner une expression explicite de la constante K.

Une application historique du théorème de Liouville est la construction explicite de nombres transcendants (et même de toute une classe de nombres transcendants, appelés nombres de Liouville) et

(4). Joseph Liouville, 1809–1882.

ce une trentaine d'années avant la théorie de la cardinalité de Cantor qui montrera que les nombres transcendants forment un ensemble infini non dénombrable. L'exemple donné par Liouville est celui du nombre

$$\alpha := \sum_{n=0}^{+\infty} \frac{1}{10^{n!}}.$$

On vérifie simplement que, pour tout $k \in \mathbb{N}^*$, en définissant $\dfrac{p_k}{q_k} = \sum\limits_{n=0}^{k} \frac{1}{10^{n!}}$ avec $q_k = 10^{k!}$, on a

$$0 < \left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^k}$$

et donc, si α était algébrique de degré d, on aurait, d'après le théorème de Liouville, pour tout $k \in \mathbb{N}^*$,

$$\frac{1}{Kq_k^d} \leq \left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^k}$$

ce qui aboutit à absurdité en faisant tendre k vers $+\infty$.

Le théorème de Liouville conduit à une question légitime : est-il possible de trouver un exposant plus faible que n dans l'inégalité $\left|\theta - \frac{p}{q}\right| \geq \dfrac{1}{Kq^n}$? Cette question en amène naturellement une autre : quelle est le borne inférieure de tels exposants ? Ceci conduit à la définition suivante.

Définition [5]. — Soit x un nombre réel. On dit qu'un réel λ est une mesure d'irrationalité de x s'il existe une constante réelle $K = K(x, \lambda) > 0$ telle que, pour tout rationnel $\frac{p}{q} \neq x$ avec $q > 0$, on ait

$$\left|x - \frac{p}{q}\right| \geq \frac{1}{Kq^\lambda}.$$

La borne inférieure de l'ensemble des mesures d'irrationalité de x est appelée la mesure optimale d'irrationalité et on la notera $\mu(x)$ (avec la convention habituelle $\mu(x) = +\infty$ si x n'admet pas de mesure d'irrationalité).

Cette notion de mesure d'irrationalité traduit, en un certain sens, un degré d'irrationalité de x. Si $x = \frac{s}{t}$ est un rationnel écrit sous forme irréductible, pour tout rationnel $\frac{p}{q} \neq \frac{s}{t}$, on a $\left|x - \frac{p}{q}\right| = \frac{|sq-tp|}{tq} \geq \frac{1}{tq}$ car $sq - tp \neq 0$. Ainsi, $\mu(x) \leq 1$. De plus, par le théorème de Bézout, on peut trouver une suite $\left(\frac{p_n}{q_n}\right)$ avec $\lim q_n = +\infty$ telle que, pour tout $n \in \mathbb{N}$, $|sq_n - tp_n| = 1$ et donc $\left|x - \frac{p_n}{q_n}\right| = \frac{1}{tq_n}$. Ceci impose que $\mu(x) \geq 1$. On en déduit que la mesure optimale d'irrationalité d'un rationnel est 1. Par ailleurs, il suit de la proposition (1.1.7) que si x est irrationnel et si $R_n = \frac{p_n}{q_n}$ est la $n-$ième réduite dans le développement en fraction continuée de x alors $|x - R_n| < \frac{1}{q_n^2}$ donc, si λ est une mesure d'irrationalité de x alors $\frac{1}{K(x,\lambda)q_n^\lambda} < \frac{1}{q_n^2}$ donc $q_n^{\lambda-2} \geq \frac{1}{K(x,\lambda)}$ ce qui assure que $\lambda \geq 2$ car $\lim q_n = +\infty$. Ainsi, si x est irrationnel alors $\mu(x) \geq 2$. En reprenant la même démarche que précédemment avec α, on montre simplement que les nombres de Liouville (i.e. les nombres réels x tels qu'ils existent une suite de rationnels $\left(\frac{p_n}{q_n}\right)$ avec $q_n > 1$ vérifiant l'inégalité $0 < \left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n^n}$ pour tout n à partir d'un certain rang) ont une mesure optimale d'irrationalité égale à $+\infty$.

(5). Il semble qu'il n'y ait pas de réel consensus sur la définition de mesure d'irrationalité. Certains auteurs ne la définissent que pour des x irrationnels, d'autres n'imposent pas $q > 0$ mais seulement $q > q_0$ pour un certain q_0 ce qui revient à admettre qu'un nombre fini de rationnels $\frac{p}{q}$ peuvent vérifier $\left|x - \frac{p}{q}\right| < \frac{1}{Kq^\lambda}$. Dans la définition que nous adoptons, x peut être rationnel et, le cas échéant, c'est le seul réel que nous autorisons à vérifier $\left|x - \frac{p}{q}\right| < \frac{1}{Kq^\lambda}$.

Le théorème de Liouville montre que si x est irrationnel algébrique de degré n alors $\mu(x) \leq n$. L'amélioration de ce théorème et la détermination de la mesure optimale d'irrationalité d'un nombre irrationnel algébrique ont été la source de nombreux travaux au cours de la première moitié du XXe siècle. La valeur n de Liouville a été successivement améliorée par Thue [6] ($\mu(x) \leq \frac{n}{2} + 1$, 1908), Siegel [7] ($\mu(x) \leq 2\sqrt{n}$, 1921), Dyson [8] et, indépendamment, Gel'fond [9] ($\mu(x) \leq \sqrt{2n}$, 1947) avant que Roth [10] ne montre le théorème qui lui a valu la médaille Field en 1958.

Théorème de Roth (1955). — Soit x un nombre irrationnel algébrique. Alors, pour tout $\varepsilon > 0$, il existe une constante $K = K(x, \varepsilon)$ telle que, pour tout rationnel $\frac{p}{q}$ avec $q > 0$, on ait

$$\left| x - \frac{p}{q} \right| > \frac{1}{Kq^{2+\varepsilon}}.$$

Autrement dit, la mesure optimale d'irrationalité de tout nombre irrationnel algébrique est 2.

Toutes ces améliorations ont une caractéristique commune : elles sont *ineffectives* i.e. leurs démonstrations assurent l'existence de la constante $K(x, \lambda)$ mais ne donnent pas de moyen de déterminer celle-ci. C'est un réel problème lorsqu'on veut appliquer ces théorèmes d'approximation à la résolution d'équations diophantiennes, d'autant que le seul théorème de Liouville est insuffisant. Par exemple, si (x, y) est une solution non triviale de $ax^n - by^n = 1$ et si $a > b$ alors on montre (inégalité (1.7) p. 35) que

$$\left| \sqrt[n]{\frac{a}{b}} - \frac{y}{x} \right| < \frac{1}{nbx^n}.$$

Dès lors, si on connait une mesure d'irrationalité λ de $\sqrt[n]{\frac{a}{b}}$, on en déduit que

$$K(x, \lambda)x^{\lambda} > nbx^n.$$

Si $\lambda \geq n$, on ne peut en tirer aucune information sur x donc, en particulier, le théorème de Liouville est insuffisant. En revanche, si $\lambda < n$, on en déduit un majorant de x

$$x < \left(\frac{K(x, \lambda)}{nb} \right)^{\frac{1}{n-\lambda}}.$$

Si on ne connait pas explicitement $K(x, \lambda)$, on ne peut rien en déduire si ce n'est que x est borné et, par suite, que (E_n) n'a qu'un nombre fini de solutions (car $by^n = ax^n - 1$ donc $y < x \sqrt[n]{\frac{b}{a}}$ est également borné). C'est d'ailleurs un cas particulier très simple d'un résultat montré par Thue.

Théorème de Thue (1909). — Si F est un polynôme homogène de $\mathbb{Z}[X, Y]$ de degré $n \geq 3$ irréductible sur $\mathbb{Q}$ alors, pour tout $m \in \mathbb{N}^*$, l'équation $F(x, y) = m$ n'a qu'un nombre fini de solutions $(x, y) \in \mathbb{Z}^2$.

De ce fait, avec des résultats non effectifs d'approximation diophantienne, on obtient des bornes non effectives pour les solutions d'équation diophantienne. Dès lors, parallèlement aux résultats que nous venons de citer, des travaux ont été menés pour déterminer des bornes effectives pour ces solutions (ou, à défaut, le nombre de ces solutions). Ces recherches se sont orientées dans trois directions principales.

1. Déterminer des mesures d'irrationalité explicites. Pour les équations (E_n) (et donc pour les nombres irrationnels $\sqrt[n]{\frac{a}{b}}$), ceci passe notamment par l'utilisation d'approximants de Padé qui sont intimement liés aux fonctions hypergéométriques (méthode dite *hypergéométrique*).

(6). Axel Thue, 1863–1922.
(7). Carl Ludwig Siegel, 1896–1981.
(8). Freeman J. Dyson, né en 1923.
(9). Alexandre Ossipovitch Gel'fond, 1906–1968.
(10). Klaus Friedrich Roth, né en 1925.

2. Améliorer le principe de démonstration initié par Thue et repris par Siegel qui, même s'il se base sur une méthode non effective pour les mesures d'irrationalité, permet d'obtenir des bornes explicites pour le nombre de solutions d'équations diophantiennes (méthode dite de *Thue-Siegel*). Pour les équations (E_n), elle utilise également des approximants de Padé de fonctions binomiales.

3. Utiliser les minorations de formes linéaires de logarithmes. Développée principalement par Baker [(11)], cette méthode a notamment permis à ce dernier de donner la première version explicite du théorème de Thue.

Ces différentes méthodes ont permis d'avoir une connaissance de plus en plus précise du nombre de solutions des équations du type $F(x,y)=m$ et notamment des équations (E_n).

Par la méthode de Thue-Siegel, Siegel [39] montre en 1937 que, si a, b et c sont des entiers naturels non nuls tels que

$$(ab)^{\frac{n}{2}-1} \geq 4c^{2n-2}\left(n\prod_{p|n}p^{\frac{1}{n-1}}\right)^n$$

alors l'inéquation $|ax^n-by^n|\leq c$ admet au plus une solution en entiers naturels non nuls et premiers entre eux. Si on suppose n premier, on peut remplacer la condition précédente par le critère plus pratique :

$$\sqrt{ab}\geq 188c^4.$$

Par la suite, Domar [10] améliore la démonstration de Siegel et obtient que l'équation (E_n) a au plus deux solutions en entiers strictement positifs si $n\geq 5$.

Dans sa thèse [13], toujours suivant la méthode de Thue-Siegel, Evertse détermine des constantes explicites μ_n et α_n telles que l'inéquation $|ax^n-by^n|\leq C$ où x et y sont des entiers strictement positifs premiers entre eux admet au plus une solution telle que $\max\{ax^n,by^n\}\geq \mu_n C^{\alpha_n}$. Ces constantes sont suffisamment petites pour montrer que (E_n) a au plus une solution en entiers strictement positifs si $n\geq 5$ et $a\neq b+1$.

La résolution des cas restants a demandé de faire appel aux autres techniques. Mignotte a été le premier dans [26] à déterminer un majorant absolu de n (en l'occurence 600) au-delà duquel l'équation $(F_n): (b+1)x^n-by^n=1$ n'a pas d'autres solutions que $(x,y)=(1,1)$. Il utilise pour cela un théorème de minoration de formes linéaires de logarithmes dû à Laurent, Mignotte et Nesterenko.

Bennett et de Weger, utilisant à la fois des méthodes algébriques pour les petites valeurs de n et des méthodes diophantiennes (notamment la méthode de Mignotte), montrent que (F_n) n'a pas d'autre solution que $(1,1)$ sauf éventuellement si n est un nombre premier entre 17 et 347 et $2\leq b\leq \min\{0{,}3n,83\}$. Enfin, Bennett traite les cas restants en utilisant la méthode hypergéométrique dans son article [5].

Ainsi, quasiment tous les cas ont pu être traités par des méthodes d'approximation diophantienne. Les seuls qui échappent à la règle sont les équations (E_3), (E_4) et (E_n) pour n premier entre 5 et 13, $a=b+1$ et b prenant un nombre fini de valeurs. Tous ces cas ont été traités par des méthodes algébriques faisant intervenir les unités fondamentales dans des corps de nombres [(12)]. Le premier résultat en ce sens est dû à Delaunay [(13)] [9] pour l'équation $x^3+dy^3=1$ où d n'est pas le cube d'un entier. L'idée est la suivante : on se place dans le corps cubique $K=\mathbb{Q}[\sqrt[3]{d}]$ et on considère son anneau des entiers $\mathbb{Z}[\sqrt[3]{d}]$. Par définition, les unités de $\mathbb{Z}[\sqrt[3]{d}]$ sont les éléments inversibles de $\mathbb{Z}[\sqrt[3]{d}]$. Si on considère la norme sur K définie par $N(x+y\sqrt{d}+z\sqrt{d^2})=x^3+y^3d+z^3d^2-3xyzd$, on montre que $\eta\in\mathbb{Z}[\sqrt[3]{d}]$ est une unité si et seulement si $N(\eta)=\pm 1$. Par ailleurs, on montre également qu'il existe une unité $\varepsilon\in\,]0\,;1[$, appelée

(11). Alan Baker, né en 1939.

(12). On peut également traiter les équations de Pell-Fermat par une telle méthode.

(13). Boris Nikolaïevitch Delaunay, 1890–1980. On trouve dans la littérature le nom Delaunay qui est la francisation ou le nom Delone qui est la translittération du cyrillique. Il semble que lui-même préférait le premier qui rendait hommage à ses origines françaises.

unité fondamentale, telle que l'ensemble des unités s'écrive $\{\pm\varepsilon^n \,|\, n \in \mathbb{Z}\}$. Ainsi, un couple $(x, y) \in \mathbb{N}^2$ est solution de $x^3 + dy^3 = 1$ si et seulement si $N(x + y\sqrt[3]{d}) = 1$ i.e. si et seulement si $x + y\sqrt[3]{d}$ est une unité positive de $\mathbb{Z}[\sqrt[3]{d}]$. Une telle unité est appelée unité binomiale. La preuve de Delaunay consiste en une série de lemmes techniques qui permettent de voir que la seule unité de $\mathbb{Z}[\sqrt[3]{d}]$ qui peut être binomiale est l'unité fondamentale. Il s'ensuit que l'équation $x^3 + dy^3 = 1$ admet au plus une solution non triviale dans $\mathbb{N}^2$ et on en déduit immédiatement qu'il en est de même pour l'équation $x^3 - dy^3 = 1$.

Par la suite, Nagell [14] [30] a généralisé la méthode de Delaunay et montré que l'équation (E_3) admet au plus une solution en entiers strictement positifs. Enfin, Tartakovskii [15] [40] et Ljunggren [16] [23] ont traité de même le cas $n = 4$.

*
* *

Comme nous l'avons dit en préambule, nous ne nous intéresserons dans ce mémoire qu'aux résultats démontrés par des techniques d'approximation diophantienne. En particulier, nous admettrons les résultats de Nagell et Ljunggren à savoir que les équations (E_3) et (E_4) admettent au plus une solution non triviale pour toutes valeurs de a et b ainsi que les résultats similaires de de Weger et Bennett pour les équations $(F_n) : (b+1)x^n - by^n = 1$ lorsque n est un nombre premier compris entre 5 et 13. Dès lors, pour montrer que (E_n) admet au plus une solution non triviale pour tout $n \geq 5$, on peut se restreindre au cas où n est premier. Nous démontrerons alors le théorème principal de ce mémoire.

Théorème 1. — Si $n \geq 3$ alors l'équation (E_n) admet au plus une solution non triviale.

L'étude qui suit se découpe en 5 chapitres qui s'organisent comme suit :

1. Dans le chapitre 1, nous rappelons la définition et les principales propriétés des fractions continuées et nous appliquons celles-ci à l'étude des équations (E_1) et (E_2) que nous résolvons complètement. Nous terminons ce chapitre par un lemme fondamental pour la suite.
2. Dans le chapitre 2, nous présentons brièvement les approximants de Padé d'un système de fonctions analytiques au voisinage de 0 puis nous détaillons la construction due à Mahler (reprenant une idée de Hermite) pour la construction explicite des approximants de Padé d'un système de fonctions binomiales. Nous explicitons, en particulier, l'exemple des approximants de Padé diagonaux de la fonction $x \mapsto (1-x)^{\frac{1}{n}}$.
3. Cet exemple est utilisé dans le chapitre 3 où nous reprenons la démonstration d'Evertse basée sur la méthode de Thue-Siegel et qui nous permet de montrer que l'équation (E_n) admet au plus une solution non triviale si $n \geq 5$ et $a \neq b+1$ mais aussi de borner b dans les autres cas.
4. Dans le chapitre 4, nous suivons la démarche de Bennett et de Weger (elle-même inspirée de celle de Mignotte) qui s'appuie sur la minoration des formes linéaires de logarithmes pour montrer que, pour tout $n \geq 347$, l'équation $(F_n) : (b+1)x^n - by^n = 1$ n'a pas d'autre solution que $(1, 1)$. Cela permet donc de ne laisser qu'un nombre fini de cas restants.
5. Ces cas sont traités dans le chapitre 5 en suivant la démarche de Bennett qui utilise la méthode hypergéométrique. L'essentiel de cette partie est consacrée à la majoration du P.P.C.M. des dénominateurs des coefficients des approximants de Padé de la famille de fonctions binomiales construits dans le chapitre 2.

(14). Trygve Nagell, 1895–1988.
(15). Vladimir Abramovich Tartakovskii, 1901–1973.
(16). Wilhelm Ljunggren, 1905–1973.

Chapitre 1

Fractions continuées
Les cas $n = 1$ et $n = 2$

L'algorithme des fractions continuées permet d'obtenir de « très bonnes » approximations rationnelles d'un irrationel α. En un certain sens, il fournit même les « *meilleures approximations possibles* » comme on le verra au travers des propositions 1.1.7 et 1.1.8. Ceci est intimement lié à la résolution de l'équation $ax^n - by^n = 1$ car on prouvera (lemmes 1.3.7 et 1.4.2) que, en général, toute solution de cette équation fournit une « très bonne » approximation de $\sqrt[n]{\frac{a}{b}}$ dès que $n \geq 2$.

1.1 Fractions continuées

1.1.1 Définition et convergence

Notation 1.1.1. — Etant donné un réel quelconque a_0, on pose $[a_0] := a_0$ et, si a_1, a_2, ..., a_n ($n \geq 1$) sont des nombres réels strictement positifs , on pose

$$[a_0, a_1, ..., a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}.$$

Remarquons que, par définition, pour tout réel $y > 0$,

$$[a_0, a_1, ..., a_n, y] = \left[a_0, a_1, ..., a_{n-1}, a_n + \frac{1}{y}\right]. \tag{1.1}$$

Lemme 1.1.2. . — *Soit (a_n) une suite d'entiers strictement positifs à partir du rang 1 et (p_n) et (q_n) les suites d'entiers définies par :*

$$\begin{cases} p_0 = a_0, \ p_1 = a_1 a_0 + 1 \\ \forall n \in \mathbb{N}, \ p_{n+2} = a_{n+2} p_{n+1} + p_n \end{cases} \quad et \quad \begin{cases} q_0 = 1, \ q_1 = a_1 \\ \forall n \in \mathbb{N}, \ q_{n+2} = a_{n+2} q_{n+1} + q_n \end{cases}. \tag{1.2}$$

1. *La suite (q_n) est croissante et, pour tout $n \in \mathbb{N}$, $q_n \geq \Phi^{n-1}$ où $\Phi := \frac{1+\sqrt{5}}{2}$ est le nombre d'or.*
2. *Pour tout $n \in \mathbb{N}$, $q_{n+1}p_n - p_{n+1}q_n = (-1)^{n+1}$ et $q_{n+2}p_n - p_{n+2}q_n = (-1)^{n+1}a_{n+2}$.*
3. *Pour tout $n \in \mathbb{N}$ et pour tout réel $y > 0$, $[a_0, a_1, ..., a_{n+1}, y] = \frac{p_{n+1}y + p_n}{q_{n+1}y + q_n}$.*
4. *Pour tout $n \in \mathbb{N}$, $\frac{p_n}{q_n}$ est l'écriture sous forme de fraction irréductible de $[a_0, a_1, ..., a_n]$.*

Preuve

1. Remarquons que, par une récurrence immediate, pour tout $n \in \mathbb{N}$, $q_n \geq 1$. La croissance vient du fait que $q_1 = a_1 \geq 1 = q_0$ et, pour tout $n \geq 1$, $q_{n+1} = a_{n+1}q_n + q_{n-1} > q_n$ car $a_{n+1} \geq 1$ et $q_n \geq 1$. Il y a donc croissance stricte à partir du rang 1 (1). Enfin, $q_0 = 1 \geq \Phi^{-1}$, $q_1 = a_0 \geq \Phi^0$ et, par récurrence, pour tout $n \in \mathbb{N}$, $q_{n+2} = a_{n+2}q_{n+1} + q_n \geq q_{n+1} + q_n \geq \Phi^n + \Phi^{n-1} = \Phi^{n+1}$. Ainsi, le résultat est démontré pour tout $n \in \mathbb{N}$.

2. On raisonne par récurrence sur n. Pour $n = 0$, $q_1p_0 - p_1q_0 = a_1a_0 - (a_1a_0 + 1) = -1$ donc la propriété est vraie. Supposons que, pour un certain $n \in \mathbb{N}$, $q_{n+1}p_n - p_{n+1}q_n = (-1)^{n+1}$. Alors,

$$\begin{aligned} q_{n+2}p_{n+1} - p_{n+2}q_{n+1} &= (a_{n+2}q_{n+1} + q_n)p_{n+1} - (a_{n+2}p_{n+1} + p_n)q_{n+1} \\ &= -(q_{n+1}p_n - p_{n+1}q_n) = -(-1)^{n+1} = (-1)^{n+2} \end{aligned}$$

ce qui montre que la propriété est vraie au rang $n+1$ et ainsi l'égalité est établie pour tout $n \in \mathbb{N}$. Par suite, pour tout $n \in \mathbb{N}$,

$$\begin{aligned} q_{n+2}p_n - p_{n+2}q_n &= (a_{n+2}q_{n+1} + q_n)p_n - (a_{n+2}p_{n+1} + p_n)q_n \\ &= (q_{n+1}p_n - p_{n+1}q_n)a_{n+2} = (-1)^{n+1}a_{n+2} \end{aligned}$$

ce qui montre la seconde églité.

3. On raisonne ici aussi par récurrence sur n. Soit $y > 0$. Etant donné que

$$\frac{p_1y + p_0}{q_1y + q_0} = \frac{(a_1a_0 + 1)y + a_0}{a_1y + 1} = a_0 + \frac{y}{a_1y + 1} = a_0 + \frac{1}{a_1 + \dfrac{1}{y}},$$

on a bien $\dfrac{p_1y + p_0}{q_1y + q_0} = [a_0, a_1, y]$. Supposons la propriété vraie pour un certain $n \in \mathbb{N}$ (et pour tout $y > 0$). Alors, en utilisant (1.1) et en appliquant l'hypothèse de récurrence à $a_{n+2} + \dfrac{1}{y}$, il vient

$$\begin{aligned} [a_0, a_1, ..., a_{n+2}, y] = \left[a_0, a_1, ..., a_{n+1}, a_{n+2} + \frac{1}{y}\right] &= \frac{p_{n+1}\left(a_{n+2} + \dfrac{1}{y}\right) + p_n}{q_{n+1}\left(a_{n+2} + \dfrac{1}{y}\right) + q_n} \\ = \frac{p_{n+1}\left(a_{n+2}y + 1\right) + p_ny}{q_{n+1}\left(a_{n+2}y + 1\right) + q_ny} &= \frac{(a_{n+2}p_{n+1} + p_n)y + p_{n+1}}{(a_{n+2}q_{n+1} + q_n)y + q_{n+1}} \\ = \frac{p_{n+2}y + p_{n+1}}{q_{n+2}y + q_{n+1}}&. \end{aligned}$$

ce qui achève la récurrence.

4. Soit $n \in \mathbb{N}$. La première relation établie au point **2.** montre que p_n et q_n sont premiers entre eux. Si $n = 0$ alors $\dfrac{p_0}{q_0} = \dfrac{a_0}{1} = a_0 = [a_0]$ et si $n = 1$ alors $\dfrac{p_1}{q_1} = \dfrac{a_1a_0 + 1}{a_1} = a_0 + \dfrac{1}{a_1} = [a_0, a_1]$. Si $n \geq 2$, en appliquant le point **3.** avec $y = a_n$, il vient $[a_0, a_1, ..., a_{n-1}, a_n] = \dfrac{p_{n-1}a_n + p_{n-2}}{q_{n-1}a_n + q_{n-2}} = \dfrac{p_n}{q_n}$ ce qui permet de conclure. ■

(1). On peut remarquer que la croissance est stricte dès le rang 0 si $a_1 > 1$. Il en est d'ailleurs de même pour la suite (p_n) à condition cette fois que $a_0 \geq 0$. En effet, dans ce cas, il est clair que (p_n) est à valeurs positives, que $p_1 = a_1a_0 + 1 > a_0 = p_0$ et ensuite on raisonne comme pour (q_n).

Définition 1.1.3. — Soit x un nombre réel quelconque. On associe à x deux suites (éventuellement finies) : une suite (a_n) de nombres entiers naturels et une suite (x_n) de nombres réels (positifs à partir du rang $n = 1$) définies par

$$\begin{cases} x_0 := x \\ a_0 := \lfloor x \rfloor \end{cases}$$

et, pour tout $n \in \mathbb{N}$,

- si $x_n \in \mathbb{N}$, le processus s'arrête,
- sinon, on pose

$$\begin{cases} x_{n+1} := \dfrac{1}{x_n - a_n} \\ a_{n+1} := \lfloor x_{n+1} \rfloor \end{cases}$$

Le rationnel $R_n := [a_0, a_1, ..., a_n]$ est alors appelé la $n-$ième réduite dans le développement en fraction continuée du réel x et les nombres $a_0, a_1, ..., a_n$ sont appelés les coefficients de R_n.

Le réel x_n est appelé le $n-$ième quotient complet dans le développement de x en fraction continuée (ou plus simplement le $n-$ième quotient complet de x) et le nombre a_n est appelé le $n-$ième quotient partiel dans le développement de x en fraction continuée (ou plus simplement le $n-$ième quotient partiel de x) .

Lemme 1.1.4. — *On conserve les notations de la définition précédente.*

1. *Soit $n \in \mathbb{N}$ tel que x_n existe. Alors, $x = [a_0, a_1, ..., a_{n-1}, x_n]$.*
2. *La suite (x_n) est finie si et seulement si $x \in \mathbb{Q}$.*

Preuve

1. On raisonne par récurrence sur n. Si $n = 0$ alors, par définition, $x = x_0 = [x_0]$. Supposons que, pour un certain $n \in \mathbb{N}$, $x = [a_0, a_1, ..., a_{n-1}, x_n]$ et que x_{n+1} existe. Alors, en remarquant que $[a_0, a_1, ..., a_n, x_{n+1}] = \left[a_0, a_1, ..., a_{n-1}, a_n + \dfrac{1}{x_{n+1}}\right]$ et que, par définition, $a_n + \dfrac{1}{x_{n+1}} = x_n$, on obtient $[a_0, a_1, ..., a_n, x_{n+1}] = [a_0, a_1, ..., a_{n-1}, x_n] = x$.
2. Si (x_n) est finie alors il existe un rang $N \in \mathbb{N}$ tel que $x_N \in \mathbb{N}$ et alors $x = [a_0, a_1, ..., a_{n-1}, x_N] \in \mathbb{Q}$. Réciproquement, supposons que $x \in \mathbb{Q}$. On va montrer qu'il existe un rang k tel que $x_k \in \mathbb{N}$ ce qui équivaut à dire que (x_n) est finie. Ecrivons $x = \dfrac{N_0}{D_0}$ sous forme irréductible et effectuons la division euclidienne de N_0 par D_0 : il existe deux entiers Q_0 et D_1 tels que $N_0 = Q_0 D_0 + D_1$ et $0 \leq D_1 < D_0$. Alors, $x = Q_0 + \dfrac{D_1}{D_0}$ avec $0 \leq \dfrac{D_1}{D_0} < 1$. Ainsi, $a_0 = Q_0$ et ou bien $D_1 = 0$ i.e. $x_0 = x \in \mathbb{N}$ ou bien $x_1 = \dfrac{D_1}{D_0}$. On réitère alors le procédé. La division euclidienne de D_1 par D_0 fournit deux entiers Q_1 et D_2 tels que $x_1 = Q_1 + \dfrac{D_2}{D_1}$ avec $0 \leq D_2 < D_1$. Alors, $a_1 = Q_1$ et ou bien $D_2 = 0$ et $x_1 \in \mathbb{N}$ ou bien $x_2 = \dfrac{D_1}{D_2}$. On construit ainsi deux suites d'entiers (Q_n) et (D_n) telles que $x_n = Q_n + \dfrac{D_{n+1}}{D_n}$ et $0 \leq D_{n+1} < D_n < \cdots < D_0$. Ainsi, (D_n) est une suite d'entiers naturels strictement décroissante donc il existe un entier $k \in \mathbb{N}$ tel que $D_k = 0$ et alors $x_k = Q_k \in \mathbb{N}$. ■

Ainsi, la suite des réduites d'un nombre est finie si et seulement si ce nombre est rationnel. En particulier, la suite des réduites d'un irrationnel est infinie. On va montrer que dans ce cas, cette suite tend vers x (ce qui justifie a posteriori le terme de développement de x en fraction continuée) et que cette suite fournit de « très bonnes » approximations de x.

Proposition 1.1.5. — *Soit x un nombre irrationnel et (R_n) la suite des réduites de x. Alors,*

1. *les suites (R_{2n}) et (R_{2n+1}) sont adjacentes et convergent vers x ;*
2. *la suite (R_n) converge vers x ;*

Preuve

1. Pour tout $n \in \mathbb{N}$, on note f_n la fonction définie sur $]0\,;+\infty[$ par $f_n(x) = [a_0, a_1, ..., a_{n-1}, x]$ (de telle sorte que $f_0(x) = x$). La relation (1.1) implique alors que, pour tout $x > 0$, $f_{n+1}(x) = f_n\left(a_n + \dfrac{1}{x}\right)$. Ainsi, étant donné que f_0 est croissante et que $x \mapsto c + \dfrac{1}{x}$ est décroissante pour toute constante $c > 0$, on obtient par récurrence que f_n est croissante si n est pair et décroissante si n est impair. Notons que, par définition, pour tout $n \in \mathbb{N}$, $R_n = f_n(a_n)$ et, d'après le lemme 1.1.4, pour tout $n \in \mathbb{N}$, $f_n(x_n) = x$. De plus, par définition, pour tout $n \in \mathbb{N}$, $a_n = \lfloor x_n \rfloor \leq x_n$. Ainsi, pour tout $n \in \mathbb{N}$, $R_{2n} = f_{2n}(a_{2n}) \leq f_{2n}(x_{2n}) = x$ et $R_{2n+1} = f_{2n+1}(a_{2n+1}) \geq f_{2n+1}(x_{2n+1}) = x$ i.e. $R_{2n} \leq x \leq R_{2n+1}$.
   En écrivant $R_n = \dfrac{p_n}{q_n}$ sous forme irréductible, il découle du point **2.** du lemme 1.1.2 que, pour tout $n \in \mathbb{N}$, $R_n - R_{n+2} = \dfrac{(-1)^{n+1} a_{n+2}}{q_{n+2} q_n}$ ce qui assure que (R_{2n}) est strictement croissante et que (R_{2n+1}) est strictement décroissante. De plus, d'après le lemme 1.1.2, pour tout $n \in \mathbb{N}$,

$$|R_{2n+1} - R_{2n}| = \left|\frac{p_{2n+1}}{q_{2n+1}} - \frac{p_{2n}}{q_{2n}}\right| = \frac{1}{q_{2n+1} q_{2n}} \leq \frac{1}{\Phi^{4n-1}}$$

   ce qui montre que $\lim\limits_{n \to +\infty} (R_{2n+1} - R_{2n}) = 0$. On déduit que les deux suites (R_{2n}) et (R_{2n+1}) sont adjacentes. Elles convergent donc vers une même limite. Mais, étant donné que, pour tout $n \in \mathbb{N}$, $R_{2n} \leq x \leq R_{2n+1}$, cette limite commune est x.
2. Par un résultat classique sur les suites extraites, on en déduit que $\lim\limits_{n \to +\infty} R_n = x$. ■

Notation 1.1.6. — Si x est irrationnel et si (a_n) est la suite des coefficients des réduites de x, on note $x = [a_0, a_1, ..., a_n, ...]$ pour traduire l'égalité $x = \lim\limits_{n \to +\infty} R_n$. On dit alors que $[a_0, a_1, ..., a_n, ...]$ est le développement de x en fraction continuée.

1.1.2 Meilleures approximations

Les résultats de ce paragraphe seront tout à fait essentiel par la suite. On montre en substance que la suite des réduites donne les meilleures approximations d'un irrationnel x par des rationnels (proposition 1.1.7) et qu'en particulier, si un rationnel est une « *très bonne approximation* » de x alors ce rationnel est nécessairement l'une des réduites de x (proposition 1.1.8).

Proposition 1.1.7. — *Soit x un irrationnel et (R_n) la suite de ses réduites écrites sous forme irréductible $R_n = \dfrac{p_n}{q_n}$. Soit $r = \dfrac{p}{q}$ un rationnel écrit sous forme irréductible. Alors,*

1. *pour tout $n \in \mathbb{N}$, $\dfrac{1}{q_n(q_n + q_{n+1})} < |x - R_n| < \dfrac{1}{q_n q_{n+1}}$;*
2. *s'il existe un entier $m \in \mathbb{N}$ tel que $q < q_{m+1}$ alors $|x - R_m| \leq \dfrac{q}{q_m} |x - r|$ avec égalité si et seulement si $r = R_m$.*

Preuve

1. Soit $n \in \mathbb{N}$. Il découle de la proposition 1.1.5 que, pour tout $k \in \mathbb{N}$,

$$R_{2k} < R_{2k+2} < x < R_{2k+3} < R_{2k+1} \quad \text{i.e.} \quad \frac{p_{2k}}{q_{2k}} < \frac{p_{2k+2}}{q_{2k+2}} < x < \frac{p_{2k+3}}{q_{2k+3}} < \frac{p_{2k+1}}{q_{2k+1}}.$$

Ainsi, en séparant les cas $n = 2k$ et $n = 2k + 1$, il s'ensuit que

$$\left| x - \frac{p_n}{q_n} \right| < \left| \frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}} \right| = \frac{|p_n q_{n+1} - p_{n+1} q_n|}{q_n q_{n+1}} = \frac{1}{q_n q_{n+1}}$$

d'après le point **2.** du lemme 1.1.2.
De même,

$$\left| x - \frac{p_n}{q_n} \right| > \left| \frac{p_n}{q_n} - \frac{p_{n+2}}{q_{n+2}} \right| = \frac{|p_n q_{n+2} - p_{n+2} q_n|}{q_n q_{n+2}} = \frac{a_{n+2}}{q_n(a_{n+2} q_{n+1} + q_n)}$$

toujours d'après le point **2.** du lemme 1.1.2. Comme, de plus, $a_{n+2} \geq 1$ et comme la fonction $x \mapsto \dfrac{x}{q_n(x q_{n+1} + q_n)}$ est croissante sur $[1\,;+\infty[$, il s'ensuit $\left| x - \dfrac{p_n}{q_n} \right| > \dfrac{1}{q_n(q_{n+1} + q_n)}$.

2. Considérons le système d'inconnues X et Y suivant :

$$\begin{cases} p_{m+1} X + p_m Y = p \\ q_{m+1} X + q_m Y = q \end{cases}.$$

Le déterminant de ce système est $p_{m+1} q_m - q_{m+1} p_m = (-1)^{m+1} \in \mathbb{Z}^\times$ donc ce système admet une unique solution $(u, v) \in \mathbb{Z}^2 \setminus \{(0,0)\}$. De plus, v est non nul. En effet, si $v = 0$ alors $R_{m+1} = \dfrac{p_{m+1} u}{q_{m+1} u} = \dfrac{p}{q} = r$ et, comme les fractions sont irréductibles, $q_{m+1} = q$ ce qui est exclu car $q_{m+1} > q$. Si u est nul alors de la même façon, $R_m = r$ et on obtient le cas d'égalité. Sinon, u et v sont non nuls et étant donné que $0 < q = u q_{m+1} + v q_m < q_m$, u et v sont de signes contraires. Comme $x - R_{m+1}$ et $x - R_m$ sont également de signes contraires, les nombres $u(x - R_{m+1})$ et $v(x - R_m)$ sont de même signe. Il s'ensuit qu'il en est de même pour $u(q_{m+1} x - p_{m+1})$ et $v(q_m x - p_m)$. En utilisant le fait que $qx - p = (u q_{m+1} + v q_m)x - (u p_{m+1} + v p_m) = u(q_{m+1} x - p_{m+1}) + v(q_m x - p_m)$, on en déduit que

$$|qx - p| = |u(q_{m+1} x - p_{m+1})| + |v(q_m x - p_m)| \geq |v|\,|q_m x - p_m| > |q_m x - p_m|$$

ce qui permet de conclure. ■

La proposition précédente implique en particulier que, pour toute réduite R_n de x, $|x - R_n| < \dfrac{1}{q_n^2}$ car $q_n \leq q_{n+1}$. On a en fait un résultat plus fort qui est une version effective du théorème de Dirichlet (corollaire 1.3.2).

Proposition 1.1.8. — *Soit x un irrationnel et (R_n) la suite de ses réduites écrites sous forme irréductible $R_n = \dfrac{p_n}{q_n}$.*

1. *Pour tout $n \in \mathbb{N}$, l'inégalité $|x - R_k| < \dfrac{1}{2q_k^2}$ est vraie pour au moins un entier $k \in \{n, n+1\}$. Autrement dit, parmi deux réduites successives, l'une au moins vérifie l'inégalité précédente.*
2. *Si un rationnel $r = \dfrac{p}{q}$ écrit sous forme irréductible vérifie $\left| x - \dfrac{p}{q} \right| < \dfrac{1}{2q^2}$ alors $r = R_n$ où n est l'unique entier tel que $q_n \leq q < q_{n+1}$.*

Preuve

1. Soit $n \in \mathbb{N}$. On a déjà vu que $x - R_n$ et $x - R_{n+1}$ sont de signes opposés. Il s'ensuit, en utilisant aussi le lemme 1.1.2, que

$$|x - R_n| + |x - R_{n+1}| = |R_n - R_{n+1}| = \frac{|q_{n+1}p_n - p_{n+1}q_n|}{q_n q_{n+1}} = \frac{1}{q_n q_{n+1}}.$$

Or, pour tous réels a et b, $ab \leq \frac{1}{2}(a^2 + b^2)$ donc, en prenant $a = \frac{1}{q_n}$ et $b = \frac{1}{q_{n+1}}$, il vient

$$|x - R_n| + |x - R_{n+1}| < \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2}$$

ce qui impose que $|x - R_n| < \frac{1}{2q_n^2}$ ou $|x - R_{n+1}| < \frac{1}{2q_{n+1}^2}$.

2. Comme la suite (q_n) est croissante et tend vers $+\infty$ et comme $q_0 = 1 \leq q$, il existe un unique entier $n \in \mathbb{N}$ tel que $q_n \leq q < q_{n+1}$. Alors, en utilisant la proposition 1.1.7 et le fait que $q_n \leq q$,

$$\left|\frac{p}{q} - \frac{p_n}{q_n}\right| \leq \left|x - \frac{p}{q}\right| + \left|x - \frac{p_n}{q_n}\right| \leq \left(1 + \frac{q}{q_n}\right)\left|x - \frac{p}{q}\right| < \frac{q_n + q}{q_n} \times \frac{1}{2q^2} \leq \frac{1}{qq_n}$$

donc

$$|q_n p - q p_n| = q q_n \left|\frac{p}{q} - \frac{p_n}{q_n}\right| < 1$$

et, comme le terme de gauche est un entier, il est donc nul ce qui implique que $\frac{p}{q} = \frac{p_n}{q_n}$ comme annoncé. ■

1.1.3 Nombres irrationnels quadratiques

Définition 1.1.9. — Un nombre irrationnel est dit irrationnel quadratique s'il est racine d'un polynôme de degré 2 à coefficients entiers. Autrement dit, α est irrationnel quadratique s'il existe des entiers a, b et c tels que $a\alpha^2 + b\alpha + c = 0$ avec $a \neq 0$ et $\Delta := b^2 - 4ac$ un entier naturel qui n'est pas un carré parfait.

Comme $\Delta \neq 0$, le polynôme $P = aX^2 + bX + c$ admet une autre racine notée α^*. Le nombre α^* est appelé le conjugué (algébrique) de α [(2)].

Enfin, on dit que α est irrationnel quadratique réduit si α est un irrationnel quadratique tel que $\alpha > 1$ et $-1 < \alpha^* < 0$.

On va à présent caractériser les irrationnels quadratiques et les irrationnels quadratiques réduits par leur développement en fraction continuée.

Proposition 1.1.10. *(Euler [(3)], 1748) — Soit α un irrationnel et $\alpha = [a_0, a_1, ..., a_n, ...]$ son développement en fraction continuée. Si la suite (a_n) est périodique à partir d'un certain rang N alors α est un irrationnel quadratique. On dit alors que la fraction continuée $[a_0, a_1, ..., a_n, ...]$ est périodique à partir du rang N.*

(2). Comme α est de la forme $\alpha = p + q\sqrt{d}$ où d est sans facteur carré, $\alpha \in \mathbb{Q}[\sqrt{d}]$ et alors α^* est le conjugué de α dans $\mathbb{Q}[\sqrt{d}]$. La conjugaison étant un $\mathbb{Q}-$automorphisme de $\mathbb{Q}[\sqrt{d}]$, on a en particulier $(\alpha + \beta)^* = \alpha^* + \beta^*$ et $\left(\frac{1}{\alpha}\right)^* = \frac{1}{\alpha^*}$.

(3). Leonhard Euler, 1707–1783.

Preuve. — Supposons que (a_n) est périodique à partir du rang N i.e. qu'il existe un entier $T > 0$ [4] tel que, pour tout $n \geq N$, $a_{n+T} = a_n$. Notons $\alpha_N = [a_N, a_{N+1}, ..., a_{n+T}, ...]$ le $N-$ième quotient complet. Puisque, pour tout $n \geq N$, $a_{n+T} = a_n$, on a également $\alpha_N = [a_{N+T}, a_{N+T+1}, ...]$ donc, en vertu du lemme 1.1.4, $\alpha_N = [a_N, a_{N+1}, ..., a_{N+T-1}, \alpha_N]$. Notons, pour tout $n \in \mathbb{N}$, $\dfrac{p'_n}{q'_n}$ la $n-$ième réduite dans le développement de α_N. On déduit alors du point **3.** du lemme 1.1.2 que

$$\alpha_N = \frac{p'_{T-1}\alpha_N + p'_{T-2}}{q'_{T-1}\alpha_N + q'_{T-2}}.$$

Il s'ensuit que α_N est racine du polynôme $q'_{T-1}X^2 + (q'_{T-2} - p'_{T-1})X - p'_{T-2}$ i.e. α_N est le forme $p + q\sqrt{d}$ où p et q sont rationnels et d est un entier (sans facteur carré car α_N est irrationnel).

Remarquons alors que, de la même façon, $\alpha = [a_0, a_1, ..., a_{N-1}, \alpha_N]$ donc, en notant $\dfrac{p_n}{q_n}$ la $n-$ième réduite de α,

$$\alpha = \frac{p_{N-1}\alpha_N + p_{N-2}}{q_{N-1}\alpha_N + q_{N-2}} = \frac{p_{N-1}(p + q\sqrt{d}) + p_{N-2}}{q_{N-1}(p + q\sqrt{d}) + q_{N-2}} = \frac{t + r\sqrt{d}}{t' + r'\sqrt{d}}$$

où r, t, r' et t' sont des entiers. Il s'ensuit que

$$\alpha = \frac{(t + r\sqrt{d})(t' - r'\sqrt{d})}{t'^2 - dr'^2} = \frac{tt' - drr' + (rt' - tr')\sqrt{d}}{t'^2 - dr'^2} = u + v\sqrt{d}$$

où u et v sont des rationnels. On en déduit l'existence de trois entiers m, a et b tels que $m\alpha = a + b\sqrt{d}$ et alors α est racine du trinôme $m^2X^2 - 2amX + a^2 - b^2d$ donc α est quadratique. ■

Proposition 1.1.11. *(Lagrange [5], 1768.) — Soit α un irrationnel quadratique. Alors, le développement en fraction continuée de α est périodique à partir d'un certain rang.*

Preuve. — Ecrivons le développement de α en fraction continuée $\alpha = [a_0, a_1, ..., a_n, ...]$. Comme α est quadratique, il existe un polynôme $P = aX^2 + BX + c \in \mathbb{Z}[X]$ de degré 2 tel que $P(\alpha) = 0$. Notons $\Delta = b^2 - 4ac$ son discriminant. Pour tout entier $n \geq 2$, d'après le lemme 1.1.2,

$$\alpha = [a_0, a_1, ..., \alpha_n] = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}$$

donc en substituant dans $P(\alpha) = 0$, on obtient

$$A_n\alpha_n^2 + B_n\alpha_n + C_n = 0 \quad \text{avec} \quad \begin{cases} A_n = ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2 \\ B_n = 2ap_{n-1}p_{n-2} + b(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2cq_{n-1}q_{n-2} \\ C_n = ap_{n-2}^2 + bp_{n-2}q_{n-2} + cq_{n-2}^2 \end{cases}.$$

Si A_n était nul alors $\dfrac{p_{n-1}}{q_{n-1}}$ serait une racine de P ce qui est exclu car α est quadratique. Ainsi, $A_n \neq 0$ donc $P_n := A_nX^2 + B_nX + C_n$ est un polynôme de degré 2 de $\mathbb{Z}[X]$ qui annule α_n. On vérifie par un simple calcul que

$$\Delta_n := B_n^2 - 4A_nC_n = (b^2 - 4ac)(q_{n-1}p_{n-2} - p_{n-1}q_{n-2})^2 = b^2 - 4ac = \Delta$$

en vertu du lemme 1.1.2. Ainsi, les polynômes P_n ont tous le même discriminant que P.

(4). Quitte à remplacer N et T par $N + 2$ et $2T$, on peut toujours supposer N et T au moins égaux à 2, ce qui permet dans la suite de considérer des termes d'indices $N - 2$ et $T - 2$.

(5). Joseph-Louis Lagrange, 1736–1813.

On va montrer que les suites d'entiers (A_n), (B_n) et (C_n) ne prennent qu'un nombre fini de valeurs. Pour cela, il suffit de montrer qu'elles sont bornées. Soit $n \geq 2$. D'après la proposition 1.1.7, $|q_{n-1}\alpha - p_{n-1}| < \dfrac{1}{q_n} \leq \dfrac{1}{q_{n-1}}$ donc il existe un réel δ_{n-1} tel que $p_{n-1} = q_{n-1}\alpha + \dfrac{\delta_{n-1}}{q_{n-1}}$ et $|\delta_{n-1}| < 1$. Il s'ensuit que

$$\begin{aligned} A_n &= a\left(q_{n-1}\alpha + \frac{\delta_{n-1}}{q_{n-1}}\right)^2 + b\left(q_{n-1}\alpha + \frac{\delta_{n-1}}{q_{n-1}}\right)q_{n-1} + cq_{n-1}^2 \\ &= (a\alpha^2 + b\alpha + c)q_{n-1}^2 + 2a\delta_{n-1}\alpha + a\frac{\delta_{n-1}^2}{q_{n-1}^2} + b\delta_{n-1} \\ &= 2a\delta_{n-1}\alpha + a\frac{\delta_{n-1}^2}{q_{n-1}^2} + b\delta_{n-1} \qquad (\text{car } P(\alpha) = 0) \end{aligned}$$

donc $|A_n| < 2\,|a\alpha| + |a| + |b|$. Ainsi, la suite (A_n) est bornée. Comme, pour tout $n \geq 3$, $C_n = A_{n-1}$, il s'ensuit que (C_n) est également bornée. De plus, pour tout entier n, $\Delta_n = \Delta$ donc $B_n^2 = 4A_nC_n + \Delta$ ce qui implique de (B_n) est aussi bornée.

Ainsi, le triplet d'entiers (A_n, B_n, C_n) ne prend qu'un nombre fini de valeurs lorsque n parcourt l'ensemble des entiers supérieurs ou égaux à 2 donc on peut trouver trois indices $j < k < \ell$ tels que $(A_j, B_j, C_j) = (A_k, B_k, C_k) = (A_\ell, B_\ell, C_\ell)$. Alors, $P_j = P_k = P_\ell$ donc α_j, α_k et α_ℓ sont des racines de P_j. Comme ce dernier est de degré 2, cela implique que deux (au moins) de ces trois nombres sont égaux. On peut supposer sans nuire à la généralité que $\alpha_j = \alpha_k$ i.e. $[a_j, a_{j+1}, ...] = [a_k, a_{k+1}, ...]$. Alors, en posant $T = k - j > 0$, pour tout $n \geq j$, $a_n = a_{n+T}$ ce qui montre que la suite (a_n) est périodique à partir du rang j. ■

Notation 1.1.12. — Soit α un irrationnel quadratique et $\alpha = [a_0, a_1, ..., a_n, ...]$ son développement en fraction continuée. Si la suite (a_n) est périodique de période T à partir du rang N, on notera $\alpha = [a_0, a_1, ..., a_{N-1}, \overline{a_N, a_{N+1}, ..., a_{N+T-1}}]$.

Proposition 1.1.13. *(Galois[6], 1828) — Un réel α est irrationnel quadratique réduit si et seulement si son développement en fraction continuée $\alpha = [a_0, a_1, ..., a_n, ...]$ est purement périodique i.e. si et seulement si la suite (a_n) est périodique à partir du rang $n = 0$.*

Preuve. — Soit α un irrationnel et $\alpha = [a_0, a_1, ..., a_n, ...]$ son développement en fraction continuée.

Supposons que α est irrationnel quadratique réduit. Montrons que tous ses quotients complets $\alpha_n = [a_n, a_{n+1}, ...]$ sont également des irrationnels quadratiques réduits. Comme le développement en fraction continuée de α_n est le même que celui de α aux $n-1$ premiers termes près, celui-ci est périodique à partir d'un certain rang donc tous les α_n sont irrationnels quadratiques. Montrons par récurrence qu'ils sont tous réduits. Pour $\alpha_0 = \alpha$, c'est vrai par hypothèse. Supposons que α_n soit réduit. Alors, $\alpha_n > 1$ et $\alpha_n^* \in \,]-1\,;0[$. Ecrivons $\alpha_n = a_n + \dfrac{1}{\alpha_{n+1}}$ (avec, rappelons-le, $a_n = \lfloor \alpha_n \rfloor$). Alors, $\alpha_{n+1} = \dfrac{1}{\alpha_n - a_n} > 1$ car $0 < \alpha_n - a_n < 1$. De plus, $\alpha_n > 1$ donc $a_n \geq 1$ et ainsi, étant donné que $\alpha_n^* = a_n + \dfrac{1}{\alpha_{n+1}^*}$ [7], $\dfrac{1}{\alpha_{n+1}^*} = \alpha_n^* - a_n < -1$ car $\alpha_n^* < 0$. Il s'ensuit que $\alpha_{n+1}^* \in \,]-1\,;0[$ et donc α_{n+1} est réduit ce qui achève la récurrence.

Ainsi, en particulier, pour tout $n \in \mathbb{N}$, $-\dfrac{1}{\alpha_{n+1}^*} = a_n - \alpha_n^*$ avec $0 < -\alpha_n^* < 1$ donc $a_n = \left\lfloor -\dfrac{1}{\alpha_{n+1}^*} \right\rfloor$.

(6). Evariste Galois, 1811–1832.
(7). Voir note (2) page 18.

Raisonnons par l'absurde en supposant que le développement de α n'est pas purement périodique. Notons T la plus petite période de ce développement et N le premier indice de la première période. Ainsi, $\alpha = [a_0, a_1, ..., a_{N-1}, \overline{a_N, ..., a_{N+T-1}}]$ avec $a_{N-1} \neq a_{N+T-1}$ et $N \geq 1$. Par définition de T, on a $\alpha_N = [a_N, a_{N+1}, ..., a_n, ...] = [a_{N+T}, a_{N+T+1}, ..., a_{n+T}, ...] = \alpha_{N+T}$ donc $-\dfrac{1}{\alpha_N^*} = -\dfrac{1}{\alpha_{N+T}^*}$ et, ainsi, $a_{N-1} = \left\lfloor -\dfrac{1}{\alpha_N^*} \right\rfloor = \left\lfloor -\dfrac{1}{\alpha_{n+T}^*} \right\rfloor = a_{N+T-1}$ ce qui fournit la contradiction souhaitée. Ainsi, le développement de α est bien purement périodique.

Réciproquement, supposons que le développement en fraction continuée de α est purement périodique i.e. qu'il existe un entier $T > 0$ tel que $\alpha = [\overline{a_0, a_1, ..., a_{T-1}}]$. Alors, $a_0 = a_T \neq 0$ donc $\alpha > a_0 \geq 1$. Montrons que $\alpha^* \in]-1\,;0[$. En reprenant le début de la démonstration de la proposition 1.1.10 et en remarquant qu'ici $N = 0$ donc $\alpha_N = \alpha_0 = \alpha$, on en déduit que α est racine du polynôme $P := q_{T-1}X^2 + (q_{T-2} - p_{T-1})X - p_{T-2}$ où $\dfrac{p_n}{q_n}$ est la $n-$ième réduite de α. Comme $\alpha > 1$, pour montrer que $\alpha^* \in]0\,;1[$, il suffit de montrer que P admet une racine dans cet intervalle. Or, $P(0) = -p_{T-2} < 0$ et $P(-1) = q_{T-1} - q_{T-2} + p_{T-1} - p_{T-2}$. De plus, (p_n) et (q_n) sont croissante car $a_0 \geq 0$ (voir la note (1) page 14) donc $P(-1) \geq 0$ et si $P(-1)$ était nul alors on aurait $q_{T-1} - q_{T-2} = p_{T-1} - p_{T-2} = 0$ donc les réduites R_{T-1} et R_{T-2} seraient égales ce qui est impossible. Ainsi, $P(-1) > 0$ et on conclut à l'aide du théorème des valeurs intermédiaires. ■

Cette propriété des irrationnels quadratiques réduits va servir pour étudier le développement en fraction continuée de $\sqrt{d}$ où d est un entier qui n'est pas un carré parfait en fournissant un algorithme permettant de déterminer la période et de calculer les réduites de ce développement.

Proposition 1.1.14. — *Soit d un entier naturel qui n'est pas un carré parfait. On pose $\alpha := \left\lfloor \sqrt{d} \right\rfloor + \sqrt{d}$ et on note (α_n) la suite des quotients complets de α.*

1. *Le développement en fraction continuée de $\sqrt{d}$ est périodique à partir du rang 1. Plus précisément, ce développement est de la forme*
$$\sqrt{d} = \left[a_0, \overline{a_1, a_2, ..., a_{T-1}, 2a_0}\right].$$
2. *Il existe deux suites d'entiers naturels non nuls (u_n) et (v_n) telles que, pour tout entier $n \in \mathbb{N}$, $\alpha_n = \dfrac{u_n + \sqrt{d}}{v_n}$ avec $u_n \leq a_0$ et v_n qui divise $d - u_n^2$.*
3. *La plus petite période T dans le développement $\sqrt{d}$ est le premier indice k tel que $a_k = 2a_0$.*
4. *S'il existe un entier $N \in [\![1, T-1]\!]$ tel que v_N divise u_N alors $T = 2N$ et, en particulier, T est pair.*

Preuve

1. Notons $\sqrt{d} = [a_0, a_1, ..., a_n, ...]$ le développement en fraction continuée de $\sqrt{d}$. On a donc, en particulier, $a_0 = \left\lfloor \sqrt{d} \right\rfloor$. Ecrivons, de même, $\alpha = [a_0', a_1', ..., a_n', ...]$ le développement de α. Remarquons que α est irrationnel quadratique car α est racine de $(X - a_0)^2 - d$. De plus, par définition, $\alpha > 1$ (car, 0 et 1 étant des carrés parfaits, $d \geq 2$) et $\alpha^* = a_0 - \sqrt{d} \in]-1\,;0[$ puisque $a_0 = \left\lfloor \sqrt{d} \right\rfloor$. Ainsi, α est réduit. On déduit alors de la proposition 1.1.13 que son développement est purement périodique. De plus, comme $a_0' = \lfloor \alpha \rfloor = 2a_0$, ce développement est de la forme $\alpha = \left[\overline{2a_0, a_1', ..., a_{T-1}'}\right]$. Prenons pour T la plus petite période de ce développement. On en déduit que le développement de $\sqrt{d} = \alpha - a_0$ est $\left[a_0, \overline{a_1', a_2', ..., a_{T-1}', 2a_0}\right] = \left[a_0, \overline{a_1, a_2, ..., a_{T-1}, 2a_0}\right]$ car, par construction de α, pour tout $n \geq 1$, $a_n' = a_n$.

2. Construisons les suites (u_n) et (v_n) par récurrence. Pour $n=0$, $\alpha_0=\alpha=a_0+\sqrt{d}$ donc $u_0=a_0$ et $v_0=1$. Supposons qu'on a construit u_n et v_n. Alors, en rappelant que $a'_n=\lfloor\alpha_n\rfloor$,

$$\alpha_n=\frac{u_n+\sqrt{d}}{v_n}=a'_n+\frac{u_n-a'_nv_n+\sqrt{d}}{v_n}=a'_n+\frac{-u_{n+1}+\sqrt{d}}{v_n}$$

en posant $u_{n+1}:=a'_nv_n-u_n$ et, par suite,

$$\alpha_n=a'_n+\frac{d-u_{n+1}^2}{v_n(u_{n+1}+\sqrt{d})}=a'_n+\frac{1}{\frac{u_{n+1}+\sqrt{d}}{\frac{d-u_{n+1}^2}{v_n}}}=a'_n+\frac{1}{\frac{u_{n+1}+\sqrt{d}}{v_{n+1}}}$$

en posant $v_{n+1}:=\dfrac{d-u_{n+1}^2}{v_n}$. Ainsi, on peut affirmer que $\alpha_{n+1}=\dfrac{u_{n+1}+\sqrt{d}}{v_{n+1}}$. Par définition, u_{n+1} est un entier. De plus, comme $u_n\leq a_0<\sqrt{d}$, $\alpha_n=\dfrac{u_n+\sqrt{d}}{v_n}>\dfrac{2u_n}{v_n}$ donc, comme $\alpha_n>1$ [(8)], $a'_n>\dfrac{\alpha_n}{2}>\dfrac{u_n}{v_n}$ ce qui assure que $u_{n+1}>0$. Par ailleurs, $u_{n+1}=a'_nv_n-u_n<\alpha_nv_n-u_n=\sqrt{d}$ donc $u_{n+1}\leq a_0$. Il ne reste plus qu'à montrer que v_n divise $d-u_{n+1}^2$ ce qui prouvera à la fois que v_{n+1} est entier et que v_{n+1} divise $d-u_{n+1}^2$. Pour le voir, il suffit d'écrire $d-u_{n+1}^2=d-(a'_nv_n-u_n)^2=d-u_n^2-v_n({a'_n}^2v_n-2a'_nu_n)$ et d'utiliser le fait que, par hypothèse de récurrence, v_n divise $d-u_n^2$.

3. Montrons que T est le premier indice tel que $a_T=2a_0$. Il est équivalent de montrer qu'aucun des coefficients a_1, a_2, ..., a_{T-1} n'est égal à $2a_0$. Pour cela, remarquons tout d'abord que, pour tout $j\in[\![1,T-1]\!]$, $\alpha_j\neq\alpha$. En effet, dans le cas contraire, on aurait $\alpha=[2a_0,a_1,...,a_{j-1},\alpha]=\overline{[2a_0,a_1,...,a_{j-1}]}$ et donc le développement serait périodique de période $j<T$ ce qui contredit la définition de T. Supposons alors que $j\geq1$ est un indice quelconque tel que $a_j=2a_0$. Ainsi, comme $j\geq1$, $a'_j=a_j$ donc $a'_j=2a_0$ et ainsi $u_{j+1}=2a_0v_j-u_j$. Or, $u_j\leq a_0$ et $u_{j+1}\leq a_0$ donc $v_j=1$ et $u_{j+1}=u_j=a_0$. On conclut donc que $\alpha_j=a_0+\sqrt{d}=\alpha$ et ainsi, d'après la remarque précédente, $j\notin[\![1,T-1]\!]$ ce qui achève la démonstration.

4. Supposons que $N\in[\![1,T-1]\!]$ soit tel que v_N divise u_N. On va montrer par une récurrence finie que, pour tout $j\in[\![0,N-1]\!]$, on a les égalités

$$u_{N+j+1}=u_{N-j},\qquad v_{N+j+1}=v_{N-j-1}\qquad\text{et}\qquad a'_{N+j+1}=a'_{N-j-1}\tag{1.3}$$

Pour $j=0$, sachant que v_N divise u_N, $\dfrac{2u_N}{v_N}$ est entier. Or, $u_N<\sqrt{d}$ donc $\dfrac{2u_N}{v_N}<\dfrac{u_N+\sqrt{d}}{v_N}$ et, comme on l'a vu dans la preuve de la proposition 1.1.13, $\alpha^*_N=\dfrac{u_N-\sqrt{d}}{v_N}$ est un irrationnel quadratique réduit donc $\dfrac{u_N-\sqrt{d}}{v_N}\in\,]-1\,;0[$. Dès lors, $\dfrac{u_N+\sqrt{d}}{v_N}=\dfrac{2u_N}{v_N}-\dfrac{u_N-\sqrt{d}}{v_N}<\dfrac{2u_N}{v_N}+1$. Il s'ensuit que $a'_n=\left\lfloor\dfrac{u_N+\sqrt{d}}{v_N}\right\rfloor=\dfrac{2u_N}{v_N}$. Or, par définition, $u_{N+1}=a'_Nv_N-u_N$ donc $u_{N+1}=u_N$. De plus, sachant que $u_{N+1}^2+v_{N+1}v_N=d=u_N^2+v_Nv_{N-1}$, on peut affirmer que $v_{N+1}=v_{N-1}$. Dès lors,

$$a'_{N+1}=\lfloor\alpha_{N+1}\rfloor=\left\lfloor\frac{u_{N+1}+\sqrt{d}}{v_{N+1}}\right\rfloor=\left\lfloor\frac{u_N+\sqrt{d}}{v_{N-1}}\right\rfloor.$$

Or, $u_N=a'_{N-1}v_{N-1}-u_{N-1}$ donc

$$a'_{N+1}=\left\lfloor a'_{N-1}-\frac{u_{N-1}-\sqrt{d}}{v_{N-1}}\right\rfloor=\lfloor a'_{N-1}-\alpha^*_{N-1}\rfloor=a'_{N-1}$$

(8). En effet, α_n est quadratique réduit d'après la démonstration de la proposition 1.1.13.

car α^*_{N-1} est réduit donc strictement compris entre -1 et 0.
Supposons que les relations 1.3 soient vraies pour un certain $j \in [\![0, N-2]\!]$. Alors,

$$\begin{aligned} u_{N+j+2} &= a'_{N+j+1}v_{N+j+1} - u_{N+j+1} = a'_{N-j-1}v_{N-j-1} - u_{N-j} \\ &= a'_{N-j-1}v_{N-j-1} - (a'_{N-j-1}v_{N-j-1} - u_{N-j-1}) \end{aligned}$$

donc $u_{N+j+2} = u_{N-j-1}$. Par suite, en écrivant que

$$u^2_{N+j+2} - v_{N+j+2}v_{N+j+1} = d = u^2_{N-j-1} + v_{N-j-1}v_{N-j-2} = u^2_{N+j+2} + v_{N+j+1}v_{N-j-2},$$

on est assuré que $v_{N+j+2} = v_{N-j-2}$. Enfin, en raisonnant comme précédemment,

$$\begin{aligned} a'_{N+j+1} = \lfloor \alpha_{N+j+1} \rfloor &= \left\lfloor \frac{u_{N+j+1} + \sqrt{d}}{v_{N+j+1}} \right\rfloor = \left\lfloor \frac{u_{N-j} + \sqrt{d}}{v_{N-j-1}} \right\rfloor \\ &= \left\lfloor a'_{N-j-1} - \frac{u_{N-j-1} - \sqrt{d}}{v_{N-j-1}} \right\rfloor = \lfloor a'_{N-j-1} - \alpha^*_{N-j-1} \rfloor \end{aligned}$$

et donc $a_{N+j+1} = a'_{N-j-1}$ car $\alpha^*_{N-j-1} \in]-1\,;0[$ ce qui achève la récurrence.
Si on applique ceci pour $j = N-1$, on obtient, en particulier, que $a'_0 = a'_{2N}$ i.e. comme $N \geq 1$, $2a_0 = a_{2N}$. Or, d'après le point **3.**, sachant que $2 \leq 2N \leq 2(T-1) < 2T$, on en déduit que $2N = T$. ■

Exemple 1.1.15. — Pour un entier qui n'est pas un carré parfait donné d, la démonstration nous donne non seulement un critère pour déterminer une période minimale dans le développement en fraction continuée de $\sqrt{d}$ (on s'arrête dès qu'un coefficient d'une réduite est égale à $2\lfloor d \rfloor$) mais, qui plus est, il fournit un algorithme pour déterminer ce développement. Par exemple, si $d = 21$, on part de $\alpha = \lfloor \sqrt{21} \rfloor + \sqrt{21} = 4 + \sqrt{21}$ puis on écrit successivement :

$$\begin{aligned} \alpha &= 8 + (\sqrt{21} - 4) = 8 + \frac{5}{\sqrt{21}+4} = \boxed{8} + \frac{1}{\alpha_1} \\ \alpha_1 &= \frac{\sqrt{21}+4}{5} = 1 + \frac{\sqrt{21}-1}{5} = 1 + \frac{20}{5(\sqrt{21}+1)} = \boxed{1} + \frac{1}{\alpha_2} \\ \alpha_2 &= \frac{\sqrt{21}+1}{4} = 1 + \frac{\sqrt{21}-3}{4} = 1 + \frac{12}{4(\sqrt{21}+3)} = \boxed{1} + \frac{1}{\alpha_3} \\ \alpha_3 &= \frac{\sqrt{21}+3}{3} = 2 + \frac{\sqrt{21}-3}{3} = 2 + \frac{12}{3(\sqrt{21}+3)} = \boxed{2} + \frac{1}{\alpha_4} \\ \alpha_4 &= \frac{\sqrt{21}+3}{4} = 1 + \frac{\sqrt{21}-1}{4} = 1 + \frac{20}{4(\sqrt{21}+1)} = \boxed{1} + \frac{1}{\alpha_5} \\ \alpha_5 &= \frac{\sqrt{21}+1}{5} = 1 + \frac{\sqrt{21}-4}{5} = 1 + \frac{5}{5(\sqrt{21}+4)} = \boxed{1} + \frac{1}{\alpha} \end{aligned}$$

donc $\alpha = [8, 1, 1, 2, 1, 1, \alpha] = \left[\overline{8, 1, 1, 2, 1, 1}\right]$ et ainsi $\sqrt{21} = \left[4, \overline{1, 1, 2, 1, 1, 8}\right]$.

1.2 Le cas $n = 1$

Etant donné deux entiers naturels a et b premiers entre eux, il est classique de résoudre l'équation diophantienne $(E_1) : ax - by = 1$ en cherchant une solution particulière grâce à l'algorithme d'Euclide puis l'ensemble des solutions à l'aide du lemme de Gauss. On propose ici une autre façon de faire (mais qui, à y regarder de près, est sensiblement la même) en utilisant des fractions continuées.

Proposition 1.2.1. — *Soit a et b deux entiers naturels non nuls et premiers entre eux. Alors, l'équation $(E_1) : ax - by = 1$ admet une infinité de solutions dans $\mathbb{N}^2$.*
Plus précisément,

1. *si $b = 1$ alors l'ensemble des solutions de (E_1) dans $\mathbb{N}^2$ est $\{(k, ka+1) \,|\, k \in \mathbb{N}\}$;*
2. *sinon, on note $R_{m-1} = \dfrac{p_{m-1}}{q_{m-1}}$ l'avant-dernière réduite dans le développement en fraction continuée du rationnel $\dfrac{a}{b}$ et alors l'ensemble des solutions de (E_1) dans $\mathbb{N}^2$ est*

$$\{(kb - (-1)^m q_{m-1}, ka - (-1)^m p_{m-1}) \,|\, k \in K_m\}$$

où $K_m = \mathbb{N}$ si m est impair et $K_m = \mathbb{N}^*$ si m est pair.

Preuve. — Soit $(x, y) \in \mathbb{N}^2$ une solution de (E_1).

1. Si $b = 1$ alors $y = 1 + ax$ donc le couple (x, y) est de la forme $(k, ka+1)$ où $k \in \mathbb{N}$. Réciproquement, tout couple de cette forme est une solution dans $\mathbb{N}^2$ de (E_1).
2. Si $b \neq 1$, posons $r = \dfrac{a}{b}$ et notons R_m la dernière réduite dans le développement en fraction continuée de r de sorte que $r = R_m = \dfrac{p_m}{q_m}$ et donc, puisque les écritures sont irréductibles, $a = p_m$ et $b = q_m$. Comme $b \neq 1$, r n'est pas entier et donc $m \geq 1$. Dès lors, d'après le lemme 1.1.2, $aq_{m-1} - bp_{m-1} = (-1)^{m+1}$ donc $a(x + (-1)^m q_{m-1}) = b(y + (-1)^m p_{m-1})$. Comme a et b sont premiers entre eux, on en déduit qu'il existe un entier relatif k tel que $x = kb - (-1)^m q_{m-1}$ et $y = ka - (-1)^m p_{m-1}$. On cherche de plus x et y dans $\mathbb{N}$ donc cela impose $k \geq \dfrac{(-1)^m q_{m-1}}{b}$ et $k \geq \dfrac{(-1)^m p_{m-1}}{a}$. Or, comme $a_0 = \left\lfloor \dfrac{a}{b} \right\rfloor \geq 0$ et $q_m = b \neq 1$, les suites (p_n) et (q_n) sont strictement croissantes [9] donc $0 < \dfrac{p_{m-1}}{a} = \dfrac{p_{m-1}}{p_m} < 1$ et $0 < \dfrac{q_{m-1}}{b} = \dfrac{q_{m-1}}{q_m} < 1$ et ainsi les conditions sur k se réduisent à $k \geq 1$ si m est pair et $k \geq 0$ si m est impair.
   Réciproquement, on vérifie que tous les couples ainsi obtenus sont solutions de (E_1). ■

Exemple 1.2.2. — Considérons l'équation $21x - 8y = 1$. Comme

$$\frac{21}{8} = 2 + \frac{5}{8} = 2 + \frac{1}{1 + \dfrac{3}{5}} = 2 + \frac{1}{1 + \dfrac{1}{1 + \dfrac{2}{3}}} = 2 + \frac{1}{1 + \dfrac{1}{1 + \dfrac{1}{1 + \dfrac{1}{2}}}},$$

$\dfrac{a}{b} = R_4 = [2, 1, 1, 1, 2]$. Ainsi, $n = 4$, $R_{n-1} = R_3 = [2, 1, 1, 1] = \dfrac{8}{3}$ et n est pair donc l'ensemble des solutions de $21x - 8y = 1$ dans $\mathbb{N}^2$ est $\{(8k - 3, 21k - 8) \,|\, k \in \mathbb{N}^*\}$.

1.3 Le cas $n = 2$

1.3.1 L'équation de Pell-Fermat

On appelle *équation de Pell-Fermat* l'équation d'inconnue $(x, y) \in \mathbb{N}^2$

$$(PF_d) : x^2 - dy^2 = 1$$

où d est un entier relatif.

(9). En tout cas, au moins à partir du rang $m - 1$, voir la note (1) page 14.

Il est clair que l'équation (PF_d) admet toujours la solution $(x, y) = (1, 0)$. Cette solution est appelée *solution triviale* de (PF_d). Remarquons tout d'abord que si $d < 0$ alors l'équation n'a qu'un nombre fini de solutions (qu'on peut déterminer, pour une valeur de d donnée, par exemple par une méthode de crible) et si $d = k^2$ est un carré parfait alors (PF_d) équivaut à $(x - ky)(x + ky) = 1$ qui n'a d'autre solution que la solution triviale. Ces deux cas ne présentant pas beaucoup d'intérêt, on fait dans toute la suite, l'hypothèse que d est un entier naturel qui n'est pas un carré parfait.

L'étude d'une telle équation remonte à l'antiquité [(10)] mais elle n'a trouvé de résolution définitive qu'au XVIIIe siècle. Il semble que le nom de Pell a été attaché à cette équation suite à une confusion d'Euler [(11)] qui a confondu Pell [(12)] avec un autre mathématicien anglais, en l'occurrence Wallis [(13)]. En Europe, la première méthode de résolution est due à Brouncker [(14)] en 1657 mais les mathématiciens indiens Brahmagupta [(15)] et Bhāskara II [(16)] avaient mis au point, entre le VIIe et le XIIe siècle, un algorithme de résolution connu aujourd'hui sous le nom de *méthode chakravala*. Par la suite, Wallis et Fermat [(17)] ont été les premiers à affirmer que l'équation (PF_d) avait toujours une infinité de solutions avant que la démonstration ne soit donnée par Lagrange en 1766.

Le théorème de Dirichlet [(18)] suivant permet de montrer relativement rapidement que l'ensemble des solutions de (PF_d) est infini mais sans toutefois donner la forme des solutions. La démonstration de ce théorème est basé sur le principe des tiroirs qu'on peut résumer ainsi : si l'on doit placer des paires de chaussettes dans différents tiroirs et s'il y a plus de paires de chaussettes que de tiroirs alors il y aura nécessairement un tiroir qui contiendra plusieurs paires de chaussettes.

Lemme 1.3.1. — *Soit α un nombre réel. Alors, pour tout $n \in \mathbb{N}^*$, il existe un rationnel $\frac{p}{q}$ tel que $\left|\alpha - \frac{p}{q}\right| < \frac{1}{qn}$ et $1 \leq q \leq n$.*

Preuve. — Soit $n \in \mathbb{N}^*$. On considère les $n+1$ réels $x_j = j\alpha - \lfloor j\alpha \rfloor$ pour $j \in [\![0, n]\!]$. Ces $n+1$ réels appartiennent tous à l'intervalle $[0\,;1[$. Or, on peut partitionner celui-ci en les n intervalles $I_k = \left[\frac{k}{n}\,;\frac{k+1}{n}\right[$ pour $k \in [\![0, n-1]\!]$. Alors, d'après le principe des tiroirs, il existe un intervalle I_k qui contient au moins deux x_j. Dès lors, il existe deux indices $j_1 < j_2$ dans $[\![0, n]\!]$ tels que $|x_{j_2} - x_{j_1}| < \frac{1}{n}$ i.e. $|j_2\alpha - \lfloor j_2\alpha \rfloor - (j_1\alpha - \lfloor j_1\alpha \rfloor)| < \frac{1}{n}$. Définissons alors les entiers $q = j_2 - j_1 \geq 1$ et $p = \lfloor j_2\alpha \rfloor - \lfloor j_1\alpha \rfloor$. On a $|q\alpha - p| < \frac{1}{n}$ donc, comme $q > 0$, $\left|\alpha - \frac{p}{q}\right| < \frac{1}{qn}$. De plus, j_1 et j_2 sont dans $[\![0, n]\!]$ donc $q \leq n$. ■

Corollaire 1.3.2. *(théorème de Dirichlet) — Soit α un nombre irrationnel. Alors, il existe une infinité de rationnels $\frac{p}{q}$ avec $q > 0$ tels que*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}. \tag{1.4}$$

(10). Voir l'article [22] qui aborde le problème dit des *boeufs au soleil* qui aurait été posé par Archimède à Eratosthène.
(11). Pour une fois qu'Euler se trompe sur quelque chose, il nous a semblé bon de le signaler.
(12). John Pell, 1661–1685.
(13). John Wallis, 1616–1703.
(14). Lord William Brouncker, 1620–1684.
(15). Brahmagupta, 598–668.
(16). Bhāskara II, aussi appelé Bhāskarācārya,1114–1185.
(17). Pierre de Fermat, 160 ?–1665 (date de naissance incertaine, entre 1601 et 1608).
(18). Johann Peter Gustav Lejeune Dirichlet, 1805–1859.

Preuve. — L'existence de tels rationnels est évidente. Il suffit par exemple de prendre $\frac{p}{q} = \frac{\lfloor \alpha \rfloor}{1}$ car alors, par définition, $\left|\alpha - \frac{p}{q}\right| < 1 = \frac{1}{q^2}$.

Supposons à présent que l'ensemble $\mathcal{R}$ des rationnels qui vérifient (1.4) soit fini et introduisons $\varepsilon = \min_{r \in \mathcal{R}} |\alpha - r|$. Comme α est irrationnel et $\mathcal{R}$ fini, $\varepsilon > 0$. Soit alors un entier $n \in \mathbb{N}^*$ tel que $\frac{1}{n} < \varepsilon$. D'après le lemme 1.3.1, il existe un rationnel $\frac{p}{q}$ tel que $\left|\alpha - \frac{p}{q}\right| < \frac{1}{qn}$ et $1 \leq q \leq n$. Alors, comme $\frac{1}{qn} \leq \frac{1}{n}$, $\left|\alpha - \frac{p}{q}\right| < \varepsilon$ ce qui impose que $\frac{p}{q} \notin \mathcal{R}$. Or, comme $q \leq n$, $\frac{1}{qn} \leq \frac{1}{q^2}$ et donc $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$ ce qui prouve que $\frac{p}{q}$ vérifie (1.4). On aboutit à une contradiction donc $\mathcal{R}$ est infini. ■

Proposition 1.3.3. — *Si $d \in \mathbb{N}$ n'est pas un carré parfait alors l'équation (PF_d) admet une solution non triviale.*

Preuve. — Appliquons le corollaire 1.3.2 à $\alpha = \sqrt{d} \notin \mathbb{Q}$. Il existe une infinité de couples $(x, y) \in \mathbb{N}^2$ tels que $\left|\sqrt{d} - \frac{x}{y}\right| < \frac{1}{y^2}$. Pour un tel couple, on a $\left|x - y\sqrt{d}\right| < \frac{1}{y}$ et donc

$$\left|x + y\sqrt{d}\right| = \left|x - y\sqrt{d} + 2y\sqrt{d}\right| < \frac{1}{y} + 2y\sqrt{d}.$$

On en déduit qu'il existe une infinité de couple $(x, y) \in \mathbb{N}^2$ tels que

$$\left|x^2 - dy^2\right| = \left|x - y\sqrt{d}\right| \times \left|x + y\sqrt{d}\right| < \frac{1}{y^2} + 2\sqrt{d} < 2\sqrt{d} + 1.$$

Il s'ensuit qu'il existe un entier $m \in \mathbb{Z}^*$ tel que l'équation $x^2 - dy^2 = m$ a une infinité de solutions. Le nombre de classes de congruence modulo $|m|$ étant fini, on en déduit qu'il existe deux solutions distinctes (x_1, y_1) et (x_2, y_2) telles que $x_1 \equiv x_2 \mod (|m|)$, $y_1 \equiv y_2 \mod (|m|)$ et $x_1 \neq x_2$. En remarquant que deux telles solutions ont nécessairement le même P.G.C.D. δ (car δ^2 divise m), on peut, toujours, quitte à remplacer m par $\frac{m}{\delta^2}$, supposer que $\mathrm{PGCD}(x_1, y_1) = \mathrm{PGCD}(x_2, y_2) = 1$. Alors, en multipliant les égalités $x_1^2 - dy_1^2 = m$ et $x_2^2 - dy_2^2 = m$, il vient, en utilisant l'identité de Brahmagupta

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - x_2y_1)^2 = m^2.$$

Notons que, modulo $|m|$,

$$x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_1^2 \equiv m \equiv 0 \quad \text{et} \quad x_1y_2 - x_2y_1 \equiv x_1y_1 - x_1y_1 \equiv 0$$

donc il existe deux entiers u et v tels que $x_1x_2 - dy_1y_2 = um$ et $x_1y_2 - x_2y_1 = vm$. Dès lors, $(|u|, |v|)$ vérifie $|u|^2 - d|v|^2 = 1$. Remarquons pour finir que $(|u|, |v|) \neq (1, 0)$ car alors on aurait $x_1y_2 - x_2y_1 = 0$ et donc $x_1 = x_2$ (puisque $\mathrm{PGCD}(x_1, y_1) = \mathrm{PGCD}(x_2, y_2) = 1$), ce qui est exclu. Ainsi, on a bien trouvé une solution non triviale de (PF_d). ■

Définition 1.3.4. — Soit $d \in \mathbb{N}$ un entier qui n'est pas un carré parfait. On appelle solution fondamentale de l'équation de Pell-Fermat (PF_d) l'unique solution non triviale (x_1, y_1) de (PF_d) telle que, pour toute autre solution non triviale (x, y) de (PF_d), on ait $x > x_1$.

Remarque 1.3.5. — Cette solution existe d'après la proposition précédente et est bien unique car si $x = x_1$ alors, comme $x^2 - dy^2 = 1 = x_1^2 - dy_1^2$, on peut en déduire que $y = y_1$.

Corollaire 1.3.6. — *Si $d \in \mathbb{N}$ n'est pas un carré parfait alors l'équation (PF_d) admet une infinité de solution. De plus, si (x_1, y_1) est la solution fondamentale de (PF_d) alors toute solution de (PF_d) est de la forme (x_n, y_n) où les suites d'entiers (x_n) et (y_n) sont définies par la relation*

$$\forall n \in \mathbb{N},\ x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n.$$

Preuve. — On vérifie par une récurrence immédiate que les nombres x_n et y_n définis par la relation $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$ sont des entiers naturels pour tout $n \in \mathbb{N}$ et que les deux suites (x_n) et (y_n) sont strictement croissantes (car $x_1 \geq 2$). De plus, en utilisant le fait que $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$ [(19)]

$$x_n^2 - dy_n^2 = (x_n + y_n\sqrt{d})(x_n - y_n\sqrt{d}) = (x_1 + y_1\sqrt{d})^n(x_1 - y_1\sqrt{d})^n = (x_1^2 - dy_1^2)^n = 1$$

donc (x_n, y_n) est une solution de (PF_d). La stricte croissance de (x_n) assure qu'il y a donc une infinité de solutions non triviales.

Supposons, par l'absurde, que (x, y) soit une solution de (PF_d) qui ne soit pas de la forme précédente. Comme la suite $(x_1 + y_1\sqrt{d})^n$ est strictement croissante et comme la solution triviale $(1, 0)$ est obtenue pour $n = 0$, $x > 1$ et donc $x + y\sqrt{d} > (x_1 + y_1\sqrt{d})^0$. Il s'ensuit qu'il existe un entier n tel que $(x_1 + y_1\sqrt{d})^n < x + y\sqrt{d} < (x_1 + y_1\sqrt{d})^{n+1}$ et donc

$$1 < \frac{x + y\sqrt{d}}{(x_1 + y_1\sqrt{d})^n} < x_1 + y_1\sqrt{d}.$$

Etant donné que $\dfrac{1}{(x_1 + y_1\sqrt{d})^n} = (x_1 - y_1\sqrt{d})^n = x_n - y_n\sqrt{d}$, on en déduit que

$$1 < (x + y\sqrt{d})(x_n - y_n\sqrt{d}) < x_1 + y_1\sqrt{d}.$$

Or, si on écrit $(x+y\sqrt{d})(x_n-y_n\sqrt{d}) = u+v\sqrt{d}$ alors, comme ci-dessus, $u-v\sqrt{d} = (x-y\sqrt{d})(x_n+y_n\sqrt{d})$ et donc $u^2 - dv^2 = 1$ ce qui montre que $(|u|, |v|)$ est une solution de (PF_d) non triviale. De plus, $u + v\sqrt{d} > 1$ donc $u - v\sqrt{d} = (u + v\sqrt{d})^{-1} \in]0\,;1[$ ce qui assure que $u > 0$ et $v > 0$. De plus, comme $u^2 - dv^2 = x_1^2 - dy_1^2$, $(x_1 - u)(x_1 + u) = d(y_1 - v)(y_1 + v)$ et ainsi x_1 et u sont rangés dans le même ordre que y_1 et v. Or, $u + v\sqrt{d} < x_1 + y_1\sqrt{d}$ donc $u < x_1$ (et $v < y_1$). On a donc trouvé une solution non triviale (u, v) de (PF_d) telle que $u < x_1$ ce qui contredit la définition de x_1. Ainsi, les solutions de (PF_d) sont exactement les couples (x_n, y_n) $(n \in \mathbb{N})$. ■

Dans cette partie, on a entièrement résolu (PF_d) à l'aide de raisonnements qui s'orientent vers la théorie des corps quadratiques (la conjugaison et la norme sur $\mathbb{Q}[\sqrt{d}]$ n'étaient jamais bien loin dans les calculs précédents !). Cependant, la méthode suivie ne permet de résoudre l'équation (PF_d) que si on sait trouver la solution fondamentale. Or, l'existence de cette solution est basée sur le théorème de Dirichlet qui, par essence, n'est pas explicite. On va à présent voir comment qu'on peut mettre à profit l'étude des fractions continuées de $\sqrt{d}$ faite précédemment pour déterminer une telle solution et élargir le raisonnement à une classe plus vaste d'équations : les équations de Pell-Fermat généralisées.

1.3.2 Les équations de Pell-Fermat généralisées

On appelle *équation de Pell-Fermat généralisée* une équation d'inconnue $(x, y) \in \mathbb{N}^2$ de la forme

$$(PF_{d,m}) : x^2 - dy^2 = m$$

où d et m sont des entiers premiers entre eux.

(19). On peut le justifier, par exemple, en utilisant le fait que la conjugaison est un automorphisme de $\mathbb{Q}[\sqrt{d}]$.

Ici aussi, le cas où d est négatif ou le cas où d est un carré parfait n'a pas beaucoup d'intérêt donc on suppose que $d > 0$ n'est pas un carré. Il s'ensuit que si $m = 0$, $(PF_{d,m})$ n'a pas de solution [(20)] donc on peut également écarter ce cas-là. Il est clair que si (x, y) est une solution de $(PF_{d,m})$ telle que x et y ne sont pas premiers entre eux, alors le carré de $\delta := \mathrm{PGCD}(x, y)$ divise m donc en divisant $(PF_{d,m})$ par δ^2, on est ramené à résoudre une certaine équation $(PF_{d,m'})$ avec $m' < m$ dont les inconnues sont des entiers premiers entre eux. On peut donc toujours supposer que $\delta = 1$.

Remarquons que, même sous ces conditions, l'équation $(PF_{d,m})$ n'a pas toujours une solution. Par exemple, pour $(d, m) = (7, 5)$, il ne peut y avoir de solution car on aurait sinon $x^2 \equiv 5 \mod (7)$ ce qui est impossible car les restes possibles d'un carré modulo 7 sont 0, 1, 2 ou 4.

Dans ce qui suit, on va donner une condition nécessaire et suffisante pour que $(PF_{d,m})$ ait une solution dans le cas où $1 \leq |m| < \sqrt{d}$ et on montrera qu'alors $(PF_{d,m})$ a une infinité de solutions. On peut toujours imposer que x et y sont non nuls. Le cas $x = 0$ ne peut pas se produire car alors $-dy^2 = m$ ce qui est absurde car $1 \leq |m| < \sqrt{d}$ et le cas $y = 0$ ne se produit que si m est un carré parfait et dans ce cas, on dira que la solution $(\sqrt{m}, 0)$ est une solution triviale de $(PF_{d,m})$.

Le résultat suivant est à mettre en rapport avec la proposition 1.3.3 dans l'idée qu'une solution de $(PF_{d,m})$ correspond à une bonne approximation rationnelle de $\sqrt{d}$.

Lemme 1.3.7. — *Soit d un entier naturel qui n'est pas un carré et m un entier relatif tel que $1 \leq |m| < \sqrt{d}$. Si x et y sont deux entiers naturels non nuls et premiers entre eux tels que (x, y) est une solution de $(PF_{d,m})$ alors $\dfrac{x}{y}$ est une réduite dans le développement en fraction continuée de $\sqrt{d}$.*

Preuve. — Soit x et y deux entiers naturels non nuls premiers entre eux tels que $x^2 - dy^2 = m$. Alors, $x - y\sqrt{d} = \dfrac{m}{x + y\sqrt{d}}$.

Si $m > 0$ alors $x^2 = m + dy^2 > dy^2$ donc $x > y\sqrt{d}$ et ainsi

$$\left|\sqrt{d} - \frac{x}{y}\right| = \frac{|m|}{xy + y^2\sqrt{d}} < \frac{\sqrt{d}}{xy + y^2\sqrt{d}} < \frac{\sqrt{d}}{2y^2\sqrt{d}} = \frac{1}{2y^2}.$$

Il s'ensuit, d'après la proposition 1.1.8, que $\dfrac{x}{y}$ est une réduite dans le développement de $\sqrt{d}$ en fraction continuée (car $\sqrt{d}$ est irrationnel).

Si $m < 0$ alors $dy^2 = x^2 - m > x^2$ donc $y\sqrt{d} > x$ et ainsi

$$\left|\frac{1}{\sqrt{d}} - \frac{y}{x}\right| = \frac{|m|}{\sqrt{d}(x^2 + xy\sqrt{d})} < \frac{\sqrt{d}}{\sqrt{d}(2x^2)} = \frac{1}{2x^2}.$$

De même, $\dfrac{y}{x}$ est une réduite dans le développement en fraction continuée de $\sqrt{d}^{-1}$. Ecrivons alors $\sqrt{d} = [a_0, a_1, ..., a_n, ...]$ et $\sqrt{d}^{-1} = [a'_0, a'_1, ..., a'_n, ...]$ les développements en fractions continuées de $\sqrt{d}$ et $\sqrt{d}^{-1}$ et notons (δ'_n) la suite des quotients complets de $\sqrt{d}^{-1}$. Comme $\sqrt{d} > 1$, $a'_0 = \left\lfloor \sqrt{d}^{-1} \right\rfloor = 0$ donc $\delta'_1 = 0 + \dfrac{1}{\sqrt{d}^{-1} - 0} = \sqrt{d}$ et ainsi $a'_1 = \lfloor \delta'_1 \rfloor = \left\lfloor \sqrt{d} \right\rfloor = a_0$. Il s'ensuit par récurrence que, pour tout $n \geq 1$, $a'_n = a_{n-1}$ et ainsi le développement en fractions continuées de $\sqrt{d}^{-1}$ est $[0, a_0, a_1, ..., a_{n-1}, ...]$. Si on note k l'entier tel que $\dfrac{y}{x}$ soit la $k-$ième réduite de $\sqrt{d}^{-1}$, remarquons que $k \neq 0$ car $y \neq 0$. Ainsi,

$$\frac{y}{x} = [0, a_0, a_1, ..., a_{k-1}] = 0 + \frac{1}{[a_0, a_1, ..., a_{k-1}]}$$

(20). Si $dy^2 = x^2$ alors il est clair que la valuation $p-$adique de d est paire pour tout nombre premier p donc d est un carré parfait.

donc $\frac{x}{y} = [a_0, a_1, ..., a_{k-1}]$ i.e. $\frac{x}{y}$ est la $(k-1)-$ième réduite dans le développement en fraction continuée de $\sqrt{d}$. ■

Cette propriété d'approximation diophantienne étant établie, on va pouvoir décrire complètement l'ensemble des solutions de $(PF_{d,m})$ lorsque $1 \leq |m| < \sqrt{d}$.

Théorème 1.3.8. — *Soit d un entier naturel qui n'est pas un carré parfait et soit m un entier relatif tel que $1 \leq |m| < \sqrt{d}$. On considère la suite (v_n) associée à $\sqrt{d}$ par la proposition 1.1.14, T la période minimale du développement de $\sqrt{d}$ en fraction continuée et $\frac{p_n}{q_n}$ la $n-$ième réduite de ce développement. On note, pour tout $\ell \in \mathbb{Z}$, $\mathcal{E}_\ell := \left\{ j \in [\![1, T]\!] \,\middle|\, (-1)^j v_j = \ell \right\}$.*

1. *Si T est pair, l'équation $(PF_{d,m})$ admet une solution non triviale si et seulement si $\mathcal{E}_m$ est non vide et, dans ce cas, l'ensemble des solutions non triviales (x, y) de $(PF_{d,m})$ avec $\mathrm{PGCD}(x, y) = 1$ est la réunion des ensembles $\{(p_{N+kT-1}, q_{N+kT-1}) \,|\, k \in \mathbb{N}\}$ pour N parcourant $\mathcal{E}_m$.*
2. *Si T est impair, l'équation $(PF_{d,m})$ admet une solution non triviale si et seulement si l'un, au moins, des deux ensembles $\mathcal{E}_m$ ou $\mathcal{E}_{-m}$ est non vide et alors l'ensemble des solutions non triviales (x, y) de $(PF_{d,m})$ avec $\mathrm{PGCD}(x, y) = 1$ est la réunion des ensembles $\{(p_{N+2kT-1}, q_{N+2kT-1}) \,|\, k \in \mathbb{N}\}$ pour N parcourant $\mathcal{E}_m$ et des ensembles $\left\{(p_{M+(2k+1)T-1}, q_{M+(2k+1)T-1}) \,\middle|\, k \in \mathbb{N}\right\}$ pour M parcourant $\mathcal{E}_{-m}$.*
3. *Dans tous les cas, si $(PF_{d,m})$ admet une solution non triviale alors elle admet une infinité de solutions.*

Preuve. — Notons (δ_n) la suite des quotients complets de $\sqrt{d}$. On sait que, pour tout $n \geq 1$ [(21)] $\delta_n = \frac{u_n + \sqrt{d}}{v_n}$ où les suites (u_n) et (v_n) sont définies dans la proposition 1.1.14. Alors, comme le développement de $\sqrt{d}$ est $T-$périodique à partir du rang 1, il en est de même de la suite $(\delta_n)_{n\geq 1}$ et, comme δ_n définit de manière unique u_n et v_n, on en déduit que les suites $(u_n)_{n\geq 1}$ et $(v_n)_{n\geq 1}$ sont également $T-$périodiques. Il s'ensuit que la suite (v_n) ne prend que les valeurs v_1, v_2, ..., v_T (certaines pouvant être identiques).

Montrons que, pour tout $n \geq 1$, $p_{n-1}^2 - dq_{n-1}^2 = (-1)^n v_n$. Soit $n \geq 2$. Alors, le développement en fraction continuée de $\sqrt{d}$ est

$$\sqrt{d} = [a_0, a_1, ..., a_n, ...] = [a_0, a_1, ..., a_{n-1}, \delta_n]$$

donc, d'après le lemme 1.1.2,

$$\sqrt{d} = \frac{p_{n-1}\delta_n + p_{n-2}}{q_{n-1}\delta_n + q_{n-2}} = \frac{p_{n-1}(u_n + \sqrt{d}) + v_n p_{n-2}}{q_{n-1}(u_n + \sqrt{d}) + v_n q_{n-2}}.$$

Il s'ensuit que

$$(q_{n-1}u_n + v_n q_{n-2})\sqrt{d} + dq_{n-1} = p_{n-1}\sqrt{d} + p_{n-1}u_n + v_n p_{n-2}$$

donc, par identification [(22)],

$$\begin{cases} p_{n-1} = q_{n-1}u_n + q_{n-2}v_n \\ dq_{n-1} = p_{n-1}u_n + p_{n-2}v_n \end{cases}. \tag{1.5}$$

(21). L'égalité n'a pas lieu pour $n = 0$ car (δ_n) est en fait la suite des quotients complets de $\alpha := \sqrt{d} + \left\lfloor \sqrt{d} \right\rfloor$ mais les deux suites coïncident seulement à partir du rang $n = 1$.

(22). Par exemple dans la $\mathbb{Q}-$base $(1, \sqrt{d})$ de $\mathbb{Q}[\sqrt{d}]$.

On en déduit, en utilisant également le point **2.** du lemme 1.1.2, que

$$\begin{aligned} p_{n-1}^2 - dq_{n-1}^2 &= p_{n-1}(q_{n-1}u_n + q_{n-2}v_n) - q_{n-1}(p_{n-1}u_n + p_{n-2}v_n) \\ &= (p_{n-1}q_{n-2} - q_{n-1}p_{n-1})v_n = (-1)^n v_n. \end{aligned}$$

De plus, si $n = 1$, $p_{n-1}^2 - dq_{n-1}^2 = a_0^2 - d$ et, d'après les relations établies dans la démonstration de la proposition 1.1.14, $v_1 = \dfrac{d - u_1^2}{v_0} = \dfrac{d - (2a_0v_0 - u_0)^2}{v_0} = \dfrac{d - (2a_0 - a_0)^2}{1} = d - a_0^2$ donc on a encore $p_{n-1}^2 - dq_{n-1}^2 = (-1)^n v_n$. Ainsi, cette relation est vraie pour tout $n \geq 1$.

1. On se place dans le cas où T est pair. Supposons que (x, y) est une solution non triviale de $(PF_{d,m})$ avec $\text{PGCD}(x, y) = 1$. On sait par le lemme 1.3.7 que $\dfrac{x}{y}$ est une réduite de $\sqrt{d}$. Ainsi, il existe un entier $j \in \mathbb{N}^*$ tel que $x = p_{j-1}$ et $y = q_{j-1}$. Il s'ensuit que $m = x^2 - dy^2 = p_{j-1}^2 - dq_{j-1}^2 = (-1)^j v_j$. De plus, si on note k le reste dans la division euclidienne de $j - 1$ par T, il existe un entier $N_j \in [\![1, T]\!]$ tel que $j = N_j + kT$. Comme (v_n) est $T-$périodique et comme T un nombre pair,

$$(-1)^{N_j} v_{N_j} = (-1)^{N_j + kT} v_{N_j + kT} = (-1)^j v_j = m$$

et, ainsi, $N_j \in \mathcal{E}_m$ donc $\mathcal{E}_m$ n'est pas vide. De plus, $(x, y) = (p_{N_j+kT-1}, q_{N_j+kT-1})$ appartient à la réunion des ensembles $\{(p_{N+kT-1}, q_{N+kT-1}) \,|\, k \in \mathbb{N}\}$ pour N parcourant $\mathcal{E}_m$.
Réciproquement, si $\mathcal{E}_m$ n'est pas vide et si (x, y) est de la forme (p_{N+kT-1}, q_{N+kT-1}) avec $N \in \mathcal{E}_m$ et $k \in \mathbb{N}$ alors, comme (v_n) est $T-$périodique et comme T est pair,

$$x^2 - dy^2 = p_{N+kT-1}^2 - dq_{N+kT-1}^2 = (-1)^{N+kT} v_{N+kT} = (-1)^N v_N = m$$

donc (x, y) est solution de $(PF_{d,m})$.

2. On se place à présent dans le cas où T est impair. Supposons que (x, y) soit une solution non triviale de $(PF_{d,m})$ avec $\text{PGCD}(x, y) = 1$. Alors, on montre, comme précédemment, qu'il existe un entier $j \in \mathbb{N}^*$ tel que $x = p_{j-1}$ et $y = q_{j-1}$ et $m = (-1)^j v_j$ et qu'on peut écrire $j = N_j + KT$ avec $K = \left\lfloor \frac{j-1}{T} \right\rfloor$ et $N_j \in [\![1, T]\!]$. Deux cas sont alors possibles.
<u>1er cas</u> : si $K = 2k$ est pair alors KT est pair et on peut raisonner comme dans le point **1.** pour montrer que $N_j \in \mathcal{E}_m$ donc $\mathcal{E}_m$ n'est pas vide et $(x, y) = (p_{N_j+2kT-1}, q_{N_j+2kT-1})$ appartient à la réunion des ensembles $\{(p_{N+2kT-1}, q_{N+2kT-1}) \,|\, k \in \mathbb{N}\}$ pour N parcourant $\mathcal{E}_m$.
<u>2e cas</u> : si $K = 2k + 1$ est impair alors, comme T est impair, KT est également impair. Dans ce cas, comme (v_n) est $T-$périodique,

$$(-1)^{N_j} v_{N_j} = (-1)^{N_j + (2k+1)T} v_{N_j + (2k+1)T} = -(-1)^j v_j = -m$$

et, ainsi, $N_j \in \mathcal{E}_{-m}$ donc $\mathcal{E}_{-m}$ n'est pas vide. De plus, $(x, y) = (p_{N_j+(2k+1)T-1}, q_{N_j+(2k+1)T-1})$ appartient à la réunion des ensembles $\left\{(p_{M+(2k+1)T-1}, q_{M+(2k+1)T-1}) \,\middle|\, k \in \mathbb{N}\right\}$ pour M parcourant $\mathcal{E}_{-m}$.
Réciproquement, si $\mathcal{E}_m$ n'est pas vide et si (x, y) est de la forme $(p_{N+2kT-1}, q_{N+2kT-1})$ avec $N \in \mathcal{E}_m$ et $k \in \mathbb{N}$ alors on montre comme en **1.** (x, y) est solution de $(PF_{d,m})$. Si $\mathcal{E}_{-m}$ n'est pas vide et si (x, y) est de la forme $(p_{M+(2k+1)T-1}, q_{M+(2k+1)T-1})$ avec $M \in \mathcal{E}_{-m}$ et $k \in \mathbb{N}$ alors, comme (v_n) est $T-$périodique et comme $(2k + 1)T$ est impair,

$$x^2 - dy^2 = (-1)^{M+(2k+1)T} v_{M+(2k+1)T} = -(-1)^M v_M = -(-m) = m$$

donc (x, y) est solution de $(PF_{d,m})$.

3. Le dernier point est une conséquence directe des deux précédents et du fait que les réduites sont deux à deux distinctes. ■

Remarque 1.3.9. — L'énoncé du théorème précédent est lourd mais sa philosophie est assez simple : si T est pair, une solution de $x^2 - dy^2 = m$ ne peut provenir, à un certain nombre de périodes près, que d'un indice $N \in [\![1, T]\!]$ tel que $(-1)^N v_N = m$. En revanche, si T est impair, une solution de $x^2 - dy^2 = m$ peut provenir soit d'un indice $N \in [\![1, T]\!]$ tel que $(-1)^N v_N = m$ à un nombre pair de périodes près soit d'un indice $M \in [\![1, T]\!]$ tel que $(-1)^M v_M = -m$ à un nombre impair de périodes près. Ainsi, dans la pratique, il est assez simple de savoir dans quel cas on se trouve et de déterminer les premières solutions de $(PF_{d,m})$ s'il y en a.

Par ailleurs, il faut garder à l'esprit que ce théorème ne traite pas le cas où les inconnues x et y ne sont pas des nombres premiers entre eux.

Exemple 1.3.10. — Considérons l'équation $(PF_{21,m})$: $x^2 - 21y^2 = m$ avec $1 \leq |m| \leq 4$. On a vu dans l'exemple 1.1.15 que la suite $(v_n)_{n\geq 1}$ associée à $\sqrt{21}$ est périodique de période $T = 6$ avec $v_1 = v_5 = 5$, $v_2 = v_4 = 4$, $v_3 = 3$ et $v_6 = 1$. On est donc dans le cas le plus simple (T est pair) et $(PF_{21,m})$ (avec $|m| \leq 4$) admet des solutions en nombres premiers entre eux si et seulement si $m = 1$, $m = 4$ ou $m = -3$.

Pour $m = 1$ qui correspond à $N = 6$, on calcule $R_5 = [4, 1, 1, 2, 1, 1] = \dfrac{55}{12}$ qui fournit la solution $(55, 12)$. C'est la solution fondamentale de l'équation de Pell-Fermat (PF_{21}). Les autres ($(x_0, y_0) = (1, 0)$, $(x_2, y_2) = (6049, 1320)$, etc...) s'en déduisent par l'identité $x_n + y_n\sqrt{21} = (55 + 12\sqrt{21})^n$.

Pour $m = 4$ qui correspond à $N = 2$ ou $N = 4$, on calcule $R_1 = [4, 1] = \dfrac{5}{1}$ et $R_3 = [4, 1, 1, 2] = \dfrac{23}{5}$ qui donnent les solutions $(5, 1)$ et $(23, 5)$ et les autres solutions correspondent aux réduites R_7, R_9, R_{13}, R_{15}, etc... Comme $m = 4$ est un carré parfait, il y a également la solution triviale $(2, 0)$.

Pour $m = -3$ qui correspond à $N = 3$, on calcule $R_2 = [4, 1, 1] = \dfrac{9}{2}$ donc $(9, 2)$ est solution de $(PF_{21,-3})$. Les autres solutions correspondent aux réduites R_8, R_{14}, etc...

Si x et y ne sont pas premiers entre eux et si on note δ leur P.G.C.D alors δ^2 divise m donc cela impose $m = 4$ et $\delta = 2$. Il s'ensuit que $x = 2x'$ et $y = 2y'$ avec (x', y') solution de $X^2 - 21Y^2 = 1$ i.e. de (PF_{21}) et on est ramené au premier cas qui va donner les solutions $(110, 24)$, $(12098, 2640)$, ... pour l'équation $(PF_{21,4})$.

Pour terminer, nous donnons une autre démonstration du corollaire 1.3.6.

Corollaire 1.3.11. — *Soit $d \in \mathbb{N}$ un entier qui n'est pas un carré parfait. Alors, l'équation de Pell-Fermat (PF_d) admet une infinité de solutions.*

Preuve. — Notons T la période du développement de $\sqrt{d}$. On a vu dans la démonstration du point **3.** de la proposition 1.1.14 que $a_T = 2a_0$ et que, lorsque $a_j = 2a_0$ alors $v_j = 1$. Ainsi, $v_T = 1$. Si T est pair alors $(-1)^T v_T = 1$ et donc $\mathcal{E}_1 \neq \varnothing$ ce qui assure que (PF_d) a une infinité de solutions. Si T est impair, $(-1)^T v_T = -1$ donc $\mathcal{E}_{-1} \neq \varnothing$ et, dans ce cas aussi, (PF_d) a une infinité de solutions. ■

Remarque 1.3.12. — On peut démontrer que $v_j = 1$ si et seulement si $j = kT$ avec $k \in \mathbb{N}^*$ donc la solution fondamentale de (PF_d) est donnée par la réduire R_{T-1} si T est pair et R_{2T-1} si T est impair.

1.3.3 L'équation (E_2)

Nous allons à présent étudier l'équation d'inconnue $(x, y) \in \mathbb{N}^2$

$$(E_2) : ax^2 - by^2 = 1$$

où a et b sont deux entiers naturels non nuls et premiers entre eux.

Remarquons que si $a = 1$ ou $b = 1$, on est dans le cas d'une équation de Pell-Fermat ((PF_b) : $x^2 - by^2 = 1$ si $a = 1$ et $(PF_{a,-1})$: $y^2 - ax^2 = -1$ si $b = 1$). On peut donc exclure ces cas dans la suite.

On peut également exclure le cas trivial où ab est un carré parfait en utilisant le lemme suivant.

Lemme 1.3.13. — *Si ab est un carré parfait et si (E_2) a une solution alors (E_2) est une équation de Pell-Fermat qui n'a qu'une solution triviale.*

Preuve. — Supposons que $ab = k^2$ pour un certain entier $k \in \mathbb{N}^*$ et que (x, y) soit une solution de (E_2). Comme a et b sont premiers entre eux, il existe deux entiers naturels non nuls r et t tels que $a = r^2$ et $b = t^2$. Alors, $(rx)^2 - (ty)^2 = 1$ donc $(rx - ty)(rx + ty) = 1$ ce qui impose que $rx - ty = rx + ty = 1$. Il s'ensuit que $2rx = 2$ i.e. $r = x = 1$ et donc $y = 0$ et $a = 1$. ■

Ainsi, on peut se restreindre aux cas où ni a ni b n'est égal à 1 et où ab n'est pas un carré parfait.

Théorème 1.3.14. — *Soit a et b deux entiers supérieurs ou égaux à 2, premiers entre eux et tels que $d := ab$ ne soit pas un carré parfait. On note (u_n) et (v_n) les suite associées à $\sqrt{d}$ par la proposition 1.1.14, $R_n = \dfrac{p_n}{q_n}$ la $n-$ième réduite dans le développement en fraction continuée de $\sqrt{d}$ et T la plus petite période de ce développement.*

1. *Si $a < b$ alors l'équation (E_2) admet une solution si et seulement s'il existe un entier pair $N \in [\![1, T-1]\!]$ tel que $v_N = a$ et tel que v_N divise u_N. De plus, dans ce cas, $T = 2N \equiv 0 \mod (4)$ et l'ensemble des solutions de (E_2) est*

$$\left\{ \left(\frac{p_{N-1+\ell T}}{a}, q_{N-1+\ell T} \right) \,\middle|\, \ell \in \mathbb{N} \right\}.$$

2. *Si $b < a$ alors l'équation (E_2) admet une solution si et seulement s'il existe un entier impair $N \in [\![1, T-1]\!]$ tel que $v_N = b$ et tel que v_N divise u_N. De plus, dans ce cas, $T = 2N \equiv 2 \mod (4)$ et l'ensemble des solutions de (E_2) est*

$$\left\{ \left(q_{N-1+\ell T}, \frac{p_{N-1+\ell T}}{b} \right) \,\middle|\, \ell \in \mathbb{N} \right\}.$$

3. *En particulier, (E_2) n'a pas de solution si T est impair.*

Preuve

1. Supposons $a < b$. Notons (s, t) une solution de $ax^2 - by^2 = 1$. En multipliant $as^2 - bt^2 = 1$ par a, il vient $a^2s^2 - abt^2 = a$ donc $(as)^2 - dt^2 = a$ i.e. (as, t) est solution de $(PF_{d,a}) : X^2 - dY^2 = a$ avec $1 \leq a < \sqrt{d}$ car $a < b$. De plus, comme $s(as) - (bt)t = 1$, le théorème de Bézout assure que $\mathrm{PGCD}(as, t) = 1$. Ainsi, d'après le théorème 1.3.8, il existe un entier $N \in [\![1, T]\!]$ et un entier $\ell \in \mathbb{N}$ tel que $(-1)^N v_N = a$ ou $(-1)^N v_N = -a$ (ce deuxième cas ne pouvant se produire que si T est impair) et tel que $(as, t) = (p_{N+\ell T-1}, q_{N+\ell-1})$. Comme v_N et a sont positifs, on en déduit que $v_N = a$. Posons, pour simplifier les notations, $j = N + \ell T$. Remarquons que $j \geq 2$ car, pour $j = 1$, $p_{j-1}^2 - dq_{j-1}^2 = p_0^2 - dq_0^2 = \left\lfloor \sqrt{d} \right\rfloor^2 - d < 0$ donc $p_{j-1}^2 - dq_{j-1}^2 \neq a$. Alors, comme $as = p_{j-1}$, $v_N = a$ divise p_{j-1}. Or, d'après (1.5), étant donné que $j \geq 2$, $p_{j-1} = q_{j-1}u_j + q_{j-2}v_j$ et, comme (u_n) et (v_n) sont $T-$périodiques, on a donc $p_{j-1} = q_{j-1}u_N + q_{j-2}v_N$. Ainsi, on en déduit que v_N divise $q_{j-1}u_N$. Mais, comme p_{j-1} et q_{j-1} sont premiers entre eux et v_N divise p_{j-1}, on peut affirmer que v_N est premier avec q_{j-1} et le lemme de Gauss assure que v_N divise u_N. Remarquons, de plus, que, a étant différent de 1, $N < T$ donc $N \in [\![1, T-1]\!]$. Dès lors, le point **4.** de la proposition 1.1.14 assure que $T = 2N$. On est donc dans le cas où $(-1)^N v_N = a$ et donc N est également pair. Ainsi, $T \equiv 0 \mod (4)$ et (s, t) est bien de la forme $\left(\dfrac{p_{N-1+\ell T}}{a}, q_{N-1+\ell T} \right)$.
Réciproquement, supposons qu'il existe un entier pair $N \in [\![1, T-1]\!]$ tel que $v_N = a$ et tel que v_N divise u_N. Comme précédemment, la proposition 1.1.14 assure que $T = 2N$ et donc $T \equiv 0 \mod (4)$. De plus, $a = (-1)^N v_N$ donc, d'après le théorème 1.3.8, pour tout entier $\ell \in \mathbb{N}$, $(p_{N+\ell T-1}, q_{N+\ell T-1})$ est une solution de $(PF_{d,a})$ i.e. si on pose $j = N + \ell T$, $p_{j-1}^2 - abq_{j-1}^2 = a$

donc $a\left(\frac{p_{j-1}}{a}\right)^2 - bq_{j-1}^2 = 1$. Il suffit alors pour conclure de montrer que a divise p_{j-1}. Or, $j \geq 2$ car N est pair et non nul, donc en réutilisant le fait que, d'après (1.5),

$$p_{j-1} = q_{j-1}u_j + q_{j-2}v_j = q_{j-1}u_N + q_{j-2}v_N,$$

et l'hypothèse $v_N = a$ divise u_N, on peut affirmer que a divise p_{j-1}.

2. Supposons $b < a$. Notons (s,t) une solution de $ax^2 - by^2 = 1$. En multipliant $as^2 - bt^2 = 1$ par $-b$, il vient $b^2t^2 - abs^2 = -b$ donc $(bt)^2 - dt^2 = -b$ i.e. (bt, s) est solution de $(PF_{d,-b}) : X^2 - dY^2 = -b$ avec $1 \leq |-b| < \sqrt{d}$ car $b < a$ et $\text{PGCD}(bt, s) = 1$. On est alors ramené à un cas similaire au précédent mais le fait que $-b < 0$ engendre quelques complications. En effet, comme précédemment, il existe des entiers $N \in [\![1, T]\!]$ et $\ell \in \mathbb{N}$ tels que $(-1)^N v_N = -b$ ou $(-1)^N v_N = b$ (seulement possible si T est impair) et $(bt, s) = (p_{N+\ell T-1}, q_{N+\ell T-1})$. On a alors $v_N = b$ car v_N et b sont positifs. Posons, $j = N + \ell T$. Si $j \geq 2$, on peut raisonner comme dans le point **1.** et en déduire que $T = 2N$ est pair. Cependant, ici, l'entier j peut être égal à 1 ce qui empêche d'utiliser (1.5). Traitons alors ce cas séparément. Si $j = 1$, on a en particulier $(bt, s) = (p_0, q_0) = (a_0, 1)$. Ainsi, $bt = a_0 = \left\lfloor \sqrt{d} \right\rfloor$ et $s = 1$ donc $a = bt^2 + 1$. On va montrer que cela implique que $T = 2$. Reprenons l'algorithme décrit dans l'exemple 1.1.15 avec $\alpha = \sqrt{d} + \left\lfloor \sqrt{d} \right\rfloor = \sqrt{d} + bt$. On écrit $\alpha = 2bt + (\sqrt{d} - bt) = 2bt + \dfrac{d - b^2t^2}{\sqrt{d} + bt} = 2bt + \dfrac{ab - b(a-1)}{\sqrt{d} + bt}$ car $a = bt^2 + 1$ et ainsi, $\alpha = 2bt + \dfrac{b}{\sqrt{d} + bt}$. Dès lors, $\alpha_1 = \dfrac{\sqrt{d} + bt}{b} = t + \dfrac{\sqrt{d}}{b}$ et, étant donné que $\left\lfloor \sqrt{d} \right\rfloor = bt$, $\left\lfloor \dfrac{\sqrt{d}}{b} \right\rfloor = t$ donc

$$\alpha_1 = 2t + \frac{\sqrt{d} - bt}{b} = 2t + \frac{d - b^2t^2}{b(\sqrt{d} + bt)} = 2t + \frac{b}{b\alpha} = 2t + \frac{1}{\alpha}$$

ce qui montre que le développement de $\sqrt{d}$ est $2-$périodique.

On peut donc conclure dans tous les cas que $T = 2N$. En particulier, T est pair donc on est dans le cas où $(-1)^N v_N = -b$ ce qui impose que N est impair. Il s'ensuit que $T \equiv 2 \mod (4)$ et (s,t) est bien de la forme $\left(\frac{p_{N-1+\ell T}}{a}, q_{N-1+\ell T}\right)$.

Réciproquement, supposons qu'il existe un entier impair $N \in [\![1, T-1]\!]$ tel que $v_N = b$ et tel que v_N divise u_N. Comme précédemment, la proposition 1.1.14 assure que $T = 2N$ et donc $T \equiv 2 \mod (4)$. De plus, $-b = (-1)^N v_N$ donc, d'après le théorème 1.3.8, pour tout entier $\ell \in \mathbb{N}$, $(p_{N+\ell T-1}, q_{N+\ell T-1})$ est une solution de $(PF_{d,-b})$ i.e. si on pose $j = N + \ell T$, $p_{j-1}^2 - abq_{j-1}^2 = -b$ donc $aq_{j-1}^2 - b\left(\frac{p_{j-1}}{b}\right)^2 = 1$. Il suffit alors pour conclure de montrer que b divise p_{j-1}. Si $j \geq 2$, on procède comme en **1.** en utilisant (1.5). Si $j = 1$ alors $N = 1$ donc il faut montrer que $b = v_1$ divise $p_0 = a_0$. Or, comme $N = 1$, par hypothèse, v_1 divise u_1 qui est justement égal à a_0 par construction de (u_n). ■

Pour terminer, nous donnons quelques exemples qui montrent que les trois conditions du théorème 1.3.14 (parité de N, $v_N = a$ et v_N divise u_N) sont minimales en ce sens que deux d'entre elles peuvent être réalisées sans que la troisième le soit.

Exemple 1.3.15.

1. Cas où $a < b$

a. Si $a = 18$ et $b = 23$ alors $d = 414$ et la suite (v_n) est $8-$périodique avec $u_4 = v_4 = 18$ donc, comme $N = 4$ est pair les solutions de $18x^2 - 23y^2 = 1$ sont tous les couples de la forme $\left(\frac{p_{3+8k}}{18}, q_{3+8k}\right)$ avec $k \in \mathbb{N}$ où $\dfrac{p_n}{q_n}$ est la $n-$ième réduite dans le développement en

fractions continuées de $\sqrt{342}$. Les 3 premières solutions sont $(26, 23)$, $(1\,265\,394, 1\,119\,433)$, $(61\,586\,725\,954, 54\,482\,804\,087)$.

b. Si $a = 19$ et $b = 25$ alors $d = 475$ et la suite (v_n) est $10-$périodique avec $v_5 = u_5 = 19$. Ainsi, on a bien $v_5 = a$ qui divise u_5 mais l'équation $19x^2 - 25y^2 = 1$ n'a pas de solution car $N = 5$ est impair.

c. Si $a = 18$ et $b = 25$ alors $d = 450$ et la suite (v_n) est $8-$périodique avec $v_4 = 9$ et $u_4 = 18$. Ainsi, on a bien $N = 4$ qui est pair et v_N qui divise u_N mais l'équation $18x^2 - 25y^2 = 1$ n'a pas de solution car $v_N \neq a$.

d. Si $a = 16$ et $b = 19$ alors $d = 304$ et la suite (v_n) est $12-$périodique avec $v_6 = 16$ et $u_6 = 8$. Ainsi, on a bien $N = 6$ qui est pair et $v_N = a$ mais l'équation $16x^2 - 19y^2 = 1$ n'a pas de solution car v_N ne divise pas u_N.

2. Cas où $b < a$

a. Si $a = 25$ et $b = 19$, d'après l'exemple **1.b.**, $N = 5$ et $u_5 = v_5 = b$ donc l'ensemble des solution de l'équation $25x^2 - 19y^2 = 1$ est $\left\{ \left(q_{4+10\ell}, \dfrac{p_{4+10\ell}}{19} \right) \,\middle|\, \ell \in \mathbb{N} \right\}$. Les 3 premières solutions sont $(34, 39)$, $(3\,930\,298, 4\,508\,361)$ et $(454\,334\,588\,170, 521\,157\,514\,839)$

b. Si $a = 23$ et $b = 18$ alors, d'après l'exemple **1.a**, $N = 4$ est pair donc $23x^2 - 18y^2 = 1$ n'a pas de solution.

c. Les exemples **1.c** et **1.d** fournissent des contres-exemples similaires en échangeant a et b.

Remarque 1.3.16. — Remarquons, pour finir, qu'on peut montrer que si T est pair et si $T = 2N$ alors $u_{N+1} = u_N$. Dès lors, avec les notations de la proposition 1.1.14, $u_N = u_{N+1} = a'_N v_N - u_N$ donc v_N divise $2u_N$. Il s'ensuit que si $v_N = a$ (resp. $v_N = b$) et si a (resp. b) est impair alors v_N divise toujours u_N et on peut donc, dans ce cas, supprimer cette hypothèse dans le point **1.** (resp. le point **2.**) du théorème 1.3.14. Celle-ci est en revanche indispensable si a (resp. b) est pair comme on l'a vu dans l'exemple ci-dessus avec $a = 16$ et $b = 19$.

1.4 Un lemme fondamental

Soit n un entier supérieur ou égal à 2. Considérons l'équation générale d'inconnue $(x, y) \in \mathbb{N}^2$

$$(E_n) : ax^n - by^n = 1$$

avec a et b deux entiers naturels non nuls premiers entre eux. On rappelle que (x, y) est une solution triviale de (E_n) si $(x, y) = (1, 0)$ (ce qui ne se produit que si $a = 1$). Comme, par ailleurs, un couple $(0, y)$ ne peut pas être solution de (E_n) puisque $-by^n \leq 0$, une solution (x, y) de (E_n) est non triviale si et seulement si $xy \neq 0$.

On peut facilement généraliser le lemme 1.3.13.

Lemme 1.4.1. — *Si ab est la puissance $n-$ième d'un entier alors (E_n) n'a pas de solution non triviale.*

Preuve. — Supposons que $ab = k^n$ pour un certain entier $k \in \mathbb{N}^*$ et que (x, y) soit une solution de (E_n). Comme a et b sont premiers entre eux, il existe deux entiers u et v tels que $a = u^n$ et $b = v^n$. Alors, $(ux)^n - (vy)^n = 1$ donc $(ux - vy) \sum_{k=0}^{n-1} (ux)^k (vy)^{n-k-1} = 1$. Il s'ensuit que $\sum_{k=0}^{n-1} (ux)^k (vy)^{n-k-1} = 1$. Or, cette somme ne contient que des entiers naturels donc tous ces entiers sont nuls sauf un. Cela impose que $x = 0$ ou $y = 0$ donc (x, y) est une solution de triviale de (E_n) (et ainsi $a = 1$ et $(x, y) = (1, 0)$). ■

En particulier, si $a = b$, (E_n) n'a pas de solution non triviale. On peut donc supposer $a \neq b$ sans nuire à la généralité. Le lemme suivant, qui sera d'une utilité constante dans toute la suite, est une généralisation du lemme 1.3.7.

Lemme 1.4.2. — *Si (x,y) est une solution non triviale de (E_n) et si $a>b$ alors $\dfrac{y}{x}$ est une réduite dans le développement en fraction continuée de $\sqrt[n]{\dfrac{a}{b}}$.*

Preuve. — Par définition, $|ax^n-by^n|=1$ avec x et y strictement positifs. Alors,

$$\left|\frac{a}{b}-\frac{y^n}{x^n}\right|=\frac{1}{bx^n}.$$

Or,

$$\frac{a}{b}-\frac{y^n}{x^n}=\left(\sqrt[n]{\frac{a}{b}}\right)^n-\left(\frac{y}{x}\right)^n=\left(\sqrt[n]{\frac{a}{b}}-\frac{y}{x}\right)\sum_{k=0}^{n-1}\left(\sqrt[n]{\frac{a}{b}}\right)^k\left(\frac{y}{x}\right)^{n-k-1}$$

donc

$$\left|\sqrt[n]{\frac{a}{b}}-\frac{y}{x}\right|=\frac{1}{bx^n\left[\sum\limits_{k=0}^{n-1}\left(\sqrt[n]{\frac{a}{b}}\right)^k\left(\frac{y}{x}\right)^{n-k-1}\right]}. \tag{1.6}$$

Comme $a>b$, $a\geq b+1$ donc $by^n=ax^n-1\geq bx^n+(x^n-1)\geq bx^n$ car $x\geq 1$. Il s'ensuit que $y\geq x$ et donc, pour tout $k\in[\![0,n-1]\!]$, $\left(\sqrt[n]{\frac{a}{b}}\right)^k\left(\frac{y}{x}\right)^{n-k-1}\geq\left(\sqrt[n]{\frac{a}{b}}\right)^k>1$ car $a>b$. Ainsi, $\sum\limits_{k=0}^{n-1}\left(\sqrt[n]{\frac{a}{b}}\right)^k\left(\frac{y}{x}\right)^{n-k-1}>n$ et on déduit de (1.6) que

$$\left|\sqrt[n]{\frac{a}{b}}-\frac{y}{x}\right|<\frac{1}{nbx^n}. \tag{1.7}$$

et, étant donné que $n>2$,

$$\left|\sqrt[n]{\frac{a}{b}}-\frac{y}{x}\right|<\frac{1}{2x^2}.$$

Remarquons que $\sqrt[n]{\frac{a}{b}}$ est irrationnel car s'il existait deux entiers r et t non nuls et premiers entre eux tels que $\sqrt[n]{\frac{a}{b}}=\frac{r}{t}$ alors on aurait $\frac{a}{b}=\frac{r^n}{t^n}$ avec $\mathrm{PGCD}(r^n,t^n)=1$ donc $a=r^n$ et $b=t^n$ et ainsi $ab=(rt)^n$ ce qui est exclu par hypothèse. On peut donc appliquer la proposition 1.1.8 qui assure que $\frac{y}{x}$ est une réduite du développement dans le développement en fraction continuée de $\sqrt[n]{\frac{a}{b}}$. ■

Remarque 1.4.3. — Nous n'aurons besoin dans toute la suite que du cas $a>b$ (et même $a=b+1$). Cependant, dans le cas où $a<b$, il n'est pas difficile de montrer de même que $\left|\sqrt[n]{\frac{b}{a}}-\frac{x}{y}\right|<\frac{1}{nay^n}$ et que $\frac{x}{y}$ est une réduite dans le développement en fractions continuées de $\sqrt[n]{\frac{b}{a}}$.

Chapitre 2

Approximants de Padé d'une famille de fonctions binomiales : la construction de Hermite-Mahler

La première utilisation d'approximants de Padé remonte probablement à Euler dans sa *De fractionibus continuis dissertatio* présentée à l'académie de Saint-Petersbourg en 1737. Il y prouve l'irrationalité de e en utilisant le critère vu dans le lemme 1.1.4. Il a ainsi besoin de déterminer le développement en fraction continuée de e. Pour ce faire, il détermine de deux façons différentes la solution d'une équation différentielle ce qui le conduit, en langage moderne, à déterminer des approximants de Padé de la fonction cotangente hyperbolique. On voit donc que dès l'origine, ces approximants furent intimement liés aux fractions continuées. Ils en sont, en un certain sens, le prolongement naturel : de la même manière que les fractions continuées permettent d'approcher un réel par un rationnel, les approximants de Padé permettent d'approcher une fonction analytique au voisinage de 0 par une fonction rationnelle, la notion d'approximation signifiant ici que les développements de Taylor en 0 des deux fonctions coïncident jusqu'à un certain ordre.

La première construction explicite d'approximants de Padé simultanés est due à Hermite [(1)] dans son mémoire sur la transcendance de e [15]. Ici, il ne s'agit plus seulement d'approcher une fonction analytique au voisinage de 0 mais toute une famille de fonctions. Hermite le fait explicitement pour des fonctions exponentielles. La même année, il donne une autre famille d'approximants simultanés ayant des propriétés légèrement différentes et dont la construction fait intervenir des intégrales multiples [16]. Quelque 20 ans plus tard, il reviendra sur le sujet [17] en utilisant cette fois le théorème des résidus.

Par la suite, Padé [(2)] entreprendra une première étude systématique des approximants qui portent aujourd'hui son nom dans sa thèse [32] (sous la direction de Hermite) où il présente et donne les propriétés de ce qu'on appelle à présent les tables de Padé puis applique cela à la fonction exponentielle [33] et aux fonctions binomiales [34]. Il consacrera par le suite de nombreux articles aux fractions continues de fonctions et aux tables de Padé.

Dans les années suivantes, les approximants de Padé de fonctions binomiales seront utilisés notamment par Thue [41] [42], Siegel [38] [39] (en lien avec les fonctions hypergéométriques) avant que Mahler [(3)] ne redécouvre le travail de Hermite et ne l'applique aux fonctions exponentielle, logarithme [25] et binomiale [24]. Il fera en particulier les liens entre les deux types d'approximants définis par Hermite en 1873 qu'il nomme approximants de type I et approximants de type II.

(1). Charles Hermite, 1822–1901.
(2). Henri Padé, 1863–1953.
(3). Kurt Mahler, 1903–1988.

L'objet de ce qui suit est de présenter l'étude faite par Mahler (reprenant les idées de Hermite) des approximants de type I d'une famille de fonctions binomiales et d'en donner certaines propriétés utiles pour la suite.

2.1 Généralités

Notation 2.1.1. — Si P est un polynôme de $\mathbb{C}[X]$, on note $\deg P$ le degré de P.

Si f est une fonction analytique non nulle dans un voisinage de 0, on note $\mathrm{ord}(f)$ l'ordre de f i.e. le plus petit indice k tel que $f^{(k)}(0) \neq 0$. En d'autres termes, si on écrit le développement en série entière $f(z) = \sum_{j=0}^{+\infty} b_j z^j$ de f dans un voisinage de 0, l'ordre de f est le plus petit entier k tel que $b_k \neq 0$. Par convention, si $f \equiv 0$, on pose $\mathrm{ord}(f) = +\infty$.

Définition 2.1.2. — Soit m un entier supérieur ou égal à 2. On considère m fonctions f_1, f_2, ..., f_m analytiques au voisinage de 0 et m entiers naturels r_1, r_2, ..., r_m. On appelle famille de $[r_1, r_2, ..., r_m]$ approximants de Padé simultanés du système de fonctions $(f_1, f_2, ..., f_m)$ la donnée de m polynômes A_1, A_2, ..., A_m non tous nuls tels que

1. pour tout $i \in [\![1, m]\!]$, $\deg A_i \leq r_i$;
2. l'ordre de la fonction $R := \sum_{i=1}^{m} A_i f_i$ est au moins égal à $\sum_{i=1}^{m}(r_i + 1) - 1$.

Dans ce cas, la fonction R est appelée la fonction reste associée aux approximants A_1, A_2, ..., A_m.

Proposition 2.1.3. — *Pour tout système $(f_1, f_2, ..., f_m)$ de fonctions analytiques au voisinage de 0 et pour tout $m-$uplet d'entiers naturels r_1, r_2, ..., r_m, il existe au moins une famille de $[r_1, r_2, ..., r_m]$ approximants de Padé simultanés du système de fonctions $(f_1, f_2, ..., f_m)$.*

Preuve. — Développons les fonctions f_1, f_2, ..., f_m en séries entières au voisinage de 0 :

$$\forall i \in [\![1, m]\!] \quad f_i(z) = \sum_{j=0}^{+\infty} b_{i,j} z^j.$$

Posons $r = \sum_{i=1}^{m}(r_i + 1)$.

Le problème revient à trouver une famille de complexes $(a_{i,j})$ telle que, pour tout $\ell \in [\![0, r-2]\!]$, le coefficient de z^ℓ dans le développement en série entière au voisinage de 0 de

$$R(z) = \sum_{i=1}^{m} \left(\sum_{j=1}^{r_i} a_{i,j} z^j \right) \left(\sum_{j=0}^{+\infty} b_{i,j} z^j \right)$$

soit nul. Or, pour un ℓ donné, ce coefficient est

$$c_\ell = \sum_{i=1}^{m} \sum_{t+s=\ell} a_{i,t} b_{i,s} = \sum_{i=1}^{m} \sum_{t=0}^{\min\{\ell, r_i\}} a_{i,t} b_{i,\ell-t} = \sum_{i=1}^{m} \sum_{t=0}^{\ell} a_{i,t} b_{i,\ell-t}$$

en posant $a_{i,t} = 0$ si $t \geq \ell + 1$. On aboutit ainsi au système :

$$(S) \begin{cases} a_{1,0}b_{1,0} + a_{2,0}b_{2,0} + \cdots + a_{m,0}b_{m,0} = 0 \\ a_{1,0}b_{1,1} + a_{2,0}b_{2,1} + \cdots + a_{m,0}b_{m,1} + a_{1,1}b_{1,0} + a_{2,1}c_{2,0} + \cdots + a_{m,1}b_{m,0} = 0 \\ \vdots \\ a_{1,0}b_{1,r-2} + a_{2,0}b_{2,r-2} + \cdots + a_{m,0}b_{m,r-2} + \cdots + a_{1,r-2}b_{1,0} + a_{2,r-2}b_{2,0} + \cdots + a_{m,r-2}b_{m,0} = 0 \end{cases}$$

qui est un système linéaire de $r-1$ équations à $\sum_{i=1}^{m}(r_i+1)=r$ inconnues. On sait donc que ce système admet au moins une solution non triviale ce qui garantit l'existence d'une famille d'approximants de Padé. ■

Il est clair qu'une telle famille d'approximants n'est pas unique puisque le système linéaire (S) ci-dessus a toujours une infinité de solutions. On a cependant un résultat intéressant lorsque la famille $(f_1,...,f_m)$ possède la propriété particulière suivante.

Définition 2.1.4. — On dit qu'un système $(f_1,...,f_m)$ de fonctions analytiques au voisinage de 0 est une système normal pour un $m-$uplet d'entiers naturels r_1, ..., r_m si, pour toute famille $(A_1,...,A_m)$ de $[r_1,...,r_m]$ approximants de Padé de $(f_1,...,f_m)$, l'ordre de la fonction reste $R:=\sum_{k=1}^{m}A_kf_k$ est exactement $\sum_{k=1}^{m}(r_k+1)-1$.

Lemme 2.1.5. — *Soit $(f_1,...,f_m)$ un système normal pour un $m-$uplet $(r_1,...,r_m)$ d'entiers naturels. Alors, une famille de $[r_1,...,r_m]$ approximants de Padé de $(f_1,...,f_m)$ est unique à une constante multiplicative près.*

Preuve. — Soit $(A_1,...,A_m)$ et $(B_1,...,B_m)$ deux familles de $[r_1,...,r_m]$ approximants de Padé de $(f_1,...,f_m)$. Considérons les fonctions restes $R=\sum_{k=1}^{m}A_kf_k$ et $S=\sum_{k=1}^{m}B_kf_k$ et notons $r:=\sum_{k=1}^{m}(r_k+1)$. Alors, comme le système $(f_1,...,f_m)$ est normal, $\mathrm{ord}(R)=\mathrm{ord}(S)=r-1$. Dès lors, $S^{(r)}(0)\neq 0$ et, si on pose $\lambda=\dfrac{R^{(r)}(0)}{S^{(r)}(0)}$, alors $R-\lambda S$ est d'ordre au moins r. Définissons alors, pour tout $k\in[\![1,m]\!]$, $C_k=A_k-\lambda B_k$. Par définition, pour tout $k\in[\![1,m]\!]$, C_k est un polynôme de degré au plus r_k et $T:=\sum_{k=1}^{m}C_kf_k=R-\lambda S$ est d'ordre au moins $r>r-1$. Cependant, $(C_1,...,C_m)$ n'est pas une famille de $[r_1,...,r_m]$ approximants de Padé de $(f_1,...,f_m)$ car ce système est normal. Il s'ensuit que les C_k sont tous nuls et donc, pour tout $k\in[\![1,m]\!]$, $A_k=\lambda B_k$. ■

Définition 2.1.6. — Soit f une fonction analytique au voisinage de 0. Soit r_1 et r_2 deux entiers naturels. On dit que deux polynômes A_1 et A_2 sont des $[r_1,r_2]$ approximants de Padé de la fonction f si (A_1,A_2) est une famille de $[r_1,r_2]$ approximants de Padé du système de fonctions $(1,f)$.

Ceci définit ce qu'on peut appeler des approximants de Padé simples (i.e. pour une seule fonction) qui sont, on le voit, un cas particulier d'approximants simultanés. Dans la pratique, et c'est ce que nous ferons dans le chapitre 3, on utilise souvent en arithmétique des approximants de Padé diagonaux i.e. ceux pour lesquels $r_1=r_2$. Les deux suites d'approximants alors obtenues ont une propriété « d'indépendance linéaire » qui est fondamentale en approximation diophantienne et qui sera utilisée dans le chapitre 3. On peut la formuler ainsi :

Proposition 2.1.7. — *Soit f une fonction analytique dans un voisinage $\mathcal{V}$ de 0. Pour tout $r\in\mathbb{N}$, on note (A_r,B_r) une famille de $[r,r]$ approximants de Padé de f et on note R_r la fonction reste associée à A_r et B_r. On suppose que, pour tout $r\in\mathbb{N}$, $B_r(0)\neq 0$ et $\mathrm{ord}(R_r)=2r+1$. Alors, pour tout $r\in\mathbb{N}$, il existe une constante $c_r\neq 0$ telle que*

$$\forall z\in\mathbb{C},\quad A_{r+1}(z)B_r(z)-A_r(z)B_{r+1}(z)=c_rz^{2r+1}.$$

Preuve. — Comme R_r est d'ordre $2r+1$, il existe une fonction $\tilde{R}_r$ analytique sur $\mathcal{V}$ telle que, pour tout $z \in \mathcal{V}$, $R_r(z) = z^{2r+1}\tilde{R}_r(z)$ avec $\tilde{R}_r(0) \neq 0$. Par définition, pour tout $r \in \mathbb{N}$ et tout $z \in \mathcal{V}$, $A_r(z) + B_r(z)f(z) = z^{2r+1}\tilde{R}_r(z)$ donc, en utilisant le caractère alterné et linéaire du déterminant, il vient

$$\begin{aligned} A_{r+1}(z)B_r(z) - A_r(z)B_{r+1}(z) &= \begin{vmatrix} A_{r+1}(z) & A_r(z) \\ B_{r+1}(z) & B_r(z) \end{vmatrix} \\ &= \begin{vmatrix} A_{r+1}(z) + B_{r+1}(z)f(z) & A_r(z) + B_r(z)f(z) \\ B_{r+1}(z) & B_r(z) \end{vmatrix} \\ &= \begin{vmatrix} z^{2r+3}\tilde{R}_{r+1}(z) & z^{2r+1}\tilde{R}_r(z) \\ B_{r+1}(z) & B_r(z) \end{vmatrix} \\ &= z^{2r+1}(z^2\tilde{R}_{r+1}(z)B_r(z) - B_{r+1}(z)\tilde{R}_r(z)) \end{aligned}$$

Or, $z \mapsto A_{r+1}(z)B_r(z) - A_r(z)B_{r+1}(z)$ est une fonction polynomiale de degré au plus $2r+1$ et la fonction $F_r : z \mapsto z^2\tilde{R}_r(z)B_r(z) - B_{r+1}(z)\tilde{R}_{r+1}(z)$ est analytique au voisinage de 0. Il s'ensuit que F est constante. De plus, $F_r(0) = -B_{r+1}(0)\tilde{R}_{r+1}(0) \neq 0$ par hypothèse ce qui permet de conclure pour tout $z \in \mathcal{V}$. Enfin, comme il s'agit d'une égalité portant sur des polynômes, elle s'étant à $\mathbb{C}$ tout entier. ■

2.2 Approximants de Padé simultanés de fonctions binomiales

Dans son article [24], Mahler donne une démonstration alternative du théorème suivant établi par Thue en 1908 :

Si ξ est un nombre algébrique de la forme $\xi = \sqrt[n]{\frac{a}{b}}$ alors, pour tout $\varepsilon > 0$, il n'existe qu'un nombre fini de rationnels $\frac{p}{q}$ tels que

$$\left|\xi - \frac{p}{q}\right| \leq q^{-\left(\frac{n}{2}+1+\varepsilon\right)}.$$

Dans la démonstration initiale, Thue utilise de façon implicite des fractions continuées. Mahler propose dans son article une autre méthode se basant sur les approximants de Padé d'une famille de fonctions binomiales. La présentation qui suit reprend la construction présentée dans cet article qui, comme on l'a déjà signalé, s'inspirait du travail initié par Hermite pour une famille de fonctions exponentielles ([16], [17]).

Dans toute la suite de ce paragraphe, m est un entier supérieur ou égal à 2, ω_1, ω_2, ..., ω_m désignent des nombres réels tels que, pour tout $i \neq j$, $\omega_i - \omega_j \notin \mathbb{Z}$ et ρ_1, ρ_2, ..., ρ_n sont des entiers naturels non nuls [(4)].

On note, pour tout réel ω, f_ω la fonction définie sur $]-\infty\,;1[$ par $f_\omega(z) = (1-z)^\omega$. On veut déterminer une famille de $[\rho_1 - 1, \rho_2 - 1, ..., \rho_m - 1]$ approximants de Padé du système de fonctions $(f_{\omega_1}, f_{\omega_2}, ..., f_{\omega_m})$. Il s'agit donc de déterminer des polynômes $A_1, ..., A_m$ tels que, pour tout $k \in [\![1, m]\!]$, $\deg(A_k) \leq \rho_k - 1$ et tels que la fonction reste $R_m = \sum_{k=1}^{m} A_k f_{\omega_k}$ soit d'ordre au moins égal à $\sigma - 1$ où $\sigma := \sum_{k=1}^{m} \rho_k$. Pour préciser la dépendance des polynômes A_k et de la fonction reste R par rapport aux paramètres ω_i et ρ_i, on utilisera les notations

$$A_k\left(z \,\middle|\, \begin{matrix} \omega_1 & \cdots & \omega_m \\ \rho_1 & \cdots & \rho_m \end{matrix}\right) \qquad \text{et} \qquad R\left(z \,\middle|\, \begin{matrix} \omega_1 & \cdots & \omega_m \\ \rho_1 & \cdots & \rho_m \end{matrix}\right). \tag{2.1}$$

(4). Ces notations, ainsi que la plupart de celles utilisées dans ce chapitre, sont dues à Mahler et ont été reprises dans la plupart des articles y faisant référence ([1], [7] ou encore [5], par exemple).

2.2.1 Expression intégrale de la fonction reste

Considérons des polynômes A_1, ..., A_m qui forment une famille de $[\rho_1-1,...,\rho_m-1]$ approximants de Padé voulus (on sait qu'il en existe d'après la proposition 2.1.3). Si on note g_1 la fonction définie sur $]-\infty\,;1[$ par $g_1(z)=(1-z)^{-\omega_1}R\left(z\left|\begin{array}{ccc}\omega_1&\cdots&\omega_m\\ \rho_1&\cdots&\rho_m\end{array}\right.\right)$ (où R est la fonction reste associée à la famille d'approximants) alors

$$\forall z<1\quad g_1(z)=(1-z)^{-\omega_1}\sum_{k=1}^{m}A_k\left(z\left|\begin{array}{ccc}\omega_1&\cdots&\omega_m\\ \rho_1&\cdots&\rho_m\end{array}\right.\right)(1-z)^{\omega_k}=\sum_{k=1}^{m}A_k\left(z\left|\begin{array}{ccc}\omega_1&\cdots&\omega_m\\ \rho_1&\cdots&\rho_m\end{array}\right.\right)(1-z)^{\omega_k-\omega_1}$$

donc, en dérivant ρ_1 fois, il vient, pour tout $z<1$,

$$g_1^{(\rho_1)}(z)=\sum_{k=2}^{m}\sum_{j=1}^{\rho_1}\binom{\rho_1}{j}A_k^{(j)}\left(z\left|\begin{array}{ccc}\omega_1&\cdots&\omega_m\\ \rho_1&\cdots&\rho_m\end{array}\right.\right)(-1)^j\prod_{\ell=1}^{j}(\omega_k-\omega_1-\ell)(1-z)^{\omega_k-\omega_1-(\rho_1-j)}$$

et donc, en posant, pour tout $k\in[\![2,m]\!]$,

$$A_k\left(z\left|\begin{array}{ccc}\omega_2-\omega_1-\rho_1&\cdots&\omega_m-\omega_1-\rho_1\\ \rho_2&\cdots&\rho_m\end{array}\right.\right):=\sum_{j=1}^{\rho_1}\binom{\rho_1}{j}A_k^{(j)}\left(z\left|\begin{array}{ccc}\omega_1&\cdots&\omega_m\\ \rho_1&\cdots&\rho_m\end{array}\right.\right)(-1)^j\prod_{\ell=1}^{j}(\omega_k-\omega_1-\ell)(1-z)^j$$

on obtient un polynôme de degré au plus ρ_k-1 tel que, pour tout $z<1$,

$$\sum_{k=2}^{m}A_k\left(z\left|\begin{array}{ccc}\omega_2-\omega_1-\rho_1&\cdots&\omega_m-\omega_1-\rho_1\\ \rho_2&\cdots&\rho_m\end{array}\right.\right)(1-z)^{\omega_k-\omega_1-\rho_1}=g_1^{(\rho_1)}(z)$$

et, comme $\mathrm{ord}(g_1)=\sigma-1$ (puisque $z\mapsto(1-z)^{\omega_1}$ ne s'annule pas en 0), $\mathrm{ord}(g_1^{(\rho_1)})=\sigma-1-\rho_1=\sum_{k=2}^{m}\sigma_k-1$. De plus, les polynômes $A_k\left(z\left|\begin{array}{ccc}\omega_2-\omega_1-\rho_1&\cdots&\omega_m-\omega_1-\rho_1\\ \rho_2&\cdots&\rho_m\end{array}\right.\right)$ ne sont pas tous nuls car si c'était le cas, $g_1^{(\rho_1)}=0$ donc g_1 serait un polynôme non nul de degré au plus ρ_1-1 ce qui incompatible avec le fait que $\mathrm{ord}(g_1)\geq\sigma-1>\rho_1$. On en déduit que la famille des $A_k\left(z\left|\begin{array}{ccc}\omega_2-\omega_1-\rho_1&\cdots&\omega_m-\omega_1-\rho_1\\ \rho_2&\cdots&\rho_m\end{array}\right.\right)$ pour $k\in[\![2,m]\!]$ est une famille de $[\rho_2-1,\rho_3-1,...,\rho_m-1]$ approximants de Padé du système de fonctions $(f_{\omega_k-\omega_1-\rho_1})_{2\leq k\leq m}$.

On voit qu'en réitérant le procédé avec la nouvelle fonction reste $R_{m-1}:=g_1^{(\rho_1)}$ (et en considérant $g_2:z\mapsto(1-z)^{-(\omega_2-\omega_1-\rho_1)}R_{m-1}$), on va construire des $[\rho_3-1,...,\rho_m-1]$ approximants de Padé du système de fonctions $(f_{\omega_k-\omega_2-\rho_2})_{3\leq k\leq m}$. Ainsi, par récurrence, on construit des fonctions restes R_{m-j} telles que, si on définit la fonction g_{j+1} par $g_{j+1}(z)=(1-z)^{-(\omega_{j+1}-\omega_j-\rho_j)}R_{m-j}$, alors $g_{j+1}^{(\rho_{j+1})}$ est la fonction reste associée à une famille de $[\rho_{j+2}-1,\rho_{j+3}-1,...,\rho_m-1]$ approximants de Padé du système de fonctions $(f_{\omega_k-\omega_{j+1}-\rho_{j+1}})_{j+2\leq k\leq m}$. En particulier, pour $j=m-1$, on aboutit à une fonction g_{m-1} telle que $(1-z)^{-(\omega_m-\omega_{m-1}-\rho_{m-1})}g_{m-1}^{(\rho_{m-1})}(z)$ est un polynôme en z de degré au plus ρ_m-1 et d'ordre au moins ρ_m-1. Il s'ensuit qu'il existe une constante non nulle c_m telle que $(1-z)^{-(\omega_m-\omega_{m-1}-\rho_{m-1})}g_{m-1}^{(\rho_{m-1})}(z)=c_mz^{\rho_m-1}$ i.e. telle que $g_{m-1}^{(\rho_{m-1})}(z)=c_mz^{\rho_m-1}(1-z)^{\omega_m-\omega_{m-1}-\rho_{m-1}}$.

Notation 2.2.1. — Posons $\mathcal{C}:=\mathcal{C}(]-\infty\,;1[\,,\mathbb{R})$ l'ensemble des fonctions continues sur $]-\infty\,;1[$ à valeurs dans $\mathbb{R}$ et notons J l'opérateur de $\mathcal{C}$ dans lui-même qui à toute fonction $f\in\mathcal{C}$ associe sa primitive Jf qui s'annule en 0. Pour tout $n\in\mathbb{N}^*$, on pose $J^n:=\underbrace{J\circ\cdots\circ J}_{n\text{ fois}}$ et, pour tout réel α et tout entier strictement positif ρ, on définit l'opérateur J_α^ρ de $\mathcal{C}$ dans lui-même qui à une fonction $f\in\mathcal{C}$ associe la fonction $J_\alpha^\rho f:t\mapsto(1-t)^\alpha(J^\rho f)(t)$.

Si on pose $\omega_0 = \rho_0 = 1$ et si on définit, pour tout $j \in [\![1, m-1]\!]$, $\alpha_j = \omega_j - \omega_{j-1} - \rho_{j-1}$, il découle de ce qui précède que la fonction reste R de départ est égale à $J_{\alpha_1}^{\rho_1} \circ J_{\alpha_1}^{\rho_1} \circ \cdots \circ J_{\alpha_{m-1}}^{\rho_{m-1}} g_m^{(\rho_{m-1})}$ donc, comme $g_m^{(\rho_{m-1})}$ est entièrement déterminer par la constante c_m, la fonction R est également entièrement déterminée par la constante c_m. De plus, comme l'opérateur J_α^ρ augmente l'ordre d'une fonction d'exactement ρ, l'ordre de R est exactement $\sigma - 1$. On a donc démontré la propriété suivante.

Proposition 2.2.2. — *Pour toute famille $(A_1, A_2, \cdots, A_m)$ de $[\rho_1 - 1, \rho_2 - 1, \cdots, \rho_m - 1]$ approximants de Padé du système de fonctions $(f_{\omega_1}, f_{\omega_2}, \cdots, f_{\omega_m})$,*

1. *la fonction reste $R = \sum_{k=1}^{m} A_k f_{\omega_k}$ est unique à une constante multiplicative près ;*
2. *la fonction R est exactement d'ordre $\sigma - 1$ i.e. le système $(f_{\omega_1}, f_{\omega_2}, \cdots, f_{\omega_m})$ est normal pour le $m-$uplet $(\rho_1 - 1, \rho_2 - 1, \cdots, \rho_m - 1)$.*

On déduit alors du lemme 2.1.5 le corollaire suivant.

Corollaire 2.2.3. — *Une famille de $[\rho_1 - 1, \rho_2 - 1, \cdots, \rho_m - 1]$ approximants de Padé du système de fonctions $(f_{\omega_1}, f_{\omega_2}, \cdots, f_{\omega_m})$ est unique à une constante multiplicative près.*

Les deux lemmes techniques suivant vont nous permettre d'aboutir à une expression sous forme d'intégrale multiple de la fonction reste R si on impose la valeur de c_m.

Lemme 2.2.4. — *Pour toute fonction $f \in \mathcal{C}$ et pour tout réel $x \in]-\infty\,;1[$,*

$$(J^n f)(x) = \int_0^x \frac{(x-t)^{n-1}}{\Gamma(n)} f(t)\,\mathrm{d}t.$$

Preuve. — Soit $f \in \mathcal{C}$ et $x \in]-\infty\,;1[$. On applique la formule de Taylor avec reste intégral à la fonction $J^n f$ qui est de classe C^n sur $[0\,;x]$:

$$(J^n f)(x) = \sum_{k=0}^{n-1} \frac{(J^n f)^{(k)}(0)}{k!} x^k + \int_0^x \frac{(x-t)^{n-1}}{(n-1)!} (J^n f)^{(n)}(t)\,\mathrm{d}t.$$

Comme $J^n f$, ainsi que toutes ses dérivées jusqu'à l'ordre $n-1$, s'annulent en 0 par définition, on en déduit que

$$(J^n f)(x) = \int_0^x \frac{(x-t)^{n-1}}{(n-1)!} f(t)\,\mathrm{d}t = \int_0^x \frac{(x-t)^{n-1}}{\Gamma(n)} f(t)\,\mathrm{d}t$$

comme annoncé. ■

Lemme 2.2.5. — *Pour toute fonction $f \in \mathcal{C}$ et tout réel $t_0 \in]-\infty\,;1[$,*

$$\left(J_{\alpha_1}^{r_1} \circ \cdots \circ J_{\alpha_k}^{r_k} f\right)(t_0) = \int_0^{t_0} \int_0^{t_1} \cdots \int_0^{t_{k-1}} \left(\prod_{j=1}^{k} \frac{(1-t_{j-1})^{\alpha_j} (t_{j-1} - t_j)^{r_j - 1}}{\Gamma(r_j)} \right) f(t_k)\,\mathrm{d}t_k \cdots \mathrm{d}t_2\,\mathrm{d}t_1.$$

Preuve. — On raisonne par récurrence sur $k \in \mathbb{N}^*$.
Si $k = 1$, c'est une réécriture du lemme 2.2.4.
Supposons le propriété vraie pour un certain $k \in \mathbb{N}^*$. Alors,

$$\left(J_{\alpha_1}^{r_1} \circ \cdots \circ J_{\alpha_{k+1}}^{r_{k+1}} f\right)(t_0) = \left[J_{\alpha_1}^{r_1} \left(J_{\alpha_2}^{r_2} \circ \cdots \circ J_{\alpha_{k+1}}^{r_{k+1}} f\right)\right](t_0) = (1-t_0)^{\alpha_1} \left[J^{r_1} \left(J_{\alpha_2}^{r_2} \circ \cdots \circ J_{\alpha_{k+1}}^{r_{k+1}} f\right)\right](t_0)$$

et donc, d'après le lemme 2.2.4,

$$\left(J_{\alpha_1}^{r_1}\circ\cdots\circ J_{\alpha_{k+1}}^{r_{k+1}}f\right)(t_0)=(1-t_0)^{\alpha_1}\int_0^{t_0}\frac{(t_0-t_1)^{r_1-1}}{\Gamma(r_1)}\left(J_{\alpha_2}^{r_2}\circ\cdots\circ J_{\alpha_{k+1}}^{r_{k+1}}f\right)(t_1)\,\mathrm{d}t_1.$$

Or, par hypothèse de récurrence,

$$\left(J_{\alpha_2}^{r_2}\circ\cdots\circ J_{\alpha_{k+1}}^{r_{k+1}}f\right)(t_1)=\int_0^{t_1}\int_0^{t_2}\cdots\int_0^{t_k}\left(\prod_{j=2}^{k+1}\frac{(1-t_{j-1})^{\alpha_j}(t_{j-1}-t_j)^{r_j-1}}{\Gamma(r_j)}\right)f(t_{k+1})\,\mathrm{d}t_{k+1}\cdots\mathrm{d}t_3\,\mathrm{d}t_2$$

donc

$$\left(J_{\alpha_1}^{r_1}\circ\cdots\circ J_{\alpha_{k+1}}^{r_{k+1}}f\right)(t_0)=$$
$$(1-t_0)^{\alpha_1}\int_0^{t_0}\frac{(t_0-t_1)^{r_1-1}}{\Gamma(r_1)}\int_0^{t_1}\int_0^{t_2}\cdots\int_0^{t_k}\left(\prod_{j=2}^{k+1}\frac{(1-t_{j-1})^{\alpha_j}(t_{j-1}-t_j)^{r_j-1}}{\Gamma(r_j)}\right)f(t_{k+1})\,\mathrm{d}t_{k+1}\cdots\mathrm{d}t_3\,\mathrm{d}t_2\,\mathrm{d}t_1$$

c'est-à-dire

$$\left(J_{\alpha_1}^{r_1}\circ\cdots\circ J_{\alpha_{k+1}}^{r_{k+1}}f\right)(t_0)=\int_0^{t_0}\int_0^{t_1}\int_0^{t_2}\cdots\int_0^{t_k}\left(\prod_{j=1}^{k+1}\frac{(1-t_{j-1})^{\alpha_j}(t_{j-1}-t_j)^{r_j-1}}{\Gamma(r_j)}\right)f(t_{k+1})\,\mathrm{d}t_{k+1}\cdots\mathrm{d}t_3\,\mathrm{d}t_2\,\mathrm{d}t_1$$

ce qui achève la récurrence. ■

Proposition 2.2.6. — *Si on impose $c_m=\Gamma(\rho_1)\cdots\Gamma(\rho_{m-1})$ alors, pour tout réel $z<1$,*

$$R\left(z\,\middle|\,\begin{matrix}\omega_1&\cdots&\omega_m\\ \rho_1&\cdots&\rho_m\end{matrix}\right)=\int_0^z\int_0^{t_1}\cdots\int_0^{t_{m-2}}R(z\mid t_1\;t_2\cdots t_{m-1})\,\mathrm{d}t_{m-1}\cdots\mathrm{d}t_2\,\mathrm{d}t_1 \tag{2.2}$$

avec

$$R(z\mid t_1\,t_2\cdots t_{m-1}):=(z-t_1)^{\rho_1-1}(t_1-t_2)^{\rho_2-1}\ldots(t_{m-2}-t_{m-1})^{\rho_{m-1}-1}t_{m-1}^{\rho_m-1}(1-z)^{\omega_1}(1-t_1)^{\omega_2-\omega_1-\rho_1}\ldots$$
$$(1-t_{m-2})^{\omega_{m-1}-\omega_{m-2}-\rho_{m-2}}(1-t_{m-1})^{\omega_m-\omega_{m-1}-\rho_{m-1}}.$$

De plus, le coefficient de $z^{\sigma-1}$ dans le développement en série entière au voisinage de 0 de R est alors $\dfrac{\Gamma(\rho_1)\cdots\Gamma(\rho_m)}{\Gamma(\sigma)}$.

Preuve. — Posons $\omega_0=\rho_0=0$, $t_0=z$ et $f:z\mapsto z^{\rho_m-1}(1-z)^{\omega_m-\omega_{m-1}-\rho_{m-1}}$. Rappelons, de plus, que, pour tout $j\in[\![1,m-1]\!]$, $\alpha_j=\omega_j-\omega_{j-1}-\rho_{j-1}$. Alors, avec les notations précédentes, $g_{m-1}^{(\rho_{m-1})}(z)=c_mz^{\rho_m-1}(1-z)^{-(\omega_m-\omega_{m-1}-\rho_{m-1})}=\Gamma(\rho_1)\cdots\Gamma(\rho_{m-1})f(z)$ donc

$$\begin{aligned}R\left(z\,\middle|\,\begin{matrix}\omega_1&\cdots&\omega_m\\ \rho_1&\cdots&\rho_m\end{matrix}\right)&=\left(J_{\alpha_1}^{\rho_1}\circ\cdots\circ J_{\alpha_{m-1}}^{\rho_{m-1}}g_{m-1}^{(\rho_{m-1})}\right)(t_0)\\&=\Gamma(\rho_1)\cdots\Gamma(\rho_{m-1})\left(J_{\alpha_1}^{\rho_1}\circ\cdots\circ J_{\alpha_{m-1}}^{\rho_{m-1}}f\right)(t_0).\end{aligned}$$

Ainsi, d'après le lemme 2.2.5,

$$R\left(z\,\middle|\,\begin{matrix}\omega_1&\cdots&\omega_m\\ \rho_1&\cdots&\rho_m\end{matrix}\right)=\int_0^{t_0}\int_0^{t_1}\cdots\int_0^{t_{m-2}}R(z\mid t_1\;t_2\cdots t_{m-1})\,\mathrm{d}t_{m-1}\cdots\mathrm{d}t_2\,\mathrm{d}t_1$$

avec

$$R(z \mid t_1\ t_2 \cdots t_{m-1}) = \Gamma(\rho_1)\cdots\Gamma(\rho_{m-1}) \left(\prod_{j=1}^{m-1} \frac{(1-t_{j-1})^{\alpha_j}(t_{j-1}-t_j)^{\rho_j-1}}{\Gamma(r_j)} \right) f(t_{m-1})$$
$$= \left(\prod_{j=1}^{m-1} (1-t_{j-1})^{\alpha_j}(t_{j-1}-t_j)^{\rho_j-1} \right) t_{m-1}^{\rho_m-1}(1-t_{m-1})^{\omega_m-\omega_{m-1}-\rho_{m-1}}$$

ce qui donne l'expression attendue en tenant compte du fait que $t_0 = z$ et $\alpha_1 = \omega_1$.

Notons $a_{\sigma-1}$ le coefficient de $z^{\sigma-1}$ dans le développement en série entière au voisinage de 0 de R. Alors, $a_{\sigma-1}$ est également le coefficient de $z^{\sigma-1}$ dans le développement en série entière au voisinage de 0 de $g_1 = (1-z)^{-\omega_1}R$. Dès lors, le coefficient de $z^{\sigma-\rho_1-1}$ dans le développement de $R_{m-1} = g_1^{(\rho_1)}$ est $\sigma(\sigma-1)...(\sigma-\rho_1+1)a_{\sigma-1} = \dfrac{\Gamma(\sigma)}{\Gamma(\sigma-\rho_1)}a_{\sigma-1}$. En raisonnant de même, $\dfrac{\Gamma(\sigma)}{\Gamma(\sigma-\rho_1)}$ est également le coefficient de $z^{\sigma-\rho_1-1}$ dans le développement en série entière au voisinage de 0 de $g_2 = (1-z)^{-(\omega_2-\omega_1-\rho_1)}R_{m-1}$ et donc le coefficient de $z^{\sigma-\rho_1-\rho_2-1}$ dans le développement de $R_{m-2} = g_2^{(\rho_2)}$ est $\dfrac{\Gamma(\sigma-\rho_1)}{\Gamma(\sigma-\rho_1-\rho_2)}\dfrac{\Gamma(\sigma)}{\Gamma(\sigma-\rho_1)}a_{\sigma-1} = \dfrac{\Gamma(\sigma)}{\Gamma(\sigma-(\rho_1+\rho_2))}a_{\sigma-1}$. En réitérant le procédé, le coefficient de z^{ρ_m-1} dans le développement de $g_{m-1}^{(\rho_{m-1})}$ est $\dfrac{\Gamma(\sigma)}{\Gamma(\sigma-(\rho_1+\rho_2+\cdots+\rho_{m-1}))}a_{\sigma-1} = \dfrac{\Gamma(\sigma)}{\Gamma(\rho_m)}a_{\sigma-1}$. Or, ce coefficient est c_m donc, si $c_m = \Gamma(\rho_1)\cdots\Gamma(\rho_{m-1})$ alors

$$a_{\sigma-1} = c_m\frac{\Gamma(\rho_m)}{\Gamma(\sigma)} = \frac{\Gamma(\rho_1)\cdots\Gamma(\rho_m)}{\Gamma(\sigma)}$$

ce qui achève la démonstration. ■

2.2.2 Construction par la formule des résidus

Si la méthode précédente permet de montrer l'unicité (à une constante près) des approximants de Padé d'une famille de fonctions binomiales et d'obtenir une expression intégrale de la fonction reste, elle ne donne pas d'expressions explicites pour les polynômes A_k $(1 \le k \le m)$. On va à présent utiliser une approche différente qui permet d'obtenir de telles formules.

Pour ce faire, on pose $R := \max\limits_{1\le k\le m}(|\omega_k| + \rho_k)$ et on considère, dans le plan complexe, le cercle γ de centre 0 et de rayon R orienté dans le sens direct. Ainsi, par construction, les ω_k sont tous dans le disque ouvert $D(0,R)$ de centre 0 et de rayon R. On introduit alors la fonction T définie sur $]-\infty\,;1[$ par l'intégrale curviligne

$$T(z) = \frac{1}{2\mathrm{i}\pi}\int_\gamma \frac{(1-z)^u}{\prod\limits_{k=1}^{m}\prod\limits_{h=0}^{\rho_k-1}(u-\omega_k-h)}\,\mathrm{d}u. \tag{2.3}$$

On va montrer que T est la fonction reste associée à une famille de $[\rho_1-1,...,\rho_m]$ approximants de Padé du système $(f_{\omega_1},...,f_{\omega_m})$.

Fixons $z \in]-\infty\,;1[$ et notons α_z la fonction définie par

$$\alpha_z(u) = \frac{(1-z)^u}{\prod\limits_{k=1}^{m}\prod\limits_{h=0}^{\rho_k-1}(u-\omega_k-h)} \tag{2.4}$$

Alors la fonction α_z est une fonction méromorphe sur $\mathbb{C}$ dont les pôles sont les $\omega_k + h$ pour $1 \le k \le m$ et $0 \le h \le \rho_k - 1$. Comme les ω_k sont tels que $\omega_i - \omega_j \notin \mathbb{Z}$ pour tout $i \ne j$, ces pôles sont tous simples.

Notons r le minimum des $|\omega_k + h|$ sur l'ensemble des indices k et h tels que $1 \leq k \leq m$, $0 \leq h \leq \rho_k - 1$ et $\omega_k + h \neq 0$ et posons $\mathcal{V} := D\left(0, \frac{1}{r}\right)$ le disque ouvert de centre 0 et de rayon $\frac{1}{r}$. Alors, la fonction β définie sur $\mathcal{V}$ par

$$\beta(v) = \frac{1}{\prod_{k=1}^{m} \prod_{h=0}^{\rho_k - 1} (1 - (\omega_k + h)v)} \tag{2.5}$$

est holomorphe sur $\mathcal{V}$, on peut donc la développer en série entière :

$$\forall v \in \mathcal{V} \quad \beta(v) = \sum_{\ell=0}^{+\infty} b_\ell v^\ell \tag{2.6}$$

avec $b_0 = \beta(0) = 1$ et convergence normale de la série sur $\mathcal{V}$. Considérons $u \in \gamma$. Alors, pour tout $k \in [\![1, m]\!]$ et tout $h \in [\![0, \rho_k - 1]\!]$ tels que $\omega_k + h \neq 0$,

$$\left|\frac{1}{u}\right| = \frac{1}{R} \leq \frac{1}{|\omega_k| + \rho_k} < \frac{1}{|\omega_k| + h} \leq \frac{1}{|\omega_k + h|} \leq \frac{1}{r}$$

Dès lors, pour tout $u \in \gamma$, on peut écrire

$$\alpha_z(u) = \frac{(1-z)^u}{u^\sigma \prod_{k=1}^{m} \prod_{h=0}^{\rho_k - 1} \left(1 - (\omega_k + h)\frac{1}{u}\right)} = \frac{(1-z)^u}{u^\sigma} \beta\left(\frac{1}{u}\right) = \frac{(1-z)^u}{u^\sigma} \sum_{\ell=0}^{+\infty} b_\ell u^{-\ell} = \sum_{\ell=0}^{+\infty} b_\ell u^{-\ell-\sigma}(1-z)^u$$

On en déduit que, pour tout $z < 1$,

$$T(z) = \frac{1}{2\mathrm{i}\pi} \int_\gamma \sum_{\ell=0}^{+\infty} b_\ell u^{-\ell-\sigma}(1-z)^u \,\mathrm{d}u = \sum_{\ell=0}^{+\infty} b_\ell \left(\frac{1}{2\mathrm{i}\pi} \int_\gamma u^{-\ell-\sigma}(1-z)^u \,\mathrm{d}u\right)$$

Or, la fonction $\varphi_\ell : u \mapsto u^{-\ell-\sigma}(1-z)^u$ admet 0 pour unique pôle sur $D(0, R)$ et ce pôle est d'ordre $\ell + \sigma$. En notant $\delta : u \mapsto (1-z)^u = \mathrm{e}^{u \ln(1-z)}$, on en déduit que le résidu de φ_ℓ en 0 est

$$\mathrm{Rés}(\varphi_\ell, 0) = \frac{1}{(\ell + \sigma - 1)!} \lim_{u \to 0} \delta^{(\ell+\sigma-1)}(u) = \frac{[\ln(1-z)]^{\ell+\sigma-1}}{\Gamma(\ell + \sigma)}.$$

Par suite, la formule des résidus assure que, pour tout $z < 1$,

$$T(z) = \sum_{\ell=0}^{+\infty} b_\ell \frac{[\ln(1-z)]^{\ell+\sigma-1}}{\Gamma(\ell + \sigma)}. \tag{2.7}$$

Sachant que $z \mapsto \ln(1-z)$ est analytique au voisinage de 0 et que $\ln(1-z) = -\sum_{j=1}^{+\infty} \frac{z^j}{j}$ pour tout $|z| < 1$, on en déduit que T est analytique au voisinage de 0, que l'ordre de T est $\sigma - 1$ et que le coefficient de $z^{\sigma-1}$ dans le développement en série entière de T est $b_0 \frac{(-1)^{\sigma-1}}{\Gamma(\sigma)} = \frac{(-1)^{\sigma-1}}{\Gamma(\sigma)}$.

Afin de trouver la même fonction reste que celle définie dans la proposition 2.2.6, on va donc considérer $\tilde{T} := (-1)^{\sigma-1}\Gamma(\rho_1) \cdots \Gamma(\rho_m) T$ plutôt que T.

Appliquons à nouveau la formule des résidus mais cette fois-ci directement à la fonction α_z définie par (2.4). Comme on l'a dit, cette fonction ne possède que des pôles simples en les $\omega_k + h$ sur $D(0, R)$. Alors, en définissant, pour tout complexe u,

$$\phi(u) := \prod_{k=1}^{m} \prod_{h=0}^{\rho_k - 1} (u - \omega_k - h),$$

on obtient

$$\forall z<1 \quad \tilde{T}(z)=(-1)^{\sigma-1}\Gamma(\rho_1)\cdots\Gamma(\rho_m)\sum_{k=1}^{m}\sum_{h=0}^{\rho_k-1}\frac{(1-z)^{\omega_k+h}}{\phi'(\omega_k+h)}$$
$$=\sum_{k=1}^{m}\left[(-1)^{\sigma-1}\Gamma(\rho_1)\cdots\Gamma(\rho_m)\sum_{h=0}^{\rho_k-1}\frac{(1-z)^{h}}{\phi'(\omega_k+h)}\right](1-z)^{\omega_k}.$$

Ainsi, si on pose, pour tout $k\in[\![1,m]\!]$,

$$A_k\left(z\,\middle|\,\begin{array}{ccc}\omega_1 & \cdots & \omega_m\\ \rho_1 & \cdots & \rho_m\end{array}\right):=(-1)^{\sigma-1}\Gamma(\rho_1)\cdots\Gamma(\rho_m)\sum_{h=0}^{\rho_k-1}\frac{(1-z)^{h}}{\phi'(\omega_k+h)}, \tag{2.8}$$

on définit des polynômes $A_1,...,A_m$ tels que $\deg(A_k)=\rho_k-1$ et la fonction $\tilde{T}=\sum_{k=1}^{m}A_kf_{\omega_k}$ est d'ordre exactement $\sigma-1$. On en déduit $(A_1,...,A_m)$ est une famille de $[\rho_1-1,...,\rho_k-1]$ approximants de Padé du système $(f_{\omega_1},...,f_{\omega_m})$ et que $\tilde{T}$ en est la fonction reste associée. Le choix de la constante multiplicative pour $\tilde{T}$ nous assure, de plus, que $\tilde{T}=R$ est la fonction reste définie par (2.2).

2.2.3 Un exemple

Pour terminer ce paragraphe, nous allons donner un exemple explicite de calcul d'approximants de Padé dans un cas simple. Ces polynômes seront au cœur de la démonstration du théorème d'Evertse que nous aborderons au chapitre 3.

Soit $r\in\mathbb{N}$ et $n\in\mathbb{N}^*$. On souhaite trouver un couple de $[r,r]$ approximants de Padé de la fonction $f:=z\mapsto(1-z)^{\frac{1}{n}}$. Ceci revient à déterminer un couple de $[r,r]$ approximants de Padé du système $(1,f)$ i.e. du système $(f_{\omega_1},f_{\omega_2})$ avec $\omega_1=0$ et $\omega_2=\frac{1}{n}$ (et $\rho_1=\rho_2=r+1$). En utilisant (2.8), on peut affirmer que les polynômes A_1 et A_2 définis par

$$A_k(z):=(-1)^{2r+1}\Gamma(r+1)^2\sum_{h=0}^{r}\frac{(1-z)^h}{\phi'(\omega_k+h)}=-(r!)^2\sum_{h=0}^{r}\frac{(1-z)^h}{\phi'(\omega_k+h)}\quad(k\in\{1,2\})$$

conviennent. Ici, la fonction ϕ est définie par $\phi(u):=\prod_{i=0}^{r}(u-i)\prod_{j=0}^{r}\left(u-\frac{1}{n}-j\right)$ donc

$$\phi'(u):=\left(\sum_{i=0}^{r}\prod_{\substack{\ell=0\\ \ell\neq i}}^{r}(u-\ell)\right)\prod_{j=0}^{r}\left(u-\frac{1}{n}-j\right)+\prod_{i=0}^{r}(u-i)\sum_{j=0}^{r}\prod_{\substack{\ell=0\\ \ell\neq j}}^{r}\left(u-\frac{1}{n}-\ell\right).$$

En particulier, pour tout $h\in[\![0,r]\!]$,

$$\phi'(\omega_1+h)=\phi'(h)=\prod_{\substack{\ell=0\\ \ell\neq h}}^{r}(h-\ell)\prod_{j=0}^{r}\left(h-\frac{1}{n}-j\right)$$

et

$$\phi'(\omega_2+h)=\phi'\left(\frac{1}{n}+h\right)=\prod_{i=0}^{r}\left(\frac{1}{n}+h-i\right)\prod_{\substack{\ell=0\\ \ell\neq h}}^{r}(h-\ell).$$

En remarquant que

$$\frac{1}{\prod\limits_{\substack{\ell=0\\ \ell\neq h}}^{r}(h-\ell)} = \frac{1}{h!(-1)^{r-h}(r-h)!} = \frac{(-1)^{r-h}}{r!}\binom{r}{h}$$

et

$$\prod_{j=0}^{r}\left(h-\frac{1}{n}-j\right) = \left[h-\frac{1}{n}\right]\left[\left(h-\frac{1}{n}\right)-1\right]\cdots\left[\left(h-\frac{1}{n}\right)-(r+1)+1\right] = \frac{1}{(r+1)!}\binom{h-\frac{1}{n}}{r+1},$$

on en déduit que

$$A_1(z) = \sum_{h=0}^{r}\frac{(-1)^{r-h-1}\binom{r}{h}}{(r+1)\binom{h-\frac{1}{n}}{r+1}}(1-z)^h. \tag{2.9}$$

De la même façon, on obtient

$$A_2(z) = \sum_{h=0}^{r}\frac{(-1)^{r-h-1}\binom{r}{h}}{(r+1)\binom{h+\frac{1}{n}}{r+1}}(1-z)^h. \tag{2.10}$$

2.3 Une propriété d'indépendance linéaire

On va s'intéresser à des familles d'approximants de Padé d'un même système de fonction binomiales et ayant des degrés différant d'au plus 1. On va montrer que de telles familles possèdent une propriété d'indépendance linéaire qui est primordiale en approximation diophantienne.

On conserve les notations précédentes : ω_1, ..., ω_m sont des réels tels que $\omega_i - \omega_j$ n'est jamais entier pour $i \neq j$ et on note, pour tout $\omega \in \mathbb{R}$, $f_\omega : z \mapsto (1-z)^\omega$. Si r_1, ..., r_m sont des entiers strictement positifs, on note

$$A_k\left(z \,\middle|\, \begin{matrix}\omega_1 & \cdots & \omega_m\\ r_1 & \cdots & r_m\end{matrix}\right) \quad (k \in [\![1,m]\!])$$

les $[r_1-1, ..., r_m-1]$ approximants de Padé de la famille $(f_{\omega_1}, ..., f_{\omega_k})$ tels qu'on les a construit précédemment et

$$R\left(z \,\middle|\, \begin{matrix}\omega_1 & \cdots & \omega_m\\ r_1 & \cdots & r_m\end{matrix}\right) := \sum_{j=1}^{m} A_j\left(z \,\middle|\, \begin{matrix}\omega_1 & \cdots & \omega_m\\ r_1 & \cdots & r_m\end{matrix}\right)(1-z)^{\omega_j}$$

la fonction reste associée.

Considérons m entiers naturels non nuls ρ_1, ..., ρ_m et notons $\sigma = \sum\limits_{k=1}^{m}\rho_k$. On définit, pour tout $(i,j) \in [\![1,m]\!]^2$, le polynôme $A_{ij}(z)$ en posant

$$A_{ij}(z) := A_j\left(z \,\middle|\, \begin{matrix}\omega_1 & \cdots & \omega_m\\ \rho_1+\delta_{i1} & \cdots & \rho_m+\delta_{im}\end{matrix}\right) \tag{2.11}$$

où δ_{ij} est le symbole de Kronecker. De plus, pour tout $i \in [\![1,m]\!]$, on note R_i la fonction reste associée à la famille $(A_{ij})_{j\in[\![1,m]\!]}$ i.e. la fonction définie par

$$R_i(z) := \sum_{j=1}^{m} A_{ij}(z)(1-z)^{\omega_j} \tag{2.12}$$

On va démontrer le résultat « d'indépendance linéaire » suivant.

Proposition 2.3.1. — *Il existe une constante non nulle c (dépendant de ω_1, ..., ω_m et de ρ_1, ..., ρ_m) telle que*

$$\forall z \in \mathbb{C} \qquad \det_{1\leq i,j\leq m}(A_{ij}(z)) = cz^{\sigma}.$$

Preuve. — Notons $D(z) := \det_{1\leq i,j\leq m}(A_{ij}(z))$. Par définition, les $A_{ij}(z)$ sont des polynômes en z de degrés exactement $\rho_i - 1 + \delta_{ij}$. Ainsi,

$$D(z) = \begin{vmatrix} A_{11}(z) & \cdots & A_{1n}(z) \\ \vdots & \ddots & \vdots \\ A_{n1}(z) & \cdots & A_{nn}(z) \end{vmatrix}$$

est un polynôme en z de degré au plus $\sigma = \sum_{i=1}^{m} \rho_i$. Par ailleurs, en développant $D(z)$ selon la $j-$ème colonne et en notant $D_{ij}(z) = \det_{\substack{1\leq h,k\leq m \\ h\neq i \\ k\neq j}}(A_{hk}(z))$ les mineurs associés, on obtient,

$$D(z)(1-z)^{\omega_j} = \sum_{i=1}^{m}(-1)^{i+j}D_{ij}(z)A_{ij}(z)(1-z)^{\omega_j}$$

Or, si $k \in [\![1, m]\!]$ est différent de j, $\sum_{i=1}^{m}(-1)^{i+j}D_{ij}(z)A_{ik}(z) = 0$ car cela correspond au développement selon la $j-$ème colonne du déterminant d'une matrice dans laquelle la $j-$ème colonne et la $k-$ième colonne sont égales. On en déduit que

$$\begin{aligned} D(z)(1-z)^{\omega_j} &= \sum_{i=1}^{m}(-1)^{i+j}D_{ij}(z)A_{ij}(z)(1-z)^{\omega_j} + \sum_{\substack{k=1 \\ k\neq j}}^{m}\left(\sum_{i=1}^{m}(-1)^{i+j}D_{ij}(z)A_{ik}(z)\right)(1-z)^{\omega_k} \\ &= \sum_{i=1}^{m}(-1)^{i+j}D_{ij}(z)\sum_{k=1}^{m}A_{ik}(z)(1-z)^{\omega_k} = \sum_{i=1}^{m}(-1)^{i+j}D_{ij}(z)R_i(z) \end{aligned}$$

Par définition, 0 est une racine d'ordre exactement σ de chaque $R_i(z)$ donc 0 est une racine d'ordre au moins σ de $D(z)$. Comme $D(z)$ est un polynôme en z de degré au plus σ, on en déduit qu'il existe une constante c telle que $D(z) = cz^{\sigma}$. De plus, en raison des degrés des polynômes $A_{ij}(z)$, c est le produit des coefficients dominants des $A_{ii}(z)$. Enfin, ces polynômes étant non nuls (car $\deg(A_{ii}) = \rho_i > 0$), $c \neq 0$. ■

Remarque 2.3.2. — Dans [24], Mahler précise, dans la note en bas de la page 272, qu'un calcul direct donne

$$D(z) = \pm \prod_{\substack{i,j=1 \\ i\neq j}}^{m} \frac{\Gamma(\omega_i - \omega_j)\Gamma(\rho_j)}{\Gamma(\rho_j + \omega_i - \omega_j)} z^{\sigma}.$$

Cette égalité est, cependant, fausse comme on le montre dans l'annexe A.

Chapitre 3

Le théorème d'Evertse Les cas $a \neq b+1$

3.1 Présentation des résultats

Le but de ce chapitre est d'obtenir, pour chaque valeur de $n \geq 3$, un majorant de a au-delà duquel l'équation $(E_n) : ax^n - by^n = 1$ a au plus une solution non triviale si $a \neq b+1$. Pour ce faire, nous allons suivre la méthode d'Evertse [13]. Notre résultat est plus précis que celui d'Evertse mais moins général que ce dernier qui est valable pour toute équation de la forme $|ax^n - by^n| = c$ avec $c \in \mathbb{N}^*$.

Dans toute la suite, si $n = 4$ ou si n est un nombre premier, on définit α_n par le tableau suivant :

n	α_n
3	0,6377
4	0,5172
5	0,4730
7	0,4159
11	0,3634
13	0,3486
17	0,3285
19	0,3213
23	0,3104
29	0,2993
31	0,2964
37	0,2896
41	0,2861
43	0,2846
47	0,2819
53	0,2786
59	0,2759
61	0,2751
67	0,2730
71	0,2718
73	0,2713
79	0,2697
83	0,2689
89	0,2677

n	α_n
97	0,2663
101	0,2657
103	0,2654
107	0,2648
109	0,2646
113	0,2641
127	0,2626
131	0,2622
137	0,2617
139	0,2616
149	0,2608
151	0,2607
157	0,2603
163	0,2599
167	0,2597
173	0,2594
179	0,2591
181	0,2590
191	0,2585
193	0,2585
197	0,2583
199	0,2582
211	0,2578
223	0,2574

n	α_n
227	0,2572
229	0,2572
233	0,2571
239	0,2569
241	0,2568
251	0,2566
257	0,2564
263	0,2563
269	0,2561
271	0,2561
277	0,2560
281	0,2559
283	0,2558
293	0,2557
307	0,2554
311	0,2553
313	0,2553
317	0,2552
331	0,2550
337	0,2549
347	0,2548
349	0,2548
353	0,2547
359	0,2546

n	α_n
367	0,2545
373	0,2545
379	0,2544
383	0,2544
389	0,2543
397	0,2542
401	0,2542
409	0,2541
419	0,2540
421	0,2540
431	0,2539
433	0,2539
439	0,2538
443	0,2538
449	0,2537
457	0,2537
461	0,2536
463	0,2536
467	0,2536
479	0,2535
487	0,2535
491	0,2534
499	0,2534
503	0,2534

n	α_n
509	0,2533
521	0,2532
523	0,2532
541	0,2531
547	0,2531
557	0,2530
563	0,2530
569	0,2530
571	0,2530
577	0,2529
587	0,2529
593	0,2529
599	0,2528
601	0,2528
607	0,2528
613	0,2528
617	0,2527
619	0,2527
631	0,2527
641	0,2526
≥ 643	0,2526

Tableau 3.1 : Les valeurs de α_n pour $n = 4$ ou n premier

Si n est un nombre composé supérieur ou égal à 6, on pose $\alpha_n = 3^{\frac{1-n}{1+n}}$.
On pose $\beta_3 = 3{,}022$, $\beta_4 = 2{,}001$, $\beta_5 = 1{,}667$ et, pour tout $n \geq 6$, $\beta_n = \frac{n}{n-2}$.
Pour tout entier $n \geq 3$, on définit t_n par

$$t_n = n \prod_{\substack{p|n \\ p \text{ premier}}} p^{\frac{1}{p-1}}.$$

Enfin, on définit, pour tout $n \geq 3$, $c_n := (\alpha_n t_n)^{\beta_n}$
On va alors démontrer le théorème suivant.

Théorème 3.1.1. — *L'équation (E_n) admet au plus une solution (x, y) telle que $ax^n \geq c_n$.*

Les valeurs de c_n, arrondies par excès, correspondant aux valeurs de α_n du tableau précédent sont données ci-dessous :

n	c_n
3	37,36
4	17,15
5	8,22
7	7,03
11	7,30
13	7,68
17	8,59
19	9,07
23	10,07
29	11,60
31	12,11
37	13,65
41	14,68
43	15,19
47	16,22
53	17,77
59	19,31
61	19,83
67	21,36
71	22,29
73	22,91
79	24,44
83	25,47
89	26,9996

n	c_n
97	29,05
101	30,07
103	30,58
107	31,59
109	32,11
113	33,12
127	36,69
131	37,70
137	39,22
139	39,74
149	42,27
151	42,79
157	44,31
163	45,82
167	46,84
173	48,37
179	49,99
181	50,39
191	52,92
193	53,44
197	54,45
199	54,95
211	57,99
223	61,03

n	c_n
227	62,02
229	62,54
233	63,56
239	65,07
241	65,56
251	68,10
257	69,60
263	71,13
269	72,63
271	73,14
277	74,67
281	75,67
283	76,16
293	78,71
307	82,22
311	83,22
313	83,73
317	84,73
331	88,26
337	89,77
347	92,30
349	92,82
353	93,81
359	95,31

n	c_n
397	97,32
373	98,86
379	100,36
383	101,39
389	102,88
397	104,89
401	105,91
409	107,92
419	110,43
421	110,94
431	113,45
433	113,97
439	115,45
443	116,47
449	117,96
457	119,997
461	120,97
463	121,48
467	122,51
479	125,01
487	127,56
491	128,52
499	130,56
503	131,58

n	c_n
509	133,06
521	136,06
523	136,57
541	141,10
547	142,62
557	145,11
563	146,63
569	148,16
571	148,67
577	150,13
587	152,67
593	154,20
599	155,41
601	156,17
607	157,69
613	159,22
617	160,17
619	160,68
631	163,72
641	166,20
643	166,70

Tableau 3.2 : Les valeurs de c_n pour $n = 4$ ou n premier inférieur à 643

On en déduira le corollaire suivant.

Corollaire 3.1.2. — *Si $n \geq 5$ et si $a \neq b + 1$ alors l'équation (E_n) admet au plus une solution non triviale.*

3.2 Propriétés arithmétiques d'approximants de Padé d'une fonction binomiale

Dans tout ce paragraphe, sauf mention explicite du contraire, r désigne un entier naturel non nul.

Lemme 3.2.1. — *On définit, pour tout $z \in \mathbb{C}$, les polynômes*

$$A_r(z) = \sum_{k=0}^{r} \frac{(-1)^{r-k-1}\binom{r}{k}}{(r+1)\binom{k-\frac{1}{n}}{r+1}} z^k \quad et \quad B_r(z) = \sum_{k=0}^{r} \frac{(-1)^{r-k}\binom{r}{k}}{(r+1)\binom{k+\frac{1}{n}}{r+1}} z^k. \tag{3.1}$$

Alors, il existe un polynôme $V_r(z)$ tel que, pour tout $z \in \mathbb{C}$,

$$A_r(z^n) - zB_r(z^n) = (1-z)^{2r+1}V_r(z).$$

De plus, $V_r(1) = n^{2r+1}\dfrac{r!^2}{(2r+1)!}$.

Preuve. — D'après les égalités (2.9) et (2.10), les polynômes $A_r(1-z)$ et $-B_r(1-z)$ forment une famille de $[r,r]$ approximants de Padé de la fonction $f : z \mapsto (1-z)^{\frac{1}{n}}$ donc, pour tout $z < 1$,

$$A_r(1-z) - B_r(1-z)(1-z)^{\frac{1}{n}} = R(z)$$

où la fonction reste R est d'ordre $2r+1$ avec, de plus, par construction, $R^{(2r+1)}(0) = \dfrac{r!^2}{(2r+1)!}$. Ainsi, il existe une fonction $\tilde{R}$ analytique au voisinage de 0 telle que, pour tout $z < 1$, $R(z) = z^{2r+1}\tilde{R}(z)$ et $\tilde{R}(0) = \dfrac{r!^2}{(2r+1)!}$. On en déduit que, pour tout $z > 0$,

$$A_r(z) - B_r(z)z^{\frac{1}{n}} = (1-z)^{2r+1}\tilde{R}(1-z)$$

et donc

$$\forall z > 0 \quad A_r(z^n) - zB_r(z^n) = (1-z^n)^{2r+1}\tilde{R}(1-z^n).$$

Dans cette égalité, le terme de gauche est un polynôme en z et le terme de droite est le produit du polynôme $(1-z)^{2r+1}$ et de la fonction $z \mapsto \tilde{R}(1-z^n)$ qui est définie en $z = 1$ donc $\tilde{R}(1-z^n)$ est un polynôme en z. En écrivant $(1-z^n)^{2r+1} = (1-z)^{2r+1}\left(\sum_{k=0}^{n-1} z^k\right)^{2r+1}$, on en déduit que

$$\forall z > 0 \quad A_r(z^n) - zB_r(z^n) = (1-z)^{2r+1}V_r(z) \tag{3.2}$$

en posant $V_r(z) := \left(\sum_{k=0}^{n-1} z^k\right)\tilde{R}(1-z^n)$. Ceci définit bien un polynôme qui, de plus, vérifie

$$V(1) = \left(\sum_{k=0}^{n-1} 1^k\right)^{2r+1} \tilde{R}(0) = \frac{r!^2}{(2r+1)!}n^{2r+1}.$$

Pour finir, l'égalité (3.2) s'étant à tout $z \in \mathbb{C}$ car il s'agit d'une égalité entre polynômes. ∎

Les polynômes ainsi définis sont à coefficients rationnels. Le lemme suivant va nous permettre de déterminer un rationnel δ_r tel que $\delta_r A_r(z)$ et $\delta_r B_r(z)$ soient à coefficients entiers.

Lemme 3.2.2. — *Soit k et j deux entiers naturels et p un nombre premier ne divisant pas n. On note v_p la valuation $p-$adique. Alors,*

$$v_p\left(\binom{\frac{j}{n}}{k}\right) \geq 0.$$

Preuve. — Par définition,

$$\binom{\frac{j}{n}}{k} = \frac{\frac{j}{n}\left(\frac{j}{n}-1\right)...\left(\frac{j}{n}-k+1\right)}{k!} = \frac{j(j-n)...(j-(k-1)n)}{n^k k!} = \frac{\prod_{\ell=0}^{k-1}(j-\ell k)}{n^k k!}. \tag{3.3}$$

Si $p > k$ alors p ne divise pas $n^k k!$ donc le résultat est évident. Si $p < k$, notons α la plus grande puissance de p telle que $p^\alpha \leq k$. Comme p ne divise pas n, il s'agit de montrer que $v_p\left(\prod_{\ell=0}^{k-1}(j-\ell k)\right) \geq v_p(k!)$. Pour ce faire, il est suffisant de montrer que, pour tout $m \in [\![1, \alpha]\!]$, le nombre $\nu_1(m)$ de multiples de p^m compris entre 1 et k est inférieur ou égal au nombre $\nu_2(m)$ de multiples de p^m de la forme $j - \ell k$ pour $\ell \in [\![0, k-1]\!]$.

Considérons un tel m. D'une part, il est clair que $\nu_1(m) = \left\lfloor \frac{k}{p^m} \right\rfloor$. D'autre part, pour déterminer $\nu_2(n)$, remarquons que, comme p ne divise pas n, n admet un inverse $\tilde{n}$ modulo p^m. On a alors $p^m \mid j - \ell n$ si et seulement si $\ell \equiv j\tilde{n}\ [p^m]$. Notons j_m le reste de $j\tilde{n}$ modulo p^m. Alors, $\nu_2(m)$ est égal au nombre d'entiers $\ell \in [\![0, k-1]\!]$ tels que $\ell \equiv j_m\ [p^m]$. Or, par définition, $0 \leq j_m < p^m \leq k$ donc $j_m \in [\![0, k-1]\!]$ et ainsi les entiers $\ell \in [\![0, k-1]\!]$ tels que $p^m \mid j - \ell n$ sont les entiers de la forme $j_m + up^m$ où u est un entier tel $0 \leq u \leq \frac{k-1-j_m}{p^m}$. Il y en a donc $1 + \left\lfloor \frac{k-1-j_m}{p^m} \right\rfloor = \left\lfloor \frac{k+p^m-(j_m+1)}{p^m} \right\rfloor$ et comme $j_m + 1 \leq p^m$, $\left\lfloor \frac{k+p^m-(j_m+1)}{p^m} \right\rfloor \geq \left\lfloor \frac{k}{p^m} \right\rfloor$ i.e. $\nu_2(m) \geq \nu_1(m)$. ■

Dans toute la suite, on note, pour tout entier $r \geq 1$, δ_r le rationnel positif défini par

$$\delta_r := (r+1)\binom{r+\frac{1}{n}}{r+1}\binom{r-\frac{1}{n}}{r} n^r \mathrm{PGCD}(n^r, r!). \tag{3.4}$$

Proposition 3.2.3. — *Pour tout $r \geq 1$, les polynômes $\delta_r A_r(z)$ et $\delta_r B_r(z)$ sont à coefficient entiers naturels.*

Preuve. — Soit $r \geq 1$ et $k \in [\![0, r]\!]$. Notons a_k le coefficient de z^k dans $A_r(z)$. Alors,

$$\delta_r a_k = (-1)^{r-k-1} \frac{\binom{r}{k}\binom{r+\frac{1}{n}}{r+1}\binom{r-\frac{1}{n}}{r}}{\binom{k-\frac{1}{n}}{r+1}} n^r \mathrm{PGCD}(n^r, r!). \tag{3.5}$$

Or,

$$\begin{aligned}
\frac{\binom{r}{k}\binom{r+\frac{1}{n}}{r+1}\binom{r-\frac{1}{n}}{r}}{\binom{k-\frac{1}{n}}{r+1}} &= \frac{r!}{k!(r-k)!} \times \frac{\prod_{j=0}^{r}\left(r+\frac{1}{n}-j\right)}{(r+1)!} \times \frac{\prod_{j=0}^{r-1}\left(r-\frac{1}{n}-j\right)}{r!} \times \frac{(r+1)!}{\prod_{j=0}^{r}\left(k-\frac{1}{n}-j\right)} \\
&= \frac{\prod_{j=0}^{k-1}\left(r+\frac{1}{n}-j\right)}{k!} \times \frac{\prod_{j=0}^{r-k-1}\left(r-\frac{1}{n}-j\right)}{(r-k)!} \times \frac{\prod_{j=k}^{r}\left(r+\frac{1}{n}-j\right)\prod_{j=r-k}^{r-1}\left(r-\frac{1}{n}-j\right)}{\prod_{j=0}^{k-1}\left(k-\frac{1}{n}-j\right)\prod_{j=k}^{r}\left(k-\frac{1}{n}-j\right)} \\
&= \binom{r+\frac{1}{n}}{k}\binom{r-\frac{1}{n}}{r-k} \frac{\prod_{j=k}^{r}\left(r+\frac{1}{n}-j\right)\prod_{j=r-k}^{r-1}\left(r-\frac{1}{n}-j\right)}{\prod_{j=0}^{k-1}\left(k-\frac{1}{n}-j\right)\prod_{j=k}^{r}\left(k-\frac{1}{n}-j\right)}
\end{aligned}$$

De plus, par les changements d'indices $s = j - r + k$ et $t = r + k - j$,

$$\prod_{j=r-k}^{r-1}\left(r-\frac{1}{n}-j\right)=\prod_{s=0}^{k-1}\left(k-\frac{1}{n}-s\right)$$

et

$$\prod_{j=k}^{r}\left(k-\frac{1}{n}-j\right)=\prod_{t=r}^{k}\left(-r-\frac{1}{n}+t\right)=(-1)^{r-k+1}\prod_{t=k}^{r}\left(r+\frac{1}{n}-t\right).$$

Ainsi,

$$\delta_r a_k=\binom{r+\frac{1}{n}}{k}\binom{r-\frac{1}{n}}{r-k}n^r\mathrm{PGCD}(n^r,r!).\ ^{(1)} \tag{3.6}$$

Ceci prouve déjà que $\delta_r A_r(z)$ est à coefficients positifs car $r \geq k$. Montrons à présent que $\delta_r a_k$ est entier. Pour cela, nous allons montrer que la valuation $p-$adique de $\delta_r a_k$ est positive ou nulle pour tout nombre premier p.

Soit p un nombre premier.

Si p divise n, notons $\alpha = v_p(n)$. Alors, étant donné que $v_p(r!) = \sum_{m=1}^{+\infty}\left\lfloor\frac{r}{p^m}\right\rfloor \leq \sum_{m=1}^{+\infty}\frac{r}{p^m} = \frac{r}{p-1} \leq \alpha r$, on peut dire que $v_p(\mathrm{PGCD}(n^r, r!)) = v_p(r!)$ et donc $v_p(n^r\mathrm{PGCD}(n^r, r!)) = \alpha r + v_p(r!)$. Or, d'après l'égalité (3.3), on a $v_p\left(\binom{r+\frac{1}{n}}{k}\right) \geq -\alpha k - v_p(k!)$ et $v_p\left(\binom{r-\frac{1}{n}}{r-k}\right) \geq -\alpha(r-k) - v_p((r-k)!)$. Ainsi, on déduit de (3.6) que

$$v_p(\delta_r a_k) \geq -\alpha k - v_p(k!) - \alpha(r-k) - v_p((r-k)!) + \alpha r + v_p(r!) = v_p\left(\frac{r!}{k!(r-k)!}\right) = v_p\left(\binom{r}{k}\right) \geq 0.$$

Si p ne divise pas n alors $v_p(n^r\mathrm{PGCD}(n^r, r!)) = 0$ et, d'après le lemme 3.2.2, $v_p\left(\binom{r+\frac{1}{n}}{k}\right) \geq 0$ et $v_p\left(\binom{r-\frac{1}{n}}{r-k}\right) \geq 0$ ce qui assure que $v_p(\delta_r a_k) \geq 0$.

On conclut que $\delta_r A_r(z)$ est un polynôme à coefficients dans $\mathbb{N}$.

Le raisonnement est identique pour $\delta_r B_r(z)$ en montrant que, si on note b_k le coefficient de z^k dans $B_r(z)$ alors

$$\delta_r b_k=\binom{r-\frac{1}{n}}{r}\binom{r+\frac{1}{n}}{r-k}n^r\mathrm{PGCD}(n^r,r!)$$

ce qui permet de conclure. ■

Proposition 3.2.4. — *Pour tout $r \geq 1$, $V_r(z)$ est un polynôme à coefficients positifs.*

Preuve. — On sait déjà que $V_r(z)$ est un polynôme et que, par construction, pour tout $z > 0$, $(1-z)^{2r+1}V_r(z) = R(1-z^n)$ où R est la fonction reste associée aux $[r, r]$ approximants de Padé de la fonction $z \mapsto (1-z)^{\frac{1}{n}}$. Or, d'après la proposition 2.2.6, pour tout $z < 1$,

$$R(z)=R\left(z\,\middle|\,\begin{matrix}0 & \frac{1}{n}\\ r+1 & r+1\end{matrix}\right)=\int_0^z(z-u)^r u^r(1-u)^{\frac{1}{n}-r-1}\,\mathrm{d}u.$$

Il s'ensuit que, pour tout $z > 0$,

$$R(1-z^n)=\int_0^{1-z^n}(1-z^n-u)^r u^r(1-u)^{\frac{1}{n}-r-1}\,\mathrm{d}u$$

(1). On retrouve ici les coefficients du polynôme A_m de Evertse (égalité (1.1) de [13]).

et donc, par le changement de variable $u = 1 - t^n$,

$$R(1-z^n) = \int_1^z (t^n - z^n)^r (1-t^n)^r t^{-nr-n+1}(-nt^{n-1})\,\mathrm{d}t = n\int_z^1 (t^n - z^n)^r (1-t^n)^r t^{-nr}\,\mathrm{d}t.$$

Ainsi, pour tout $z \in]0\,;1[$,

$$V_r(z) = \frac{n}{(1-z)^{2r+1}} \int_z^1 (t^n - z^n)^r (1-t^n)^r t^{-nr}\,\mathrm{d}t.$$

Définissons, pour tout $r \geq 0$, la fonction F_r par

$$\forall z \in]0\,;1[\qquad F_r(z) = \frac{1}{(1-z)^{2r+1}} \int_z^1 (t^n - z^n)^r (1-t^n)^r t^{-nr}\,\mathrm{d}t.$$

On a donc, pour tout $r \geq 1$ et tout $z \in]0\,;1[$, $V_r(z) = nF_r(z)$ de sorte que F_r est une fonction polynômiale. De plus,

$$\forall z \in]0\,;1[\quad F_0(z) = \frac{1}{1-z}\int_z^1 \mathrm{d}t = 1$$

donc F_0 est également une fonction polynomiale.

Remarquons que, pour tout $r \in \mathbb{N}$ et tout $z \in]0\,;1[$,

$$F_r'(z) = \frac{2r+1}{(1-z)^{2r+2}} \int_z^1 (t^n - z^n)^r (1-t^n)^r t^{-nr}\,\mathrm{d}t - \frac{nrz^{n-1}}{(1-z)^{2r+1}} \int_z^1 (t^n - z^n)^{r-1}(1-t^n)^r t^{-nr}\,\mathrm{d}t$$

i.e. si on définit, pour tout $r \in \mathbb{N}$, W_r par,

$$\forall z \in]0\,;1[\quad W_r(z) = \frac{nrz^{n-1}}{(1-z)^{2r}} \int_z^1 (t^n - z^n)^{r-1}(1-t^n)^r t^{-nr}\,\mathrm{d}t$$

alors

$$\forall z \in]0\,;1[\quad W_r(z) = (2r+1)F_r(z) - (1-z)F_r'(z) \tag{3.7}$$

ce qui assure que W_r est également une fonction polynomiale pour tout $r \in \mathbb{N}$. Calculons sa dérivée pour $r \geq 1$. Pour simplifier, on pose, pour tout $h \geq 0$, $g_h(t,z) := (t^n - z^n)^h (1-t^n)^r t^{-nr}$ et $g_h(t,z) = 0$ si $h = -1$. Il vient alors, pour tout $z \in]0\,;1[$,

$$W_r'(z) = \frac{nr(n-1)z^{n-2}}{(1-z)^{2r}} \int_z^1 g_{r-1}(t,z)\,\mathrm{d}t + \frac{2nr^2 z^{n-1}}{(1-z)^{2r+1}} \int_z^1 g_{r-1}(t,z)\,\mathrm{d}t - \frac{n^2 r(r-1)z^{2n-2}}{(1-z)^{2r}} \int_z^1 g_{r-2}(t,z)\,\mathrm{d}t$$

et donc

$$(1-z)W_r'(z) = 2rW_r(z) - \frac{nrz^{n-2}}{(1-z)^{2r-1}} \int_z^1 n(r-1)z^n g_{r-2}(t,z) - (n-1)g_{r-1}(t,z)\,\mathrm{d}t. \tag{3.8}$$

Or, si $r \geq 2$,

$$\begin{aligned} n(r-1)z^n g_{r-2}(t,z) - (n-1)g_{r-1}(t,z) &= [n(r-1)z^n - (n-1)(t^n - z^n)]\,(t^n - z^n)^{r-2}(1-t^n)^r t^{-nr} \\ &= [n(r-1)t^n - (nr-1)(t^n - z^n)]\,(t^n - z^n)^{r-2}(1-t^n)^r t^{-nr} \end{aligned}$$

et donc une intégration par parties montre que, pour tout $r \geq 2$,

$$\begin{aligned} nr\int_z^1 (t^n - z^n)^{r-1}(1-z^n)^{r-1} t^{-n(r-1)}\,\mathrm{d}t &= -\int_z^1 [(t^n - z^n)^{r-1} t^{-nr+1}](-rnt^{n-1})(1-t^n)^{r-1}\,\mathrm{d}t \\ &= 0 + \int_z^1 [(r-1)nt^{n-1}(t^n - z^n)^{r-2}t^{-nr+1} + (t^n - z^n)^{r-1}(-nr+1)t^{-nr}](1-t^n)^r\,\mathrm{d}t \\ &= \int_z^1 [n(r-1)t^n - (nr-1)(t^n - z^n)](t^n - z^n)^{r-2}(1-t^n)^r t^{-nr}\,\mathrm{d}t \\ &= \int_z^1 n(r-1)z^n g_{r-2}(t,z) - (n-1)g_{r-1}(t,z)\,\mathrm{d}t \end{aligned}$$

On déduit alors de (3.8) que, pour tout $r \geq 2$,

$$2rW_r(z) - (1-z)W_r'(z) = (nr)^2 z^{n-2} \frac{1}{(1-z)^{2r-1}} \int_z^1 (t^n - z^n)^{r-1}(1-z^n)^{r-1} t^{-n(r-1)} \, \mathrm{d}t$$

i.e.

$$2rW_r(z) - (1-z)W_r'(z) = (nr)^2 z^{n-2} F_{r-1}(z).$$

De plus, pour $r = 1$, on a

$$\forall z \in]0\,;1[\quad (1-z)^2 W_1(z) = nz^{n-1} \int_z^1 t^{-n} - 1 \, \mathrm{d}t = \frac{n}{n-1}\left(1 - nz^{n-1} + (n-1)z^n\right)$$

donc, en dérivant,

$$\forall z \in]0\,;1[\quad -2(1-z)W_1(z) + (1-z)^2 W_1'(z) = n^2 z^{n-2}(z-1)$$

et donc, puisque $F_0(z) = 1$ pour tout z,

$$2W_1(z) - (1-z)W_1'(z) = n^2 z^{n-2} F_0(z).$$

On peut donc affirmer que, pour tout $r \in \mathbb{N}^*$ et tout $z \in]0\,;1[$,

$$2rW_r(z) - (1-z)W_r'(z) = (nr)^2 z^{n-2} F_{r-1}(z) \tag{3.9}$$

Nous disposons à présent de tout le nécessaire pour démontrer que les coefficients de F_r sont positifs ce qui est suffisant pour conclure puisque $V_r = nF_r$. On raisonne par récurrence sur r. Pour $r = 0$, le résultat est évident car $F_0 = 1$. Supposons que, pour un certain rang $r \in \mathbb{N}^*$, F_{r-1} ait des coefficients positifs. Ecrivons alors $F_{r-1}(z) = \sum_{j=0}^{+\infty} a_j z^j$ et $W_r = \sum_{j=0}^{+\infty} w_j z^j$ où les suites (a_j) et (w_j) sont presque nulles. Alors, d'après (3.9),

$$2r \sum_{j=0}^{+\infty} w_j z^j - (1-z) \sum_{j=0}^{+\infty} j w_j z^{j-1} = (nr)^2 \sum_{j=0}^{+\infty} a_j z^{j+n-2}$$

donc, en posant $a_{j-n+2} := 0$ si $j < n-2$, il vient, pour tout $j \in \mathbb{N}$,

$$(2r+j)w_j = (nr)^2 a_{j-n+2} + (j+1)w_{j+1}.$$

Par hypothèse de récurrence, pour tout $j \in \mathbb{N}$, $(nr)^2 a_{j-n+2} \geq 0$ donc, si w_{j+1} est positif ou nul, il en est de même pour w_j. Or, la suite (w_j) est presque nulle donc, par une récurrence (finie et descendante) sur j, tous les w_j sont positifs ou nuls. Ecrivons alors $F_r(z) = \sum_{j=0}^{+\infty} b_j z^j$. D'après (3.7),

$$\sum_{j=0}^{+\infty} w_j z^j = (2r+1) \sum_{j=0}^{+\infty} b_j z^j - (1-z) \sum_{j=0}^{+\infty} j b_j z^{j-1}$$

donc, pour tout $j \in \mathbb{N}$,

$$(2r+j+1)b_j = w_j + (j+1)b_{j+1}$$

et on conclut comme précédemment que, puisque tous les w_j sont positifs ou nuls, il en est de même des b_j et ainsi F_r est à coefficients positifs. ■

Lemme 3.2.5. — *Pour tout $r \geq 1$ et pour tout réel $z \in [0\,;1]$,*

$$0 \leq \delta_r A_r(z) \leq \binom{2r}{r} n^r \mathrm{PGCD}(n^r, r!) \quad \textit{et} \quad 0 \leq V_r(z) \leq n^{2r+1} \frac{r!^2}{(2r+1)!}.$$

Preuve. — Le polynôme $\delta_r A_r(z)$ étant à coefficients positifs, pour tout $z \in [0\,;1]$,

$$0 \leq \delta_r A_r(z) \leq \delta_r A_r(1).$$

Or, d'après la formule de Vandermonde généralisée,

$$\sum_{k=0}^{r} \binom{r+\frac{1}{n}}{k} \binom{r-\frac{1}{n}}{r-k} = \binom{2r}{r}$$

donc, d'après l'identité (3.6), $\delta_r A_r(1) = \binom{2r}{r} n^r \mathrm{PGCD}(n^r, r!)$.

Par ailleurs, la proposition 3.2.4 assure que V_r est à coefficients positifs donc, pour tout $z \in [0\,;1]$, $0 \leq V_r(z) \leq V_r(1)$ ce qui permet de conclure car, d'après le lemme 3.2.1, $V_r(1) = n^{2r+1} \dfrac{r!^2}{(2r+1)!}$. ■

3.3 Cas particuliers et lemmes préliminaires

Lemme 3.3.1. — *Pour tout $n \geq 3$, $c_n \geq 7$ et, pour tout $n \geq 647$ premier, $c_n \geq 167$.*

Preuve. — On vérifie la propriété pour $n \in [\![3, 20]\!]$ et si n est un nombre premier inférieur ou égal à 643. Si n est un nombre premier supérieur ou égal à 647 alors $c_n = \left(0{,}2526 n^{\frac{n}{n-1}}\right)^{\frac{n}{n-2}}$ croit avec n donc $c_n \geq c_{647} \approx 167{,}7$. Enfin, dans les autres cas, $n \geq 21$ et alors comme $\frac{n-1}{n+1} \leq 1$, $\alpha_n \geq \frac{1}{3}$ donc, comme $t_n \geq n$, $\alpha_n t_n \geq \frac{n}{3} \geq 7$. Finalement, sachant que $\beta_n \geq 1$, on a, à plus forte raison, $c_n \geq 7$. ■

Lemme 3.3.2. — *Pour tout $n \geq 3$ et tout $r \geq 1$, $n^r \mathrm{PGCD}(n^r, r!) \leq t_n^r$.*

Preuve. — Il suffit de montrer que $\mathrm{PGCD}(n^r, r!) \leq \left(\prod_{p|n} p^{\frac{1}{p-1}}\right)^r$. Or, si p est un diviseur premier de n alors, comme on l'a vu dans la preuve de la proposition 3.2.3, $v_p(\mathrm{PGCD}(n^r, r!)) = v_p(r!) \leq \frac{r}{p-1}$ donc $\mathrm{PGCD}(n^r, r!) = \prod_{p|n} p^{v_p(\mathrm{PGCD}(n^r, r!))} \leq \left(\prod_{p|n} p^{\frac{1}{p-1}}\right)^r$. ■

D'après le lemme 1.4.1, on peut supposer que ab n'est pas la puissance $n-$ième d'un entier (ou, ce qui est équivalent, que $\frac{a}{b}$ n'est pas la puissance $n-$ième d'un rationnel). En particulier, $ab \geq 2$.

Le lemme suivant va jouer un rôle fondamental dans la démonstration du théorème 3.1.1. L'idée générale qui va être utilisée dans la suite est que, si (x_1, y_1) et (x_2, y_2) sont deux solutions distinctes de (E_n) telles que $ax_2 \geq ax_1 \geq c_n$ alors il y a un *grand écart* [(2)] entre ces deux solutions. Le point (i), dû à Evertse ([13] lemme 2.6 (i)), donne un majorant particulièrement précis de $1 - \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y}{x}$ pour une solution (x, y) de (E_n) telle que $ax^n \geq c_n$. Le point (ii) est une amélioration du lemme 2.6 (ii) d'Evertse qui permet de supprimer un facteur 2^n dans le majorant, ce qui jouera un rôle déterminant pour les petites valeurs de n.

Dans toute la suite, on pose

$$s_n = \left(\frac{c_n}{c_n - 1}\right)^{\frac{n-1}{2n}} \tag{3.10}$$

(2). En anglais, on parle de *gap principle*. Cette idée était déjà à la base du résultat de Siegel [39].

Lemme 3.3.3. *(i) Soit (x, y) une solution de (E_n). Si $ax^n \geq c_n$ alors*

$$0 < 1 - \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y}{x} < \frac{s_n}{nax^n}.$$

(ii) Si (x_1, y_1) et (x_2, y_2) sont deux solutions différentes de (E_n) telles que $ax_2 \geq ax_1 \geq c_n$ alors

$$ax_2^n \geq 2\left(\frac{n}{s_n}\right)^n (ax_1^n)^{n-1}.$$

Preuve. — (i) Etant donné que $ax^n - by^n = 1$, on a $1 - \frac{b}{a}\left(\frac{y}{x}\right)^n = \frac{1}{ax^n}$. Il s'ensuit que

$$\left(1 - \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y}{x}\right) \sum_{k=0}^{n-1} \left(\left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y}{x}\right)^k = \frac{1}{ax^n}. \tag{3.11}$$

Or, la somme est une somme de terme positifs et $\frac{1}{ax} > 0$ donc $1 - \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y}{x} > 0$.

Pour la majoration, nous réutilisons l'inégalité (3.11) en remarquant que, d'après la comparaison entre moyenne arithmétique et moyenne géométrique (l'inégalité étant stricte car $\left(\frac{a}{b}\right)^{\frac{1}{n}} \neq \frac{y}{x}$),

$$\sum_{k=0}^{n-1} \left(\left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y}{x}\right)^k > n \left(\prod_{k=0}^{n-1} \left(\left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y}{x}\right)^k\right)^{\frac{1}{n}} = n \left(\left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y}{x}\right)^{\frac{n-1}{2}}. \tag{3.12}$$

Par hypothèse, $ax^n \geq c_n$ donc

$$\left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y}{x} = \left(\frac{by^n}{ax^n}\right)^{\frac{1}{n}} = \left(1 - \frac{1}{ax^n}\right)^{\frac{1}{n}} \geq \left(1 - \frac{1}{c_n}\right)^{\frac{1}{n}} = \left(\frac{c_n - 1}{c_n}\right)^{\frac{1}{n}} \tag{3.13}$$

et il suit alors de (3.11), (3.12) et (3.13) que

$$\frac{1}{ax^n} > \left(1 - \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y}{x}\right) \times n \left[\left(\frac{c_n - 1}{c_n}\right)^{\frac{1}{n}}\right]^{\frac{n-1}{2}} = \left(1 - \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y}{x}\right) \frac{n}{s_n}$$

ce qui permet de conclure.

(ii) Comme $\mathrm{PGCD}(x_1, y_1) = \mathrm{PGCD}(x_2, y_2) = 1$, le fait que (x_1, y_1) diffère de (x_2, y_2) implique que $x_1 y_2 \neq x_2 y_1$. Dès lors, $|x_1 y_2 - x_2 y_1| \geq 1$. Or,

$$\begin{aligned}
|x_1 y_2 - x_2 y_1| &= x_1 x_2 \left|\frac{y_2}{x_2} - \frac{y_1}{x_1}\right| = x_1 x_2 \left|\frac{y_2}{x_2} - \left(\frac{a}{b}\right)^{\frac{1}{n}} + \left(\frac{a}{b}\right)^{\frac{1}{n}} - \frac{y_1}{x_1}\right| \\
&= x_1 x_2 \left(\frac{a}{b}\right)^{\frac{1}{n}} \left|\left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y_2}{x_2} - 1 + 1 - \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y_1}{x_1}\right| \\
&= x_1 x_2 \left(\frac{a}{b}\right)^{\frac{1}{n}} \left|\left(1 - \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y_1}{x_1}\right) - \left(1 - \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y_2}{x_2}\right)\right|
\end{aligned}$$

Or, les deux nombres $1-\left(\frac{b}{a}\right)^{\frac{1}{n}}\frac{y_1}{x_1}$ et $1-\left(\frac{b}{a}\right)^{\frac{1}{n}}\frac{y_2}{x_2}$ sont positifs (d'après (i)) donc

$$\begin{aligned}|x_1y_2-x_2y_1| &\leq x_1x_2\left(\frac{a}{b}\right)^{\frac{1}{n}}\max\left(1-\left(\frac{b}{a}\right)^{\frac{1}{n}}\frac{y_1}{x_1},1-\left(\frac{b}{a}\right)^{\frac{1}{n}}\frac{y_2}{x_2}\right)\\ &\leq x_1x_2\left(\frac{a}{b}\right)^{\frac{1}{n}}\max\left(\frac{s_n}{nax_1^n},\frac{s_n}{nax_2^n}\right)\quad\text{(d'après (i))}\\ &\leq x_1x_2\left(\frac{a}{b}\right)^{\frac{1}{n}}\frac{s_n}{nax_1^n}\quad(\text{car } ax_2^n\geq ax_1^n)\end{aligned}$$

En utilisant le fait que $|x_1y_2-x_2y_1|\geq 1$, on en déduit l'inégalité $\frac{nax_1^n}{s_n}\leq x_1x_2\left(\frac{a}{b}\right)^{\frac{1}{n}}$ et donc $\left(\frac{nax_1^n}{s_n}\right)^n\leq x_1^nx_2^n\frac{a}{b}$. De plus, $ab\geq 2$ donc $\frac{a}{b}\leq\frac{a^2}{2}$ et ainsi $\left(\frac{nax_1^n}{s_n}\right)^n\leq\frac{ax_1^nax_2^n}{2}$. Ceci permet de conclure que $2\left(\frac{n}{s_n}\right)^n(ax_1^n)^{n-1}\leq ax_2^n$. ■

3.4 Démonstration du théorème 3.1.1

On raisonne par l'absurde en supposant que l'équation (E_n) admet deux solutions distinctes (x_1,y_1) et (x_2,y_2) telles que $ax_2^n\geq ax_1^n\geq c_n$.

On définit alors, pour tout entier naturel $r\geq 1$, le nombre D_r par

$$D_r:=\frac{y_2}{x_2}A_r\left(\frac{by_1^n}{ax_1^n}\right)-\frac{y_1}{x_1}B_r\left(\frac{by_1^n}{ax_1^n}\right)$$

où A_r et B_r sont les polynômes définis en (3.1).

Le lemme suivant est une version plus faible du lemme 2.7 de [13] mais qui sera suffisante pour la suite.

Lemme 3.4.1. — *Le nombre D_r n'est pas nul dans les cas suivants :*
(i) $r=1$ et $n=3$ ou $n=4$;
(ii) $r\in\{2,3,4\}$ et $n=3$.

Preuve. — On pose dans toute la suite $z=\frac{b^{\frac{1}{n}}y_1}{a^{\frac{1}{n}}x_1}$ et $w=ax_1^n$ de sorte que $w-1=by_1^n$ et $z^n=\frac{w-1}{w}$. On va dans les différents cas raisonner par l'absurde.

(i) Commençons par le cas $r=1$ et $n=3$. Dans ce cas, $A_1(z^3)=\frac{9}{4}+\frac{9}{2}z^3$ et $B_1(z^3)=\frac{9}{2}+\frac{9}{4}z^3$. Ainsi, si $D_1=0$, $\frac{y_2}{x_2}\left(\frac{9}{4}+\frac{9}{2}z^3\right)=\frac{y_1}{x_1}\left(\frac{9}{2}+\frac{9}{4}z^3\right)$ et donc, en multipliant par $\frac{4}{9}x_1x_2w$, on obtient $x_1y_2(w+2(w-1))=x_2y_1(2w+(w-1))$ soit

$$x_1y_2(3w-2)=x_2y_1(3w-1),\tag{3.14}$$

cette égalité ne faisant apparaitre que des entiers. Comme x_1 et y_1 sont premiers entre eux, il s'ensuit x_1 divise $x_2(3w-1)$. Mais, comme x_1 divise w, x_1 est également premier avec $3w-1$ et ainsi x_1 divise x_2. Notons k l'entier tel que $x_2=kx_1$.

On a de la même façon, y_1 qui divise $y_2(3w-2)$ et y_1 divise $w-1$ donc y_1 est premier avec $3w-2$ ce qui assure que y_1 divise y_2 et qu'il existe un entier k' tel que $y_2=k'y_1$. Ainsi, on déduit de (3.14) que $k'(3w-2)=k(3w-1)$. Or, $3w-2$ et $3w-1$ sont premiers entre eux donc il existe un entier λ

tel que $k = \lambda(3w-2)$ et $k' = \lambda(3w-1)$. Il s'ensuit que $x_2 = \lambda(3w-2)x_1$ et $y_2 = \lambda(3w-1)y_1$. Mais, comme x_2 et y_2 sont premiers entre eux, $\lambda = 1$. On en déduit que

$$\begin{aligned} 1 &= ax_2^3 - by_2^3 = a((3w-2)x_1)^3 - b((3w-1)y_1)^3 = ax_1^3(3w-2)^3 - by_1^3(3w-1)^3 \\ &= w(3w-2)^3 - (w-1)(3w-1)^3 = 2w-1. \end{aligned}$$

Il s'ensuit que $w = 1$ ce qui est absurde car $w \geq c_3 > 1$ [(3)].

Considérons ensuite le cas $r = 1$ et $n = 4$. Dans ce cas, $A_1(z^4) = \frac{16}{5} + \frac{16}{3}z^4$ et $B_1(z^4) = \frac{16}{3} + \frac{16}{5}z^4$ et donc, si $D_1 = 0$, en multipliant par $\frac{15}{16}x_1x_2w$, il vient

$$x_1y_2(8w-5) = x_2y_1(8w-3). \tag{3.15}$$

Posons $L := 8w-5$ et $M := 8w-3$ de sorte que $x_1y_2L = x_2y_1M$. Comme précédemment, x_1 divise x_2M. Notons $d = \mathrm{PGCD}(x_1, M)$. Comme x_1 divise w, d divise 3 donc $d = 1$ ou $d = 3$. En écrivant $x_1 = dx_1'$ et $M = dM'$, on a donc que x_1' divise x_2M' et donc x_1' divise x_2. On note k l'entier tel que $x_2 = kx_1'$.

De même, en notant $d' = \mathrm{PGCD}(y_1, L)$, étant donné que $L = 8(1+by_1^4) - 5 = 8by_1^3 + 3$, d' divise 3 donc $d' = 1$ ou $d' = 3$ [(4)]. En écrivant $y_1 = d'y_1'$ et $L = d'L'$, on en déduit qu'il existe un entier k' tel que $y_2 = k'y_1'$.

Considérons $\delta = \mathrm{PGCD}(L, M)$. Alors, δ divise $M - L = 2$ et L est impair donc $\delta = 1$. D'après (3.15), $dx_1'k'y_1'L = kx_1'd'y_1'M$ donc $dk'L = d'kM$ et comme L et M sont premiers entre eux, il existe un entier λ tel que $d'k = \lambda L$ et $dk' = \lambda M$. Mais alors $dd'x_2 = dd'kx_1' = (d'k)(dx_1') = \lambda Lx_1$ et $dd'y_2 = dd'k'y_1' = (dk')(d'x_1') = \lambda My_1$. Comme x_2 et y_2 sont premiers entre eux, ceci implique que λ divise dd'. On a, de plus,

$$\begin{aligned} (dd')^4 &= (dd')^4(ax_2^4 - by_2^4) = a(dd'x_2)^4 - b(dd'y_2)^4 = a(\lambda Lx_1)^4 - b(\lambda My_1)^4 \\ &= \lambda^4(ax_1^4L^4 - by_1^4M^4) = \lambda^4(wL^4 - (w-1)M^4) \\ &= \lambda^4(320w^2 - 320w + 81) \end{aligned}$$

Ainsi, w est solution de l'équation $320x^2 - 320x + 81 = \left(\frac{dd'}{\lambda}\right)^4$ où $\frac{dd'}{\lambda} \in \{1, 3\}$. Or, on vérifie que l'équation $320x^2 - 320x + 81 = t$ avec $t \in \{1, 81\}$ n'a de solution entière que si $t = 81$ et alors ces solutions sont 0 et 1 ce qui conduit à une absurdité car $w \geq c_4 > 1$.

(ii) On va, dans ces trois cas, utiliser un raisonnement similaire au précédent à cette différence près que les facteurs L et M ne sont plus nécessairement premiers entre eux. Cependant, une application attentive de la proposition 2.1.7 permet de déterminer une combinaison linéaire de L et M indépendante de w. Plus précisément, si L_r et M_r sont les polynômes en w correspondant à r alors $L_rM_{r+1} - L_{r+1}M_r$ est une constante.

Si $r = 2$ et $n = 3$, $D_2 = \frac{y_2}{x_2}\left(\frac{27}{14} + \frac{27}{2}z^3 + \frac{27}{5}z^6\right) - \frac{y_1}{x_1}\left(\frac{27}{5} + \frac{27}{2}z^3 + \frac{27}{14}z^6\right)$ donc, si $D_2 = 0$, on obtient, en multipliant par $\frac{70}{27}x_1x_2w^2$,

$$x_1y_2(54w^2 - 63w + 14) = x_2y_1(54w^2 - 45w + 5). \tag{3.16}$$

Avec les mêmes notations que précédemment, $L = 54w^2 - 63w + 14$ et $M = 54w^2 - 45w + 5$, $d = \mathrm{PGCD}(x_1, M)$ divise 5 donc $d = 1$ ou $d = 5$.

De même, en notant $d' = \mathrm{PGCD}(y_1, L)$, sachant que $L = 54(by_1^3)^2 + 45by_1^3 + 5$, d' divise 5 donc $d' = 1$ ou $d' = 5$.

On considère $\delta = \mathrm{PGCD}(L, M)$. Alors, étant donné que $(3w-2)M - (3w-1)L = 4$, δ divise 4 i.e. $\delta \in \{1, 2, 4\}$. Ecrivons $L = \delta L''$ et $M = \delta M''$. Alors, on déduit de (3.16) que $dx_1'k'y_1'\delta L'' = kx_1'd'y_1'\delta M''$

(3). On peut en fait même conclure sans cette hypothèse.

(4). On peut remarquer que x_1 et y_1 étant premiers entre eux, d et d' ne peuvent pas être tous les deux égaux à 3.

donc $dk'L'' = d'kM''$. Il s'ensuit qu'il existe un entier λ tel que $d'k = \lambda L''$ et $dk' = \lambda M''$. Mais alors $dd'x_2 = dd'kx_1' = (d'k)(dx_1') = \lambda L''x_1$ et $dd'y_2 = dd'k'y_1' = (dk')(d'x_1') = \lambda M''y_1$. Comme x_2 et y_2 sont premiers entre eux, ceci implique que λ divise dd'. On a, de plus,

$$\begin{aligned}(\delta dd')^3 &= (\delta dd')^3(ax_2^3 - by_2^3) = a(\delta dd'x_2)^3 - b(\delta dd'y_2)^3 = a(\delta\lambda L''x_1)^3 - b(\delta\lambda M''y_1)^3\\ &= \lambda^3(ax_1^3L^3 - by_1^3M^3) = \lambda^3(wL^3 - (w-1)M^3)\\ &= \lambda^3(756w^2 - 756w + 125)\end{aligned}$$

Ainsi, w est solution de l'équation $756x^2 - 756x + 125 = \delta^3\left(\frac{dd'}{\lambda}\right)^3$ où $\delta \in \{1, 2, 4\}$ et $\frac{dd'}{\lambda} \in \{1, 5\}$. Or, on vérifie que l'équation $756x^2 - 756x + 125 = t$ n'a de solution entière pour $t \in \{1, 8, 64, 125, 1000, 8000\}$ que si $t = 125$ et alors $x \in \{0, 1\}$. Ceci est absurde car $w \geq c_3$.

Si $r = 3$ et $n = 3$, avec les mêmes notations, on trouve

$$A_3(z^3) = \frac{243}{140} + \frac{729}{28}z^3 + \frac{729}{20}z^6 + \frac{243}{40}z^9 \quad \text{et} \quad B_3(z^3) = \frac{243}{40} + \frac{729}{20}z^3 + \frac{729}{28}z^6 + \frac{243}{140}z^9$$

ce qui donne, si $D_3 = 0$, $x_1y_2L = x_2y_1M$ avec $L = 81w^3 - 135w^2 + 63w - 7$ et $M = 81w^3 - 108w^2 + 36w - 2$. On en déduit que d et d' divise 2.

Etant donné que $(54w^2 - 63w + 14)M - (54w^2 - 45w + 5)L = 7$, $\delta \in \{1, 7\}$. Par ailleurs, on a

$$(\delta dd')^3 = \lambda^3(ax_1^3L^3 - by_1^3M^3) = \lambda^3(wL^3 - (w-1)M^3) = \lambda^3(162w^3 - 243w^2 + 97w - 8)$$

donc w est solution de $162x^3 - 243x^2 + 97x - 8 = t$ avec $t \in \{1, 8, 343, 2744\}$. On vérifie que cette équation n'a de solution entière que si $t = 8$ et alors $x = 1$ ce qui conduit à une absurdité car $w \geq c_3$.

Enfin, si $r = 4$ et $n = 3$, on a

$$A_4(z^3) = \frac{729}{455} + \frac{1\,458}{35}z^3 + \frac{4\,374}{35}z^6 + \frac{729}{10}z^9 + \frac{729}{110}z^12 \text{ et } B_4(z^3) = \frac{729}{110} + \frac{729}{10}z^3 + \frac{4\,374}{35}z^6 + \frac{1\,458}{35}z^9 + \frac{729}{455}z^{12}$$

donc, si $D_4 = 0$, $x_1y_2L = x_2y_1M$ avec

$$L = 3\,402w^4 - 7\,371w^3 + 5\,265w^2 - 1\,365w + 91 \text{ et } M = 3\,402w^4 - 6\,237w^3 + 3\,564w^2 - 660w + 22.$$

On en déduit que d et d' divise 22.

Etant donné que $(81w^3 - 135w^2 + 63w - 7)M - (81w^3 - 108w^2 + 36w - 2)L = 28$, $\delta \in \{1, 2, 4, 7, 14, 28\}$. Par ailleurs, on a

$$\begin{aligned}(\delta dd')^3 = \lambda^3(ax_1^3L^3 - by_1^3M^3) &= \lambda^3(wL^3 - (w-1)M^3)\\ &= \lambda^3(756\,756w^4 - 1\,513\,512w^3 + 972\,153w^2 - 215\,397w + 10\,648)\end{aligned}$$

donc w est solution de $756\,756x^4 - 1\,513\,512x^3 + 972\,153x^2 - 215\,397x + 10\,648 = t$ avec

$$t \in \{1, 8, 64, 343, 512, 1\,331, 2\,744, 10\,648, 21\,952, 85\,184, 175\,616, 456\,533, 3\,652\,264, 29\,218\,112\}.$$

On vérifie que cette équation n'a de solutions entières que si $t = 10\,648$ et alors les solutions entières sont 0 et 1 ce qui contredit l'hypothèse $w \geq c_3$. ■

On définit pour tout entier $r \geq 1$, les nombres

$$P_r := \frac{\binom{2r}{r} n^r \mathrm{PGCD}(n^r, r!) s_n (ax_1^n)^{r+\frac{1}{n}}}{n 2^{\frac{1}{n}} (ax_2^n)^{1-\frac{1}{n}}} \quad \text{et} \quad Q_r := \frac{\delta_r s_n^{2r+1} (ax_2^n)^{\frac{1}{n}} r!^2}{2^{\frac{1}{n}} (ax_1^n)^{r+1-\frac{1}{n}} (2r+1)!} \tag{3.17}$$

où δ_r et s_n sont définis respectivement en (3.4) et (3.10).

Lemme 3.4.2. — *Si $D_r \neq 0$ alors $P_r + Q_r > 1$.*

Preuve. — Comme $A_r(z)$ et $B_r(z)$ sont de degré r, d'après la proposition 3.2.3, $\delta_r x_1 x_2 (a x_1^n)^r D_r$ est un entier relatif. Si $D_r \neq 0$, on en déduit que

$$1 \leq \delta_r x_1 x_2 (a x_1^n)^r \left| D_r \right|. \tag{3.18}$$

Or,

$$|D_r| = \left| \frac{y_2}{x_2} A_r\left(\frac{b y_1^n}{a x_1^n}\right) - \frac{y_1}{x_1} B_r\left(\frac{b y_1^n}{a x_1^n}\right) \right| = \left(\frac{a}{b}\right)^{\frac{1}{n}} \left| \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y_2}{x_2} A_r\left(\frac{b y_1^n}{a x_1^n}\right) - \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y_1}{x_1} B_r\left(\frac{b y_1^n}{a x_1^n}\right) \right|$$

donc, d'après le lemme 3.2.1,

$$\begin{aligned}
\delta_r |D_r| &= \left(\frac{a}{b}\right)^{\frac{1}{n}} \left| \left(\left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y_2}{x_2} - 1 \right) \delta_r A_r\left(\frac{b y_1^n}{a x_1^n}\right) + \left(1 - \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y_1}{x_1}\right)^{2r+1} \delta_r V_r\left(\left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y_1}{x_1} \right) \right| \\
&\leq \left(\frac{a}{b}\right)^{\frac{1}{n}} \left[\left(1 - \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y_2}{x_2}\right) \delta_r A_r\left(\frac{b y_1^n}{a x_1^n}\right) + \left(1 - \left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y_1}{x_1}\right)^{2r+1} \delta_r V_r\left(\left(\frac{b}{a}\right)^{\frac{1}{n}} \frac{y_1}{x_1} \right) \right].
\end{aligned}$$

On déduit alors des lemmes 3.2.5 et 3.3.3 (i) que

$$\delta_r |D_r| < \left(\frac{a}{b}\right)^{\frac{1}{n}} \left(\frac{s_n}{n a x_2^n} \binom{2r}{r} n^r \mathrm{PGCD}(n^r, r!) + \delta_r \left(\frac{s_n}{n a x_1^n}\right)^{2r+1} n^{2r+1} \frac{r!^2}{(2r+1)!} \right). \tag{3.19}$$

Ainsi, d'après (3.18) et (3.19),

$$1 < x_1 x_2 (a x_1^n)^r \left(\frac{a}{b}\right)^{\frac{1}{n}} \left(\frac{\binom{2r}{r} n^r \mathrm{PGCD}(n^r, r!) s_n}{n a x_2^n} + \delta_r \left(\frac{s_n}{a x_1^n}\right)^{2r+1} \frac{r!^2}{(2r+1)!} \right). \tag{3.20}$$

Or, en tenant compte du fait que $ab \geq 2$,

$$x_1 x_2 (a x_1^n)^r \left(\frac{a}{b}\right)^{\frac{1}{n}} = \frac{(a x_1^n)^{\frac{1}{n}} (a x_2^n)^{\frac{1}{n}}}{a^{\frac{2}{n}}} (a x_1^n)^r \left(\frac{a}{b}\right)^{\frac{1}{n}} = (a x_1^n)^{\frac{1}{n}+r} (a x_2^n)^{\frac{1}{n}} \left(\frac{1}{ab}\right)^{\frac{1}{n}} \leq (a x_1^n)^{\frac{1}{n}+r} (a x_2^n)^{\frac{1}{n}} \frac{1}{2^{\frac{1}{n}}}$$

donc, d'après (3.20),

$$\begin{aligned}
1 &< (a x_1^n)^{\frac{1}{n}+r} (a x_2^n)^{\frac{1}{n}} \frac{1}{2^{\frac{1}{n}}} \left(\frac{\binom{2r}{r} n^r \mathrm{PGCD}(n^r, r!) s_n}{n a x_2^n} + \frac{\delta_r s_n^{2r+1} r!^2}{(a x_1^n)^{2r+1} (2r+1)!} \right) \\
&= \frac{\binom{2r}{r} n^r \mathrm{PGCD}(n^r, r!) s_n (a x_1^n)^{\frac{1}{n}+r}}{n 2^{\frac{1}{n}} (a x_2^n)^{1-\frac{1}{n}}} + \frac{\delta_r s_n^{2r+1} (a x_2^n)^{\frac{1}{n}} r!^2}{2^{\frac{1}{n}} (a x_1^n)^{r+1-\frac{1}{n}} (2r+1)!} \\
&= P_r + Q_r
\end{aligned}$$

qui est bien le résultat annoncé. ∎

Dans la suite, on suit l'idée d'Evertse qui consiste à aboutir à une absurdité en montrant qu'il existe un entier k tel que $D_k \neq 0$ (et donc $P_k + Q_k > 1$) avec dans le même temps $P_k \leq \frac{1}{n}$ et $Q_k \leq 1 - \frac{1}{n}$.

Le lemme suivant est une amélioration du lemme 2.9 de [13].

Lemme 3.4.3. — *Soit (u_r) la suite définie, pour tout $r \geq 1$, par*

$$u_r = \frac{\binom{2r}{r} n^r \mathrm{PGCD}(n^r, r!) s_n}{2^{\frac{1}{n}}} (a x_1^n)^r.$$

Il existe un entier $t \geq \left\lfloor \frac{n-1}{2} \right\rfloor$ tel que

$$u_t \leq \frac{(a x_2^n)^{1-\frac{1}{n}}}{(a x_1^n)^{\frac{1}{n}}} < u_{t+1}.$$

Preuve. — Pour tout $r \geq 1$, $u_r > 0$ et

$$\frac{u_{r+1}}{u_r} = 2n \frac{2r+1}{r+1} \frac{\mathrm{PGCD}(n^{r+1}, (r+1)!)}{\mathrm{PGCD}(n^r, r!)} a x_1^n \geq 2na x_1^n > 1$$

donc (u_r) tend en croissant vers $+\infty$. Il suffit donc de montrer que $u_\ell \leq \frac{(a x_2^n)^{1-\frac{1}{n}}}{(a x_1^n)^{\frac{1}{n}}}$ où $\ell = \left\lfloor \frac{n-1}{2} \right\rfloor$.

Raisonnons par l'absurde en supposant que $u_\ell > \frac{(a x_2^n)^{1-\frac{1}{n}}}{(a x_1^n)^{\frac{1}{n}}}$ i.e.

$$\frac{(a x_2^n)^{1-\frac{1}{n}}}{(a x_1^n)^{\frac{1}{n}}} < \frac{\binom{2\ell}{\ell} n^\ell \mathrm{PGCD}(n^\ell, \ell!) s_n}{2^{\frac{1}{n}}} (a x_1^n)^\ell.$$

Alors,

$$a x_2^n < \left(\frac{\binom{2\ell}{\ell} n^\ell \mathrm{PGCD}(n^\ell, \ell!) s_n}{2^{\frac{1}{n}}} \right)^{\frac{n}{n-1}} (a x_1^n)^{\frac{n\ell+1}{n-1}}$$

donc, d'après le lemme 3.3.3 (ii),

$$2 \left(\frac{n}{s_n} \right)^n (a x_1^n)^{n-1} < \left(\frac{\binom{2\ell}{\ell} n^\ell \mathrm{PGCD}(n^\ell, \ell!) s_n}{2^{\frac{1}{n}}} \right)^{\frac{n}{n-1}} (a x_1^n)^{\frac{n\ell+1}{n-1}}$$

i.e. en élevant à la puissance $n-1$,

$$(a x_1^n)^{n(n-2-\ell)} < \frac{1}{2^n} \binom{2\ell}{\ell}^n s_n^{n^2} n^{-n(n-1)} \left(n^\ell \mathrm{PGCD}(n^\ell, \ell!) \right)^n.$$

Or, comme $\ell \leq \frac{n-1}{2}$, $n(n-2-\ell) \geq n\left(n-2-\frac{n-1}{2}\right) = \frac{n(n-3)}{2} \geq 0$ donc, sachant que $a x_1^n \geq c_n$,

$$c_n^{\frac{n(n-3)}{2}} \leq (a x_1^n)^{n(n-2-\ell)} < \frac{1}{2^n} \binom{2\ell}{\ell}^n s_n^{n^2} n^{-n(n-1)} \left(n^\ell \mathrm{PGCD}(n^\ell, \ell!) \right)^n. \tag{3.21}$$

En utilisant les majorations $\binom{2\ell}{\ell} \leq 4^\ell \leq 2^{n-1}$ et $n^\ell \mathrm{PGCD}(n^\ell, \ell!) \leq n^{2\ell} \leq n^{n-1}$ ainsi que le lemme 3.3.1 qui assure que $c_n \geq 7$ et qui implique donc que

$$s_n^{n^2} = \left(\frac{c_n}{c_n - 1} \right)^{\frac{n(n-1)}{2}} \leq \left(\frac{7}{6} \right)^{\frac{n(n-1)}{2}},$$

on déduit alors de (3.21) que

$$7^{\frac{n(n-3)}{2}} \leq 2^{n(n-2)} \left(\frac{7}{6} \right)^{\frac{n(n-1)}{2}} \quad i.e. \quad 3^{n-1} < 7^2 . 2^{n-3}.$$

Il s'ensuit que

$$n < \frac{\ln \frac{147}{8}}{\ln \frac{3}{2}} < 8$$

donc $n \leq 7$. Or, on vérifie que si $n \in \{3,4,5,6,7\}$ alors le terme de droite dans l'inégalité (3.21) est inférieur strictement à 1 (le maximum étant atteint pour $n = 3$ et valant environ 0,01) ce qui est absurde car $c_n^{\frac{n(n-3)}{2}} \geq 1$. ■

On note t l'entier défini par le lemme précédent et on considère l'entier k défini de la manière suivante : si $D_t \neq 0$, on pose $k = t$ et si $D_t = 0$, on pose $k = t - 1$. Le lemme 3.4.1 (i) et le fait que $t \geq \lfloor \frac{n-1}{2} \rfloor$ assure que $k \geq 1$.

Remarquons que $D_k \neq 0$. En effet, si $D_t = D_{t-1} = 0$ alors, en posant $z_1 = \frac{y_1}{x_1}$ et $z_2 = \frac{y_2}{x_2}$, on aurait

$$z_1 B_t\left(\frac{b}{a} z_1^n\right) = z_2 A_t\left(\frac{b}{a} z_1^n\right) \quad \text{et} \quad z_1 B_{t-1}\left(\frac{b}{a} z_1^n\right) = z_2 A_{t-1}\left(\frac{b}{a} z_1^n\right)$$

et donc

$$z_1 z_2 A_t\left(\frac{b}{a} z_1^n\right) B_{t-1}\left(\frac{b}{a} z_1^n\right) = z_1 z_2 B_t\left(\frac{b}{a} z_1^n\right) A_{t-1}\left(\frac{b}{a} z_1^n\right).$$

Comme $z_1 z_2 \neq 0$, il s'ensuivrait que

$$A_t\left(\frac{b}{a} z_1^n\right) B_{t-1}\left(\frac{b}{a} z_1^n\right) = B_t\left(\frac{b}{a} z_1^n\right) A_{t-1}\left(\frac{b}{a} z_1^n\right).$$

En posant $z_0 = 1 - \frac{b}{a} z_1^n \neq 0$, on a donc $A_t(1-z_0)[-B_{t-1}(1-z_0)] = [-B_t(1-z_0)]A_{t-1}(1-z_0)$ ce qui rentre en contradiction avec la proposition 2.1.7 car, par définition, les polynômes $A_t(1-z)$ et $-B_t(1-z)$ forment une famille de $[t,t]$ approximants de Padé de la fonction $f : z \mapsto (1-z)^{\frac{1}{n}}$, $-B_t(1) \neq 0$ et l'ordre de la fonction reste est $2t+1$ car le système $(1, f)$ est normal d'après la proposition 2.2.2. Ainsi, $D_k \neq 0$.

D'autre part, en reprenant les notations du lemme 3.4.3, la suite (u_r) est croissante donc $u_k \leq u_t$ et ainsi

$$P_k = \frac{u_k}{n} \times \frac{(ax_1^n)^{\frac{1}{n}}}{(ax_2^n)^{1-\frac{1}{n}}} \leq \frac{u_t}{n} \times \frac{(ax_1^n)^{\frac{1}{n}}}{(ax_2^n)^{1-\frac{1}{n}}} \leq \frac{1}{n}$$

par définition de u_t.

Reste donc à montrer que $Q_k \leq 1 - \frac{1}{n}$. Pour cela, on note, dans toute la suite de ce chapitre, $\varepsilon = t - k \in \{0,1\}$ de sorte que $t = k + \varepsilon$. On remarquera que, d'après le lemme 3.4.1, $\varepsilon = 0$ si $n = 3$ et $t \in \{1,2,3,4\}$ ainsi que si $n = 4$ et $t = 1$. On va en fait plutôt considérer Q_k^{n-1} afin de pouvoir utiliser l'inégalité de droite du lemme 3.4.3. En effet, cette dernière assure que

$$(ax_2^n)^{\frac{n-1}{n}} < u_{k+\varepsilon+1}(ax_1^n)^{\frac{1}{n}}$$

donc

$$Q_k^{n-1} = \left[\frac{\delta_k s_n^{2k+1} k!^2}{2^{\frac{1}{n}}(2k+1)!}\right]^{n-1} (ax_1^n)^{-(n-1)\left(k+1-\frac{1}{n}\right)} (ax_2^n)^{\frac{n-1}{n}} < \left[\frac{\delta_k s_n^{2k+1} k!^2}{2^{\frac{1}{n}}(2k+1)!}\right]^{n-1} u_{k+\varepsilon+1}(ax_1^n)^{1-(n-1)(k+1)}$$

et donc, étant donné que $[k+\varepsilon+1] + [1-(n-1)(k+1)] = (2-n)(k+1) + 1 + \varepsilon \leq 0$ et $ax_1^n \geq c_n$,

$$Q_k^{n-1} < \left[\frac{\delta_k s_n^{2k+1} k!^2}{2^{\frac{1}{n}}(2k+1)!}\right]^{n-1} \frac{\binom{2k+2\varepsilon+2}{k+\varepsilon+1} n^{k+\varepsilon+1} \mathrm{PGCD}(n^{k+\varepsilon+1}, (k+\varepsilon+1)!) s_n}{2^{\frac{1}{n}}} c_n^{(2-n)(k+1)+1+\varepsilon}. \quad (3.22)$$

Posons, pour tout entier $r \geq 1$,

$$E_n(r,\varepsilon) = \left[\frac{\delta_r s_n^{2r+1} r!^2}{2^{\frac{1}{n}}(2r+1)!}\right]^{n-1} \frac{\binom{2r+2\varepsilon+2}{r+\varepsilon+1} n^{r+\varepsilon+1}\mathrm{PGCD}(n^{r+\varepsilon+1},(r+\varepsilon+1)!)s_n}{2^{\frac{1}{n}}}.$$

On va montrer qu'on peut majorer $E_n(r,\varepsilon)$ à l'aide de α_n et t_n. Plus précisément, on a le résultat suivant.

Lemme 3.4.4. — *Quelle que soit la valeur de l'entier $r \geq 1$, $E_n(r,\varepsilon) \leq (\alpha_n t_n)^{nr+\varepsilon+1}$.*

Preuve. — On sait, d'après le lemme 3.3.2 que, pour tout entier $m \geq 1$, $n^m\mathrm{PGCD}(n^m, m!) \leq t_n^m$. Dès lors, par définition de δ_r ((3.4)),

$$\begin{aligned}
E_n(r,\varepsilon) &= \left[\frac{(r+1)\binom{r+\frac{1}{n}}{r+1}\binom{r-\frac{1}{n}}{r} n^r \mathrm{PGCD}(n^r, r!) s_n^{2r+1} r!^2}{2^{\frac{1}{n}}(2r+1)!}\right]^{n-1} \frac{\binom{2r+2\varepsilon+2}{r+\varepsilon+1} n^{r+\varepsilon+1}\mathrm{PGCD}(n^{r+\varepsilon+1},(r+\varepsilon+1)!)s_n}{2^{\frac{1}{n}}} \\
&\leq \left[\frac{(r+1)\binom{r+\frac{1}{n}}{r+1}\binom{r-\frac{1}{n}}{r} s_n^{2r+1} r!^2}{2^{\frac{1}{n}}(2r+1)!}\right]^{n-1} \frac{\binom{2r+2\varepsilon+2}{r+\varepsilon+1} s_n}{2^{\frac{1}{n}}} t_n^{r(n-1)+r+\varepsilon+1} \\
&\leq \frac{s_n}{2}\left[\frac{\binom{r+\frac{1}{n}}{r+1}\binom{r-\frac{1}{n}}{r} s_n^{2r+1}}{\binom{2r+1}{r}}\right]^{n-1} \binom{2r+2\varepsilon+2}{r+\varepsilon+1} t_n^{nr+\varepsilon+1}.
\end{aligned}$$

Il suffit donc de montrer que, pour tout $r \geq 1$,

$$\varphi_n(r,\varepsilon) := \frac{s_n}{2}\left[\frac{\binom{r+\frac{1}{n}}{r+1}\binom{r-\frac{1}{n}}{r} s_n^{2r+1}}{\binom{2r+1}{r}}\right]^{n-1} \binom{2r+2\varepsilon+2}{r+\varepsilon+1} \leq \alpha_n^{nr+\varepsilon+1}.$$

Or, pour tout $r \geq 1$,

$$\frac{\varphi_n(r+1,\varepsilon)}{\varphi_n(r,\varepsilon)} = \frac{4(r+\varepsilon)+6}{r+\varepsilon+2}\left[\frac{(r+1)^2 - \frac{1}{n^2}}{(r+1)(4r+6)} s_n^2\right]^{n-1} \leq 4\left(\frac{s_n^2}{4}\right)^{n-1}$$

donc

$$\varphi_n(r,\varepsilon) \leq \left[4\left(\frac{s_n^2}{4}\right)^{(n-1)}\right]^{r-1} \varphi_n(1,\varepsilon) = \left[4\left(\frac{s_n^2}{4}\right)^{(n-1)}\right]^{r-1} \frac{s_n}{2}\binom{4+2\varepsilon}{2+\varepsilon}\left(\frac{n^2-1}{6n^3}s_n^3\right)^{n-1}.$$

Posons $\gamma_n := \left[4\left(\frac{s_n^2}{4}\right)^{n-1}\right]^{\frac{1}{n}}$. On va montrer que $\varphi_n(r,\varepsilon) \leq \gamma_n^{nr+\varepsilon+1}$. Pour cela, il suffit de montrer que $\frac{s_n}{2}\binom{4+2\varepsilon}{2+\varepsilon}\left(\frac{n^2-1}{6n^3}s_n^3\right)^{n-1} \leq \gamma_n^{n+\varepsilon+1}$. Dans cette inégalité, le terme de gauche est croissant en ε alors que celui de droite est décroissant (car $\gamma_n < 1$ puisque $s_n \leq \frac{7}{6}$) donc il suffit de prouver que $\frac{s_n}{2}\binom{6}{3}\left(\frac{n^2-1}{6n^3}s_n^3\right)^{n-1} \leq \gamma_n^{n+2}$. C'est bien le cas pour $n = 3$ ($0{,}03 < 0{,}1$) ainsi que pour $n = 4$ ($7{,}5.10^{-4} < 1{,}9.10^{-2}$). Supposons $n \geq 5$. Alors, en utilisant l'inégalité $\frac{n^2-1}{6n^3} \leq \frac{4}{125}$, il vient

$$\frac{s_n}{2}\binom{6}{3}\left(\frac{n^2-1}{6n^3}s_n^3\right)^{n-1} \leq 10\left(\frac{4}{125}\right)^{n-1} s_n^{3n-2} < \left(\frac{1}{4}\right)^{2n-2} s_n^{3n-2}.$$

Par ailleurs, étant donné que $4\left(\frac{s_n^2}{4}\right)^{n-1} < 1$ et $\frac{n+2}{n} \leq \frac{5}{3}$,

$$\gamma_n^{n+2} = \left[4\left(\frac{s_n^2}{4}\right)^{n-1}\right]^{\frac{n+2}{n}} \geq \left[4\left(\frac{s_n^2}{4}\right)^{n-1}\right]^{\frac{5}{3}} = \left(\frac{1}{4}\right)^{\frac{5}{3}n-\frac{10}{3}} s_n^{\frac{10}{3}n-\frac{10}{3}}.$$

Or, pour $n \geq 5$, $2n-2 \geq \frac{5}{3}n - \frac{10}{3}$ et $3n-2 \leq \frac{10}{3}n - \frac{10}{3}$ donc

$$\gamma_n^{n+2} \geq \left(\frac{1}{4}\right)^{2n-2} s_n^{3n-2} > \frac{s_n}{2}\binom{6}{3}\left(\frac{n^2-1}{6n^3}s_n^3\right)^{n-1}.$$

Ainsi, quelle que soit la valeur de n, on a $\varphi_n(r,\varepsilon) \leq \gamma_n^{nr+\varepsilon+1}$.

Montrons, pour terminer, que $\gamma_n \leq \alpha_n$.

Pour $n = 4$ ou n un nombre premier entre 3 et 643, les valeurs de γ_n (arrondies par excès) sont données dans le tableau suivant.

n	γ_n
3	0,63761
4	0,517192
5	0,472992
7	0,41584
11	0,36338
13	0,3485
17	0,32841
19	0,32127
23	0,31038
29	0,29922
31	0,296391
37	0,28959
41	0,28608
43	0,28456
47	0,28186
53	0,27854
59	0,27585
61	0,27507
67	0,27298
71	0,27177
73	0,27121
79	0,269696
83	0,26880
89	0,26761

n	γ_n
97	0,26623
101	0,26563
103	0,26554
107	0,264793
109	0,26454
113	0,26405
127	0,26257
131	0,2621995
137	0,26169
139	0,26153
149	0,26079
151	0,26065
157	0,26026
163	0,259893
167	0,25967
173	0,25935
179	0,25904
181	0,25895
191	0,258491
193	0,25841
197	0,25824
199	0,25816
211	0,25771
223	0,25731

n	γ_n
227	0,25719
229	0,25713
233	0,25701
239	0,25684
241	0,25678
251	0,25652
257	0,25637
263	0,25623
269	0,256091
271	0,25605
277	0,25592
281	0,25584
283	0,255797
293	0,25661
307	0,25536
311	0,25529
313	0,25526
317	0,25519
331	0,25498
337	0,25489
347	0,25475
349	0,25473
353	0,25468
359	0,254595

n	γ_n
367	0,254497
373	0,25443
379	0,25436
383	0,25432
389	0,25425
397	0,25417
401	0,25413
409	0,25405
419	0,25395
421	0,25393
431	0,25385
433	0,25383
439	0,25378
443	0,25374
449	0,25369
457	0,25363
461	0,253596
463	0,25359
467	0,25355
479	0,25347
487	0,25341
491	0,25338
499	0,25333
503	0,2532994

n	γ_n
509	0,25327
521	0,25319
523	0,25318
541	0,25308
547	0,25304
557	0,25299
563	0,25296
569	0,25293
571	0,25292
577	0,25289
587	0,25284
593	0,25281
599	0,25278
601	0,25277
607	0,25275
613	0,25272
617	0,252699
619	0,25269
631	0,25264
641	0,252599
643	0,252591

Tableau 3.3 : Les valeurs de γ_n arrondies par excès pour $n = 4$ ou n premier inférieur à 643

En comparant avec les valeurs de α_n données par le tableau 3.1 p.48, on vérifie que $\gamma_n \leq \alpha_n$ dans chacun de ces cas.

Si n est un nombre premier supérieur à 647 alors d'après le lemme 3.3.1, $c_n \geq 167$ donc, $s_n = \left(\frac{c_n}{c_n-1}\right)^{\frac{n-1}{2n}} \leq \left(\frac{167}{166}\right)^{\frac{n-1}{2n}} \leq \left(\frac{167}{166}\right)^{\frac{1}{2}}$. Comme, à n fixé, la fonction $x \mapsto \left[4\left(\frac{x^2}{4}\right)^{n-1}\right]^{\frac{1}{n}}$ est croissante sur $\mathbb{R}_+$, $\gamma_n \leq \left[4\left(\frac{167}{664}\right)^{n-1}\right]^{\frac{1}{n}}$. De plus, la suite $n \mapsto \left[4\left(\frac{167}{664}\right)^{n-1}\right]^{\frac{1}{n}}$ est décroissante donc

$\gamma_n \leq \left[4\left(\frac{167}{664}\right)^{646}\right]^{\frac{1}{647}}$. Etant donné que $\left[4\left(\frac{167}{664}\right)^{646}\right]^{\frac{1}{647}} \approx 0{,}252584$ et $\alpha_n = 0{,}2526$, on conclut que $\gamma_n \leq \alpha_n$.

Enfin, supposons qu'on ne soit pas dans l'un des cas précédent. Alors, en particulier, $n \geq 6$ et $c_n \geq 7$ donc

$$\gamma_n^{\frac{n+1}{n-1}} = \left[4\left(\frac{s_n^2}{4}\right)^{n-1}\right]^{\frac{n+1}{n(n-1)}} = 4^{\frac{-n^2+n+2}{n(n-1)}}\left(\frac{c_n}{c_n-1}\right)^{1-\frac{1}{n^2}} \leq 4^{\frac{-n^2+n+2}{n(n-1)}} \times \frac{7}{6}.$$

Or, $v : n \mapsto 4^{\frac{-n^2+n+2}{n(n-1)}}$ est décroissante donc $v(n) \leq v(6) = 4^{-\frac{14}{15}}$ et ainsi

$$\gamma_n^{\frac{n+1}{n-1}} \leq 4^{-\frac{14}{15}} \times \frac{7}{6} \leq \frac{1}{3}.$$

On conclut que $\gamma_n \leq \left(\frac{1}{3}\right)^{\frac{n-1}{n+1}} = \alpha_n$ et on a donc montré que, dans tous les cas,

$$E_n(r,\varepsilon) \leq \varphi_n(r,\varepsilon) t_n^{nr+\varepsilon+1} \leq \gamma_n^{nr+\varepsilon+1} t_n^{nr+\varepsilon+1} \leq \alpha_n^{nr+\varepsilon+1} t_n^{nr+\varepsilon+1} = (\alpha_n t_n)^{nr+\varepsilon+1}$$

ce qui était le résultat annoncé. ■

La proposition suivante permettra de terminer la démonstration.

Proposition 3.4.5. — *Quelles que soient les valeurs de k et ε,*

$$E_n(k,\varepsilon) c_n^{(2-n)(k+1)+1+\varepsilon} \leq \left(1-\frac{1}{n}\right)^{n-1}.$$

Preuve. — Commençons par traiter le cas $n = 3$. Il faut alors montrer que

$$E_3(k,\varepsilon) c_3^{-k+\varepsilon} \leq \frac{4}{9}.$$

Si $t \in \{1,2,3,4\}$ alors $k = t$, $\varepsilon = 0$ et

$$E_3(1,0)c_3^{-1} \approx 1{,}7.10^{-2}, \quad E_3(2,0)c_3^{-2} \approx 4{,}8.10^{-3}, \quad E_3(3,0)c_3^{-3} \approx 5{,}1.10^{-3} \text{et} \quad E_3(4,0)c_3^{-4} \approx 6{,}7.10^{-4}$$

donc la proposition est vérifiée dans ces cas-là. Etant donné que $\varepsilon \mapsto E_n(k,\varepsilon)c_3^{-k+\varepsilon}$ est croissante (car $c_3 \geq 1$), il suffit pour les valeurs supérieures de k de démontrer la proposition pour $\varepsilon = 1$. On le vérifie numériquement pour $k \in [\![5, 259]\!]$, le maximum étant $E_3(9,1) \approx 0{,}441$. De plus, si $k \geq 260$, d'après le lemme 3.4.4 et par définition de c_3,

$$E_3(k,1)c_3^{-k+1} \leq (\alpha_3 t_3)^{3k+2}(\alpha_3 t_3)^{\beta_3(-k+1)} = (\alpha_3 t_3)^{(3-\beta_3)k+\beta_3+2}$$

et, comme $k \geq 260$, $(3-\beta_3)k + \beta_3 + 2 \leq -0{,}698$ donc, comme $a_3 t_3 > 1$,

$$E_3(k,\varepsilon)c_3^{-k+\varepsilon} \leq (\alpha_3 t_3)^{-0{,}698} \approx 0{,}434 < \frac{4}{9}$$

ce qui achève le preuve dans le cas $n = 3$.

Dans toute la suite, on suppose que $\varepsilon = 1$, ce qui est suffisant pour prouver le cas général, comme on l'a remarqué précédemment.

Pour $n = 4$, on vérifie que $E_4(k,1)c_4^{-2k} < \frac{27}{64}$ pour $k \in [\![1, 1304]\!]$ (le maximum étant $E_4(1,1)c_4^{-2} \approx 0{,}021$) et, si $k \geq 1305$, d'après le lemme 3.4.4,

$$E_4(k,1)c_4^{-2k} \leq (\alpha_4 t_4)^{4k+2}(\alpha_4 t_4)^{\beta_4(-2k)} = (\alpha_4 t_4)^{(4-2\beta_4)k+2} \leq (\alpha_4 t_4)^{-0{,}61} \approx 0{,}421 < \frac{27}{64}.$$

Pour $n = 5$, on vérifie que $E_5(k,1)c_5^{-3k-1} \leq \frac{256}{625}$ pour $k \in [\![1, 1039]\!]$ (le maximum étant $E_5(1,1)c_5^{-4} \approx 3{,}6.10^{-4}$) et, si $k \geq 1040$, d'après le lemme 3.4.4,

$$E_5(k,1)c_5^{-3k-1} \leq (\alpha_5(t_5)^{5k+2}(\alpha_5 t_5)^{\beta_5(-3k-1)} = (\alpha_5 t_5)^{(5-3\beta_5)k+2-\beta_5} \leq (\alpha_5 t_5)^{-0{,}707} \approx 0{,}40941 < \frac{256}{625}.$$

Traitons pour finir le cas $n \geq 6$. Alors, d'après le lemme 3.4.4 et par définition de c_n,

$$E_n(k,1)c_n^{(2-n)(k+1)+2} \leq (\alpha_n t_n)^{nk+2}(\alpha_n t_n)^{\frac{n}{n-2}((2-n)(k+1)+2)} = (\alpha_n t_n)^{\frac{-n^2+6n-4}{n-2}} = c_n^{-n+6-\frac{4}{n}}.$$

Pour tout $n \geq 6$, $-n + 6 - \frac{4}{n} < 0$ donc, comme $c_n \geq 7$, $c_n^{-n+6-\frac{4}{n}} \leq 7^{-n+6-\frac{4}{n}}$. Or, $w : n \mapsto 7^{-n+6-\frac{4}{n}}$ est décroissante donc $w(n) \leq w(6) < 0{,}28$ et la suite $n \mapsto \left(1 - \frac{1}{n}\right)^{n-1}$ tend en décroissant vers $\frac{1}{e}$ donc $\left(1 - \frac{1}{n}\right)^{n-1} \geq \frac{1}{e}$. Il s'ensuit que

$$E_n(k,1)c_n^{-(n-2)(k+1)+2} \leq 0{,}28 \leq \frac{1}{e} \leq \left(1 - \frac{1}{n}\right)^{n-1}$$

ce qui achève la démonstration. ■

Pour résumer, on a montré que si (x_1, y_1) et (x_2, y_2) sont deux solutions distinctes de (E_n) telles que $ax_2^n \geq c_n$ et $ax_1^n \geq c_n$ alors il existe un entier $k \geq 1$ (défini à l'aide du lemme 3.4.3) tel que, d'une part, $D_k \neq 0$ et, d'autre part, $P_k \leq \frac{1}{n}$ (par définition de k) et $Q_k \leq 1 - \frac{1}{n}$ (par la proposition 3.4.5 et l'inégalité (3.22)). Il s'ensuit donc que $P_k + Q_k \leq 1$. Or, d'après le lemme 3.4.2, le fait que $D_k \neq 0$ assure que $P_k + Q_k > 1$ ce qui est manifestement contradictoire.

Ainsi, on a bien démontré le théorème 3.1.1 en raisonnant par l'absurde.

Avant de passer à la démonstration du corollaire 3.1.2, terminons cette section par deux remarques. Les valeurs proposées pour α_n et β_n (et donc pour c_n) se comprennent a posteriori. La plus simple à expliquer est la valeur de β_n qui provient simplement de la nécessité de « faire disparaître » le terme en k dans la majoration obtenue dans la proposition 3.4.5. En effet, comme d'après le lemme 3.4.4, $E_n(r,\varepsilon) \leq (\alpha_n t_n)^{nr+\varepsilon+1}$, on a, puisque $c_n = (\alpha_n t_n)^{\beta_n}$,

$$E_n(k,\varepsilon)c_n^{(2-n)(k+1)+1+\varepsilon} \leq (\alpha_n t_n)^{nk+\varepsilon+1+\beta_n[(2-n)(k+1)+1+\varepsilon]}$$

donc la seule valeur possible pour β_n si on veut obtenir une majoration indépendante de k (ce qui est nécessaire car on a besoin d'appliquer la proposition à une valeur de k dont on sait l'existence mais sans connaître la valeur) est $\beta_n = \frac{n}{n-2}$. Le choix des valeurs de α_n est moins évident. Il est le fruit de deux contraintes : s'assurer, d'une part, que γ_n soit inférieure à α_n dans le lemme 3.4.4 tout en vérifiant, d'autre part, qu'on a bien $E_n(k,\varepsilon)c_n^{(2-n)(k+1)+1+\varepsilon} \leq \left(1 - \frac{1}{n}\right)^{n-1}$. Ces deux contraintes s'avèrent contradictoires en ce sens que, par exemple, diminuer la valeur de α_n permet de renforcer l'une mais peut mettre l'autre en défaut. Il faut donc trouver une sorte de « point d'équilibre » et c'est ce qui a été fait pour déterminer empiriquement α_n.

Enfin, remarquons que les choses seraient beaucoup plus simples pour les petites valeurs de n si on était assuré que $\varepsilon = 0$ i.e. que l'entier t défini par le lemme 3.4.3 vérifiait $D_t \neq 0$. On pourrait en particulier avoir l'espoir d'améliorer la valeur de c_3 si on parvenait à démontrer que D_r n'est jamais nulle pour $n = 3$. Ce n'est cependant pas le cas car une étude empirique montre que la valeur de ε a un effet primordial pour les petites valeurs de k mais négligeable pour les grandes valeurs de k. Ainsi, même sous l'hypothèse $\varepsilon = 0$, la contrainte de la proposition 3.4.5 conduit à une valeur de c_3 proche de 37.

3.5 Application à l'équation (E_n)

3.5.1 Démonstration du corollaire 3.1.2

On applique le théorème 3.1.1 pour montrer que si $n \geq 5$ et $b \neq a+1$ alors l'équation (E_n) admet au plus une solution. C'est une conséquence directe du lemme suivant.

Lemme 3.5.1. — *Pour tout $n \geq 5$, $c_n < n^2$.*

Preuve. — On vérifie que $c_n < n^2$ pour $n = 6$ ($c_6 \approx 29{,}2$) et pour n un nombre premier $n \in [\![5, 643]\!]$ grâce au tableau 3.2 p. 49. Dans tous les autres cas, $\alpha_n \leq \left(\frac{1}{3}\right)^{\frac{n-1}{n+1}}$ donc

$$c_n = (\alpha_n t_n)^{\beta_n} \leq \left(\frac{1}{3}\right)^{\frac{n(n-1)}{(n+1)(n-2)}} \left(n \prod_{p|n} p^{\frac{1}{p-1}}\right)^{\frac{n}{n-2}} \leq \frac{2^{\frac{n}{n-2}}}{3} \left(n \prod_{\substack{p|n \\ p\geq 3}} p^{\frac{1}{2}}\right)^{\frac{n}{n-2}} < \frac{2^{\frac{n}{n-2}}}{3} n^{\frac{3n}{2(n-2)}}.$$

Or, pour $n \geq 8$, $\dfrac{2^{\frac{n}{n-2}}}{3} < 1$ et $\dfrac{3n}{2(n-2)} < 2$ donc $c_n < n^2$. ■

Le corollaire 3.1.2 s'ensuit immédiatement. En effet, si $a \neq b+1$ alors $(1,1)$ n'est pas solution de (E_n). Si l'équation (E_n) admet une solution (x, y), on a donc $x \geq 2$ ou $y \geq 2$. Ainsi, dans ce cas, toute solution de (E_n) vérifie $ax^n \geq 2^n$. Or, si $n \geq 5$, $2^n \geq n^2$ donc $ax^n \geq n^2 > c_n$ d'après le lemme 3.5.1. On conclut alors, grâce au théorème 3.1.1 que, si $a \neq b+1$ et si $n \geq 5$, (E_n) admet au plus une solution.

Pour $n \in \{3, 4\}$, on ne peut pas conclure de même mais on peut cependant réduire sensiblement le nombre de cas restant à traiter.

3.5.2 Le cas $n = 3$

On s'intéresse ici à l'équation

$$(E_3) : ax^3 - by^3 = 1.$$

Supposons que (E_3) admette au moins deux solutions non triviales.

D'après le théorème 3.1.1, (E_3) a au plus une solution telle que $ax^3 \geq c_3$ i.e. telle que $ax^3 \geq 38$ donc il existe une solution non triviale (x_1, y_1) de (E_3) telle que $ax_1^3 \leq 37$. Il y a alors 3 cas possibles :

- Si $x_1 \geq 3$, cela impose que $a \leq \frac{37}{27}$ i.e. $a = 1$. De plus, comme $by_1^3 = ax_1^3 - 1$, $by_1^3 \in [\![26, 36]\!]$. Si $y_1 \geq 3$ alors $b = 1$ et le lemme 1.4.1 conduit à une absurdité. Si $y_1 = 2$ alors $b = 4$ mais on a, là aussi une absurdité, car $1 + 4y_1^3 = 33$ n'est pas le cube d'un entier. Enfin, si $y_1 = 1$ alors $x^3 = 1 + b$ avec $b \in [\![26, 36]\!]$, ce qui impose $b = 26$ et $x = 3$.
- Si $x_1 = 2$, cela impose que $a \leq \frac{37}{8}$ i.e. $a \in [\![1, 4]\!]$. L'examen des quatre cas montre alors que la seule valeur possible pour y_1 est 1 et ainsi $(a, b) \in \{(1, 7), (2, 15), (3, 23), (4, 31)\}$.
- Si $x_1 = 1$, cela impose que $a \leq 37$ et $by_1^3 = a - 1 \leq 36$. Dès lors, $y_1 \in \{1, 2, 3\}$. Si $y_1 = 1$ alors $b = a + 1$. Si $y_1 = 2$ alors $8b = a - 1 \leq 36$ implique $(a, b) \in \{(9, 1), (17, 2), (25, 3), (33, 4)\}$ Enfin, si $y_1 = 3$ alors $(a, b) = (28, 1)$.

Ainsi, les seules équations possibles restantes si $a \neq b + 1$ sont

$$\begin{array}{ccccc} x^3 - 26y^3 = 1 & x^3 - 7y^3 = 1 & 2x^3 - 15y^3 = 1 & 3x^3 - 23y^3 = 1 & 4x^3 - 31y^3 = 1 \\ 9x^3 - y^3 = 1 & 17x^3 - 2y^3 = 1 & 25x^3 - 3y^3 = 1 & 28x^3 - y^3 = 1 & 33x^3 - 4y^3 = 1 \end{array}$$

3.5.3 Le cas $n = 4$

On s'intéresse ici à l'équation

$$(E_4) : ax^4 - by^4 = 1.$$

On raisonne comme pour le cas $n = 3$ en supposant que (E_4) admet au moins deux solutions non triviales. Alors, il existe une solution non triviale (x_1, y_1) de (E_4) telle que $ax_1^4 \leq 17$. Il y a alors 2 cas possibles :

- Si $x_1 \leq 2$, cela impose que $a \leq \frac{17}{16}$ donc $a = 1$ et $x_1 = 2$. Dès lors, $by_1^4 = ax_1^4 - 1 = 15$ donc $y_1 = 1$ et $b = 15$.
- Si $x_1 = 1$, cela impose que $a \leq 17$ et $by_1^4 = a - 1 \leq 16$. Dès lors, $y_1 \in \{1, 2\}$. Si $y_1 = 1$ alors $b = a + 1$. Si $y_1 = 2$ alors $b = 1$ et donc $a = 17$.

Ainsi, les seules équations possibles restantes si $a \neq b + 1$ sont $x^4 - 15y^4 = 1$ et $17x^4 - y^4 = 1$.

Chapitre 4

Minoration de formes linéaires de logarithmes : le théorème de Laurent, Mignotte et Nesterenko
Les cas $a = b + 1$ et $n \geq 347$

4.1 Enoncé du résultat

On s'intéresse à présent à l'équation

$$(F_n) : (b+1)x^n - by^n = 1$$

où b est un entier naturel non nul.

L'équation (F_n) admet de façon évidente $(1,1)$ comme solution. Nous appellerons cette solution la solution triviale de (F_n). Le but de ce chapitre est de déterminer une borne explicite pour n telle que (F_n) n'a pas de solution non triviale au-delà de cette borne. Pour cela, nous utiliserons le théorème établi par Laurent, Mignotte et Nesterenko dans [21] (théorème 2). Nous en donnons ci-dessous une version simplifiée plus faible mais qui sera suffisante pour notre propos en diminuant cependant la contrainte sur a_1 et a_2 comme suggéré dans [26] (lemme 1).

Théorème 4.1.1. *(Laurent, Mignotte, Nesterenko) — Soit $\alpha_1 = \dfrac{p_1}{q_1}$ et $\alpha_2 = \dfrac{p_2}{q_2}$ deux nombres rationnels strictement positifs écrits sous formes irréductibles et soit b_1 et b_2 deux entiers naturels non nuls. On pose*

$$\Lambda = b_2 \ln(\alpha_2) - b_1 \ln(\alpha_1).$$

On suppose que $\ln(\alpha_2)$ et $\ln(\alpha_1)$ sont linéairement indépendants sur $\mathbb{Q}$. Soit ρ un réel strictement supérieur à 1 et $\lambda = \ln \rho$. On considère deux réels a_1 et a_2 tels que

$$(1)\quad a_i \geq (\rho - 1)\,|\ln(\alpha_i)| + 2\max\{p_i, q_i\} \quad \textit{pour } i \in \{1,2\}$$
$$(2)\quad a_1 + a_2 \geq 4\max\{1, \lambda\}$$
$$(3)\quad \frac{1}{a_1} + \frac{1}{a_2} \leq \min\{1, \lambda^{-1}\}.$$

Enfin, on considère un réel h tel que

$$h \geq \max\left\{\frac{1}{2}, 5\lambda, \ln\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \ln(\lambda) + 1{,}56\right\}$$

et on pose

$$A = \frac{4h}{\lambda} + 4 + \frac{\lambda}{h} \quad \textit{et} \quad B = 1 + \frac{h}{\lambda}.$$

Alors,

$$\ln|\Lambda| \geq -\frac{a_1a_2}{9\lambda}A^2 - \frac{2}{3}(a_1+a_2)A - \frac{16}{3}\sqrt{2a_1a_2B^3} - \ln\left(\frac{a_1a_2}{\lambda}B^2\right) - \frac{3}{2}\lambda - 2h - \frac{3}{20}.$$

La quantité Λ du théorème 4.1.1 est une *forme linéaire de logarithmes* et la conclusion du théorème permet d'en déterminer une minoration. C'est cette minoration qui va nous permettre de déterminer une borne pour n. Plus précisément, on va démontrer le théorème suivant.

Théorème 4.1.2. — *Pour tout $n \geq 347$, l'équation (F_n) n'a pas de solution non triviale.*

Nous procèderons pour l'essentiel comme dans [6] où les auteurs reprennent les idées utilisées dans [26].

4.2 Résultats préliminaires

Dans [6], Bennett et de Weger écartent le cas $b = 1$ en faisant référence à un résultat de Darmon et Merel [8]. Nous allons voir qu'en reprenant et en développant une idée présentée dans [26], on peut cependant intégrer le cas $b = 1$ dans l'étude générale.

Lemme 4.2.1. — *Quelles que soient les valeurs des entiers $b \geq 1$ et $n \geq 3$, l'équation*

$$(b+1)x^n - b(x+1)^n = 1$$

n'a pas de solution dans $\mathbb{N}$.

Preuve. — Supposons que x soit un entier tel que $(b+1)x^n - b(x+1)^n = 1$. Alors, en développant $(x+1)^n$ selon la formule du binôme de Newton, on obtient

$$x^n - b\sum_{k=0}^{n-1}\binom{n}{k}x^k = 1.$$

On en déduit, d'une part, que

$$x^n = 1 + bnx^{n-1} + b\sum_{k=0}^{n-2}\binom{n}{k}x^k > nbx^{n-1}$$

donc $x > nb$ et, d'autre part, que

$$x\left(x^{n-1} - b\sum_{k=1}^{n-1}\binom{n}{k}x^{k-1}\right) = b+1$$

donc x divise $b+1$. Ainsi, $3b \leq nb < x \leq b+1$ ce qui est absurde car $b \geq 1$. ■

Lemme 4.2.2. — *Si $(x,y) \in \mathbb{N}^2$ est une solution non triviale de (F_n) alors $x \geq 2nb$ et $y \geq 2(nb+1)$.*

Preuve. — Soit $(x,y) \in \mathbb{N}^2$ une solution non triviale de (F_n). Si $x = 1$ alors $by^n = b$ donc $y = 1$ ce qui est exclu. Ainsi, $x > 1$. De plus, si $y \leq x$ alors

$$1 = (b+1)x^n - by^n \geq (b+1)x^n - bx^n = x^n$$

et ainsi $x = 1$ ce qui n'est pas possible comme on vient de voir. Dès lors, $x < y$.

Ecrivons alors $y = x + t$ avec $t \in \mathbb{N}^*$. D'après le lemme 4.2.1, $y \neq x+1$ donc $t \geq 2$. De plus, en raisonnant comme dans la démonstration de ce lemme,

$$x^n = 1 + bnx^{n-1}t + \sum_{k=0}^{n-2}\binom{n}{k}b^kt^{n-k} \geq nbtx^{n-1}$$

donc $x \geq nbt \geq 2nb$ et alors, comme $y = x + t \geq x + 2$, $y \geq 2(nb+1)$. ■

4.3 Une première majoration

Dans toute la suite, (x, y) désigne une solution non triviale de (F_n) et n un nombre premier supérieur ou égal à 347. Ceci implique en particulier que (F_n) admet au moins deux solutions distinctes donc, d'après le théorème 3.1.1, $(b+1) \times 1^n < c_n$ i.e.

$$b \leq \lfloor c_n \rfloor - 1. \tag{4.1}$$

Commençons par quelques remarques simples. Comme n est premier et supérieur à 347, le nombre c_n est défini dans le théorème 3.1.1 par $c_n = \left(\alpha_n n^{\frac{n}{n-1}}\right)^{\frac{n}{n-2}}$ avec $\alpha_n \leq \alpha_{347} = 0{,}2548$. Or, une étude élémentaire montre que $n \mapsto \frac{1}{n}\left(0{,}2548 n^{\frac{n}{n-1}}\right)^{\frac{n}{n-2}}$ est décroissante à partir du rang 3 donc $\frac{c_n}{n} \leq \frac{c_{347}}{347} < 0{,}266$ et ainsi $c_n < 0{,}266n$. Ceci implique en particulier que

$$b < 0{,}266n - 1 \text{ (1)}. \tag{4.2}$$

Ensuite, d'après le lemme 4.2.2, $y \geq 2(nb+1)$. Ainsi, d'une part, on peut dire que $2(nb+1) > 2n \geq 694$ donc $y > 694$. D'autre part, d'après (4.2), $n > \frac{b+1}{0{,}266}$ donc $2(nb+1) > 2\frac{b(b+1)}{0{,}266} > (b+1)^2$ car $b \geq 1$. Ainsi,

$$y > \max\{(b+1)^2, 694\} \tag{4.3}$$

Suivant [26] et [6], nous allons appliquer le théorème 4.1.1 en prenant

$$\alpha_1 = \frac{y}{x}, \quad \alpha_2 = \frac{b+1}{b} = 1 + \frac{1}{b}, \quad b_1 = n \quad \text{et} \quad b_2 = 1.$$

Remarquons tout d'abord que $\ln(\alpha_1)$ et $\ln(\alpha_2)$ sont linéairement indépendants sur $\mathbb{Q}$. En effet, supposons qu'il existe deux rationnels r_1 et r_2 tels que $r_1 \ln(\alpha_1) = r_2 \ln(\alpha_2)$ alors il existe deux entiers naturels k_1 et k_2 tels que $k_1 \ln\left(\frac{y}{x}\right) = k_2 \ln\left(\frac{b+1}{b}\right)$ (car, comme on l'a vu dans la démonstration du lemme 4.2.2, $x < y$). Il s'ensuit alors que $(b+1)^{k_2} x^{k_1} = b^{k_2} y^{k_1}$. Or, l'égalité $(b+1)x^n - by^n = 1$ assure que y est premier avec x et $b+1$ et donc avec $(b+1)^{k_2} x^{k_1}$ et, comme $y > 1$, on aboutit à une absurdité.

Ensuite, en posant $\Lambda = b_2 \ln(\alpha_2) - b_1 \ln(\alpha_1)$, on déduit de l'égalité $(b+1)x^n - by^n = 1$ que

$$|\Lambda| = \left|\ln\left(1 + \frac{1}{b}\right) - n \ln\left(\frac{y}{x}\right)\right| = \ln\left(\frac{(b+1)x^n}{by^n}\right) = \ln\left(1 + \frac{1}{by^n}\right) < \frac{1}{by^n} \tag{4.4}$$

et, par conséquent,

$$n \ln\left(\frac{y}{x}\right) < \ln\left(1 + \frac{1}{b}\right) + \frac{1}{by^n}. \tag{4.5}$$

Pour le choix de ρ, ensuite, nous posons

$$\rho = \begin{cases} 1 + \dfrac{\ln 4}{\ln \frac{4}{3}} & \text{si } b \leq 2 \\ 1 + \dfrac{\ln(b+1)}{\ln\left(1 + \frac{1}{b}\right)} & \text{si } b \geq 3 \end{cases}. \tag{4.6}$$

Nous allons à présent donner trois lemmes qui nous permettrons de choisir des valeurs adéquates pour les réels a_1, a_2 et h du théorème 4.1.1.

(1). Dans [6], les auteurs établissent la majoration plus faible $b < 0{,}3n$ mais qu'ils démontrent pour tout $n \geq 3$. Ce résultat s'appuie sur d'autres résultats d'approximation diophantienne et nous montrons ici qu'une application minutieuse du théorème d'Evertse dans la forme que nous avons démontré au chapitre 3 est en fait suffisante.

Lemme 4.3.1. — *Quelle que soit la valeur de l'entier b,*

$$(\rho-1)\ln\left(\frac{y}{x}\right)+2\ln y<2{,}002\ln y.$$

Preuve. — Il suffit évidemment de montrer que $(\rho-1)\ln\left(\frac{y}{x}\right)<0{,}002\ln y$. On déduit de (4.5) que $\ln\left(\frac{y}{x}\right)<\frac{1}{n}\left[\ln\left(1+\frac{1}{b}\right)+\frac{1}{by^n}\right]$.

Si $b=1$ alors

$$(\rho-1)\ln\left(\frac{y}{x}\right)=\frac{\ln 4}{\ln\frac{4}{3}}\ln\left(\frac{y}{x}\right)<\frac{1}{n\ln\frac{4}{3}}\left[\ln 2+\frac{1}{y^n}\right]\frac{\ln 4}{\ln y}\ln y$$

et comme $y>694$ et $n\geq 347$, $\frac{1}{n\ln\frac{4}{3}}\left[\ln 2+\frac{1}{y^n}\right]\frac{\ln(4)}{\ln(y)}<0{,}002$.

Si $b=2$, on a raisonne de même en remplaçant $\ln 2$ par $\ln\frac{3}{2}$.

Enfin, si $b\geq 3$ alors

$$(\rho-1)\ln\left(\frac{y}{x}\right)=\frac{\ln(b+1)}{\ln\left(1+\frac{1}{b}\right)}\ln\left(\frac{y}{x}\right)<\frac{\ln(b+1)}{n}+\frac{\ln(b+1)}{nb\ln\left(1+\frac{1}{b}\right)y^n}.$$

En utilisant la croissance de $b\mapsto b\ln\left(1+\frac{1}{b}\right)$ et le fait que, d'après (4.3), $y>(b+1)^2$, on en déduit que

$$(\rho-1)\ln\left(\frac{y}{x}\right)<\frac{\ln(b+1)}{n}+\frac{\ln(b+1)}{3\ln\left(\frac{4}{3}\right)ny^n}<\frac{1}{2n}\left[1+\frac{1}{3\ln\left(\frac{4}{3}\right)y^n}\right]\ln y.$$

Pour finir, le fait que $y>694$ et $n\geq 347$ assure que $\frac{1}{2n}\left[1+\frac{1}{3\ln\left(\frac{4}{3}\right)y^n}\right]<0{,}002$. ■

Ce lemme nous montre en particulier que le choix $a_1=2{,}002\ln y$ satisfait la condition (1) du théorème 4.1.1. Pour a_2, on peut remarquer que, si $b\geq 3$,

$$(\rho-1)\ln\left(1+\frac{1}{b}\right)+2\ln(b+1)=3\ln(b+1)$$

donc le choix $a_2=3\ln(b+1)$ satisfait la condition (1) pour $b\geq 3$. Pour $b=1$, un simple calcul montre que $(\rho-1)\ln\left(1+\frac{1}{b}\right)+2\ln(b+1)<4{,}72$ et, de même, pour $b=2$, $(\rho-1)\ln\left(1+\frac{1}{b}\right)+2\ln(b+1)<4{,}15$. Ainsi, on définit les réels a_1 et a_2 par

$$a_1=2{,}002\ln y\qquad\text{et}\qquad a_2=\begin{cases}4{,}72\text{ si }b=1\\4{,}15\text{ si }b=2\\3\ln(b+1)\text{ si }b\geq 3\end{cases}\tag{4.7}$$

Il nous faut encore vérifier que a_1 et a_2 satisfont les conditions (2) et (3) du théorème 4.1.1. Pour cela, nous allons utiliser le lemme suivant.

Lemme 4.3.2. — *Pour tout $b\geq 3$, $\ln(b+1)<\lambda<1{,}365\ln(b+1)$.*

Preuve. — Soit un entier $b\geq 3$. Alors, étant donné que $0<\ln\left(1+\frac{1}{b}\right)<\frac{1}{b}$ et que $\ln(b+1)>1$, $\frac{\ln(b+1)}{\ln\left(1+\frac{1}{b}\right)}>b$. Par suite, $\lambda=\ln\rho=\ln\left(1+\frac{\ln(b+1)}{\ln\left(1+\frac{1}{b}\right)}\right)>\ln(1+b)$.

D'autre part, une étude de la fonction $t \mapsto \ln\left(1+\dfrac{\ln(t+1)}{\ln\left(1+\frac{1}{t}\right)}\right) - 1{,}365\ln(t+1)$ montre qu'elle est négative sur $]0\,;+\infty[$ donc $\lambda < 1{,}365\ln(b+1)$. ■

On peut à présent montrer que a_1 et a_2 satisfont les conditions (2) et (3).

Si $b=1$, $a_1+a_2 = 4{,}72 + 2{,}002\ln y \geq 4{,}72 + 2{,}002\ln 694 > 17{,}8$ alors que $4\max\{1,\lambda\} < 7{,}1$ et $\frac{1}{a_1}+\frac{1}{a_2} = \frac{1}{4{,}72}+\frac{1}{2{,}002\ln y} < \frac{1}{4{,}72}+\frac{1}{2{,}002\ln 694} < 0{,}3$ alors que $\min\{1,\lambda^{-1}\} > 0{,}5$.

Si $b=2$, de même, $a_1+a_2 > 17{,}2$ alors que $4\max\{1,\lambda\} < 7{,}1$ et $\frac{1}{a_1}+\frac{1}{a_2} < 0{,}3$ alors que $\min\{1,\lambda^{-1}\} > 0{,}5$.

Enfin, si $b \geq 3$, en utilisant le lemme 4.3.2 ainsi que (4.3),

$$a_1+a_2 = 3\ln(b+1) + 2{,}002\ln y > 3\ln(b+1) + 4{,}004\ln(b+1) > 4\times 1{,}365\ln(b+1) > 4\lambda$$

et

$$\frac{1}{a_1}+\frac{1}{a_2} = \frac{1}{3\ln(b+1)} + \frac{1}{2{,}002\ln y} < \frac{1}{3\ln(b+1)} + \frac{1}{4{,}004\ln(b+1)} < \frac{1}{1{,}365\ln(b+1)} < \lambda^{-1}$$

ce qui, dans les deux cas, permet de conclure car $\lambda > \ln(b+1) > 1$.

Pour terminer, il nous reste à choisir h. On va pour se faire s'appuyer sur le lemme suivant.

Lemme 4.3.3. — *Quelle que soit la valeur de l'entier b,*

$$\ln\left(\frac{n}{a_2}+\frac{1}{a_1}\right) + \ln\lambda + 1{,}56 < 1{,}2\ln n.$$

Preuve. — En écrivant $\ln\left(\frac{n}{a_2}+\frac{1}{a_1}\right) = \ln n + \ln\left(\frac{1}{a_2}+\frac{1}{na_1}\right)$, il suffit pour prouver le lemme de montrer que $\mu := \ln\left(\frac{1}{a_2}+\frac{1}{na_1}\right) + \ln\lambda + 1{,}56 < 0{,}2\ln n$.

Pour $b=1$, en minorant $n\ln y$ par $347\ln(694)$, il vient

$$\mu = \ln\left(\frac{1}{4{,}72}+\frac{1}{2{,}002n\ln y}\right) + \ln\ln\left(1+\frac{\ln 4}{\ln\frac{4}{3}}\right) + 1{,}56 < 0{,}58$$

et donc, comme $\frac{0{,}58}{\ln n} < \frac{0{,}58}{\ln 347} < 0{,}2$, on a bien $\mu < 0{,}2\ln n$.

Pour $b=2$, on a de même $\mu < 0{,}71$ et $\frac{0{,}571}{\ln 347} < 0{,}2$.

Enfin, pour $b \geq 3$, en utilisant le lemme 4.3.2, (4.3) et le fait que $n \geq 347$,

$$\begin{aligned}
\mu &= \ln\left(\frac{1}{3\ln(b+1)}+\frac{1}{2{,}002n\ln y}\right) + \ln\lambda + 1{,}56 \\
&< \ln\left(\frac{1}{3\ln(b+1)}+\frac{1}{2{,}002n\ln(b+1)^2}\right) + \ln(1{,}365\ln(b+1)) + 1{,}56 \\
&< \ln\left(\frac{1{,}365}{3}+\frac{1{,}365}{4{,}004n}\right) + 1{,}56 \leq 0{,}78
\end{aligned}$$

et $\frac{0{,}78}{\ln 347} < 0{,}2$ donc $\mu < 0{,}2\ln n$ ■

Ainsi, d'après ce lemme, on peut choisir $h = \max\{5\lambda, 1{,}2\ln n\}$. On va en fait montrer que ce maximum vaut 5λ.

Pour cela, on raisonne par l'absurde en supposant que $h = 1{,}2 \ln n > 5\lambda$. Alors, d'une part, on déduit du lemme 4.3.2 que, si $b \geq 3$, $n > \exp(\lambda)^{\frac{5}{1,2}} > (b+1)^{\frac{5}{1,2}}$ donc en particulier $n > (b+1)^4$. Comme, par ailleurs, $n \geq 347$, cette égalité reste vraie pour $b = 1$ et $b = 2$. D'autre part, en remarquant que $\exp(\lambda) = \rho$, on a $n > \rho^{\frac{5}{1,2}}$. Or, ρ croît avec b donc $\rho \geq 1 + \dfrac{\ln 4}{\ln \frac{4}{3}}$ et ainsi $n > \left(1 + \dfrac{\ln 4}{\ln \frac{4}{3}}\right)^{\frac{5}{1,2}}$ ce qui assure, en particulier que $n > 1\,500$. On a donc

$$n > \max\{(b+1)^4, 1\,500\} \tag{4.8}$$

On va montrer que, sous l'hypothèse $h = 1{,}2 \ln n > 5\lambda$, le théorème 4.1.1 conduit à une absurdité. Pour cela, nous allons traiter séparément les cas $b \leq 2$ et $b \geq 3$ en commençant à chaque fois par majorer les nombres A et B qui, rappelons-le, sont définis par

$$A = \frac{4h}{\lambda} + 4 + \frac{\lambda}{h} \quad \text{et} \quad B = 1 + \frac{h}{\lambda}.$$

- Cas $b \leq 2$

Si $b = 1$ ou $b = 2$, $\lambda = \ln\left(1 + \dfrac{\ln 4}{\ln \frac{4}{3}}\right) \in]1{,}76\,;1{,}77[$ donc

$$A = \frac{4 \times 1{,}2 \ln n}{\lambda} + 4 + \frac{\lambda}{1{,}2 \ln n} < \frac{4{,}8}{1{,}76} \ln n + 4 + \frac{1{,}77}{1{,}2 \ln 1\,500} < 2{,}73 \ln n + 4{,}21.$$

Or, on vérifie que, pour $n \geq 1\,500$, $2{,}73 \ln n + 4{,}21 < 3{,}31 \ln n$ donc $A < 3{,}31 \ln n$. Par ailleurs, $B = \dfrac{1}{4}\left(4 + \dfrac{4h}{\lambda}\right) < \dfrac{A}{4}$. On va à présent distinguer les cas $b = 1$ et $b = 2$.

Si $b = 1$, l'application du théorème 4.1.1 donne

$$\ln|\Lambda| > -6{,}54 \ln y \ln^2 n - 4{,}42 \ln y \ln n - 12{,}82 \ln n - 17{,}46\sqrt{\ln y \ln^3 n} - \ln(3{,}68 \ln y \ln^2 n) - 2{,}49.$$

D'après le lemme 4.2.2, $y > 2n$ donc $\ln(y) > \ln(n)$ et, en particulier, $\ln y \ln^3 n < (\ln y \ln n)^2$. Il s'ensuit que

$$\ln|\Lambda| > -6{,}54 \ln y \ln^2 n - 21{,}88 \ln y \ln n - 12{,}82 \ln n - \ln(\ln y) - 2\ln(\ln n) - 3{,}8$$

et, comme $\ln(\ln(n)) < \ln(\ln(y))$,

$$\ln|\Lambda| > -6{,}54 \ln y \ln^2 n - 21{,}88 \ln y \ln n - 12{,}82 \ln y - 3\ln(\ln y) - 3{,}8.$$

Enfin, $y > 2n > 3\,000$, et on vérifie que, pour tout $y > 3\,000$, $3\ln(\ln y) + 3{,}8 < 1{,}26 \ln y$ donc

$$\ln|\Lambda| > -(6{,}54 \ln^2 n + 21{,}88 \ln n + 14{,}08) \ln y.$$

Or, pour tout $t \geq 373$, $6{,}54 \ln^2 t + 21{,}88 \ln t + 14{,}08 < t$ donc, comme $n \geq 1\,500$,

$$\ln|\Lambda| > -n \ln y.$$

Or, d'après (4.4),

$$\ln|\Lambda| < -\ln(by^n) \leq -n \ln y \tag{4.9}$$

ce qui fournit la contradiction voulue.

Si $b = 2$, on raisonne de même en montrant que

$$\begin{aligned}\ln|\Lambda| &> -5{,}75\ln y\ln^2 n - 4{,}42\ln y\ln n - 11{,}56\ln n - 16{,}37\sqrt{\ln y\ln^3 n} - \ln(3{,}24\ln y\ln^2 n) - 2{,}49\\ &> -5{,}75\ln y\ln^2 n + 20{,}79\ln y\ln n - 11{,}56\ln y - 3\ln(\ln y) - 3{,}67\\ &> -(5{,}75\ln^2 n + 20{,}79\ln n + 12{,}8)\ln y.\end{aligned}$$

Or, pour tout $t \geq 326$, $5{,}75\ln^2 t + 20{,}79\ln t + 12{,}8 < t$ et on conclut de même.

• Cas $b \geq 3$

Si $b \geq 3$,

$$A = \frac{4{,}8\ln n}{\lambda} + 4 + \frac{\lambda}{1{,}2\ln n} = \frac{\ln n}{\lambda}\left(4{,}8 + \frac{4\lambda}{\ln n} + \frac{\lambda^2}{1{,}2\ln^2 n}\right).$$

Or, par hypothèse, $1{,}2\ln n > 5\lambda$ donc $\dfrac{\lambda}{\ln n} < \dfrac{1{,}2}{5}$ et ainsi

$$A < \frac{\ln n}{\lambda}\left(4{,}8 + \frac{4{,}8}{5} + \frac{1{,}2}{25}\right) < 5{,}81\frac{\ln n}{\lambda}.$$

De même,

$$B = 1 + \frac{h}{\lambda} = 1 + \frac{1{,}2\ln n}{\lambda} = \frac{\ln n}{\lambda}\left(\frac{\lambda}{\ln n} + 1{,}2\right) < 1{,}44\frac{\ln n}{\lambda}.$$

En utilisant le fait que $\lambda > \ln(b+1)$, l'application du théorème 4.1.1 donne alors

$$\begin{aligned}\ln|\Lambda| > -22{,}53\left(\frac{\ln n}{\lambda}\right)^2\ln y - 7{,}76\left(\frac{\ln n}{\lambda}\right)\ln y - 14{,}02\ln n\\ - 31{,}95\frac{\sqrt{\ln y\ln^3 n}}{\lambda} - \ln\left(12{,}45\ln y\left(\frac{\ln n}{\lambda}\right)^2\right) - \frac{3}{2}\lambda - 0{,}15.\end{aligned}$$

En raisonnant comme dans les cas $b \leq 2$ et en utilisant l'encadrement $1{,}76 < \lambda < \dfrac{1{,}2\ln n}{5}$, on en déduit que

$$\ln|\Lambda| > -7{,}28\ln y\ln^2 n - 22{,}56\ln y\ln n - 14{,}38\ln y - 3\ln(\ln y) - 1{,}55$$

On vérifie que, pour $y > 3000$, $3\ln(\ln y) + 1{,}55 < 0{,}98\ln y$ donc

$$\ln|\Lambda| > -(7{,}28\ln^2 n + 22{,}56\ln n + 15{,}36)\ln y.$$

Or, pour tout $t \geq 417$, $7{,}28\ln^2 t + 22{,}56\ln t + 15{,}36 < t$ donc, comme $n \geq 1\,500$, $\ln|\Lambda| > -n\ln y$ et on conclut comme dans les cas précédents.

Ainsi, on conclut que $h = 5\lambda$ et donc $A = \dfrac{20\lambda}{\lambda} + 4 + \dfrac{\lambda}{5\lambda} = 24{,}2$ et $B = 1 + \dfrac{5\lambda}{\lambda} = 6$. L'application du théorème 4.1.1 donne

$$\begin{aligned}\ln|\Lambda| > -\left(\frac{14\,655\,641\ln(b+1)}{37\,500\lambda} + \frac{121121}{3750}\right)\ln y - \frac{242}{5}\ln(b+1) - \frac{96}{25}\sqrt{5\,005\ln(b+1)}\sqrt{\ln y}\\ - \ln(\ln y) - \ln\left(\frac{27\,027\ln(b+1)}{125\lambda}\right) - \frac{23}{2}\lambda - \frac{3}{20}\end{aligned} \quad (4.10)$$

et alors, en utilisant encore une fois le fait que $\ln(b+1) < \lambda$,

$$\begin{aligned}\ln|\Lambda| &> -423{,}12\ln y - 48{,}4\ln(b+1) - 271{,}67\sqrt{\ln y\ln(b+1)} - \ln(\ln y) - 11{,}5\lambda - 5{,}53\\ &> -423{,}12\ln y - 59{,}9\ln(b+1) - 271{,}67\sqrt{\ln y\ln(b+1)} - \ln(\ln y) - 5{,}53.\end{aligned}$$

Etant donné que $y > (b+1)^2$, il vient alors

$$\ln|\Lambda| > -645{,}17\ln y - \ln(\ln y) - 5{,}53.$$

Or, pour tout $t > 694$, $\ln(\ln t) + 5{,}53 < 1{,}14\ln(t)$ donc

$$\ln|\Lambda| > -646{,}36\ln y$$

et, d'après (4.9), $\ln|\Lambda| < -n\ln y$ donc $n \leq 646$ soit, comme n est premier, $n \leq 643$.

Ainsi, le théorème de Laurent, Mignotte et Nesterenko nous permet de conclure que si (F_n) admet au moins deux solutions alors $n \leq 643$. On obtient ainsi une majoration absolue de n i.e. indépendante de la valeur de b. On va voir dans le paragraphe suivant qu'on peut, en raisonnant de façon un peu plus fine, améliorer encore cette borne toujours grâce au théorème 4.1.1.

4.4 Démonstration du théorème 4.1.2

Commençons par remarquer qu'à l'aide de (4.1) et du tableau 3.2 p. 49, la majoration $n \leq 643$ implique que $b \leq 165$. On est donc ramené à étudier un nombre fini de valeurs de b.

Posons

$$K_1(b) = \frac{14\,655\,641\ln(b+1)}{37\,500\lambda} + \frac{121121}{3750}, \qquad K_2(b) = \frac{96}{25}\sqrt{5\,005\ln(b+1)}$$
$$\text{et} \qquad K_3(b) = \frac{242}{5}\ln(b+1) + \ln\left(\frac{27\,027\ln(b+1)}{125\lambda}\right) + \frac{23}{2}\lambda + \frac{3}{20}.$$

Ces quantités ne dépendent que de b car, rappelons-le, $\lambda = \ln\rho$ où $\rho = \rho(b)$ est définie par (4.6). Avec ces notations, l'inégalité (4.10) s'écrit

$$\ln|\Lambda| > -K_1(b)\ln y - K_2(b)\sqrt{\ln y} - \ln(\ln y) - K_3(b)$$

et, d'après (4.9), $\ln|\Lambda| < -\ln b - n\ln y$ donc

$$(n - K_1(b))\ln y - K_2(b)\sqrt{\ln y} - \ln(\ln y) - K_3(b) + \ln b < 0. \tag{4.11}$$

On vérifie que, pour tout $b \in [\![1, 165]\!]$, $K_1(b) < 340$, le maximum étant atteint pour $b = 3$. Ainsi, pour toutes les valeurs de b et de n considérées,

$$n - K_1(b) > 0. \tag{4.12}$$

Une étude élémentaire de la fonction $g : y \mapsto (n - K_1(b))\ln y - K_2(b)\sqrt{\ln y} - \ln(\ln y) - K_3(b) + \ln b$ définie sur $]1\,;+\infty[$ montre qu'elle est décroissante sur $]1\,;\alpha_{n,b}]$ et croissante sur $[\alpha_{n,b}\,;+\infty[$ où

$$\alpha_{n,b} = \exp\left[\frac{\left(\frac{K_2(b)}{2} + \sqrt{\left(\frac{K_2(b)}{2}\right)^2 + 4(n - K_1(b))}\right)^2}{4(n - K_1(b))^2}\right].$$

En calculant les valeurs de $\alpha_{n,b}$ pour $n \in [\![347, 643]\!]$ et $b \in [\![1, 165]\!]$, on constate que $\alpha_{n,b}$ est toujours supérieur à 1,06, le minimum étant atteint pour $(n, b) = (643, 1)$. Or, en calculant les valeurs de $g(n, b, 1{,}06)$ pour $n \in [\![347, 643]\!]$ et $b \in [\![1, 165]\!]$, on constate que $g(n, b, 1{,}06)$ est toujours inférieur à -83, le maximum étant atteint pour $(n, b) = (643, 1)$. Ainsi, pour tout $y \in [1{,}06\,;\alpha_{n,b}]$, $g(n, b, y) < 0$.

Comme par ailleurs la condition (4.12) assure que $\lim_{y\to+\infty} g(n,b,y) = +\infty$, il existe un unique réel $M_n(b) \in]1{,}06\,;+\infty[$ telle que $g(n,b,y) < 0$ pour tout $y \in]1{,}06\,;M_n(b)[$ et $g(n,b,y) \geq 0$ pour tout $y \in [M_n(b)\,;+\infty[$.

La relation (4.11) assure alors que

$$y < M_n(b). \tag{4.13}$$

Si $n \geq 541$, on vérifie que le majorant $M_n(b)$ ainsi obtenu est en contradiction avec la minoration du lemme 4.2.2. On peut donc restreindre l'étude aux valeurs de n telles que $n \leq 523$.

En calculant les valeurs de $K_1(b)$, $K_2(b)$ et $K_3(b)$ pour les différentes valeurs de b entre 1 et 165, on détermine à l'aide de Maple 16 une valeur par excès de $M_n(b)$. On a rassemblé dans le tableau suivant, pour chaque valeur de n, un majorant M_n des $M_n(b)$ (la plus grande valeur étant obtenue, à chaque fois, pour $b = 165$ excepté si $n \leq 349$ dans quel cas la maximum est atteint pour $b = 3$).

n	347	349	353	359	367	373	379	383
M_n	10^{904}	10^{551}	10^{288}	10^{188}	10^{119}	10^{90}	10^{71}	10^{61}
n	389	397	401	409	419	421	431	433
M_n	10^{50}	10^{40}	10^{36}	10^{29}	10^{24}	10^{23}	10^{19}	10^{18}
n	439	443	449	457	461	463	467	479
M_n	10^{16}	10^{15}	10^{14}	10^{13}	10^{12}	10^{12}	10^{11}	10^{10}
n	487	491	499	503	509	521	523	
M_n	10^{9}	10^{8}	10^{8}	10^{7}	10^{7}	10^{6}	10^{6}	

On va alors pouvoir conclure grâce à la remarque suivante qui découle du lemme 1.4.2 vu à la fin du premier chapitre. Ce lemme nous assure que si (x,y) est une solution de (F_n) alors $\frac{y}{x}$ est une réduite dans le développement en fractions continuées de $\sqrt{1+\frac{1}{b}}$. Notons, comme dans le chapitre 1, pour tout $k \in \mathbb{N}$, $R_k = \frac{p_k}{q_k}$ la $k-$ième réduite de $\sqrt{1+\frac{1}{b}}$, x_k le $k-$ième quotient complet et $a_k = \lfloor x_k \rfloor$ le $k-$ième quotient partiel. Comme $x \neq 1$, il existe un indice $i \in \mathbb{N}^*$ tel que $y = p_i$ et $x = q_i$ (car $\mathrm{PGCD}(y,x) = \mathrm{PGCD}(p_i,q_i) = 1$). D'après (1.7),

$$\left|\sqrt{1+\frac{1}{b}} - \frac{p_i}{q_i}\right| < \frac{1}{nbq_i^n}$$

et, d'après la proposition (1.1.7),

$$\frac{1}{q_i(q_i+q_{i+1})} < \left|\sqrt{1+\frac{1}{b}} - \frac{p_i}{q_i}\right|$$

donc

$$q_i + q_{i+1} > nbq_i^{n-1}.$$

Or, d'après le lemme 1.1.2, $q_{i+1} = a_iq_i + q_{i-1} \leq a_iq_i + q_i = (a_i+1)q_i$ donc $(2+a_i)q_i > nbq_i^{n-1}$ i.e. comme a_i est entier,

$$a_i \geq nbq_i^{n-2} - 1 \tag{4.14}$$

Enfin, d'après le lemme 4.2.2, $q_i = x \geq 2nb$ donc

$$a_i \geq nb(2nb)^{n-2} - 1 > (nb)^{n-1} \tag{4.15}$$

On en déduit donc qu'une solution non triviale de (F_n) induit un quotient partiel a_i qui est tel que $a_i > 347^{346} > 10^{878}$.

Or, en calculant les quotients partiels pour $n \in [\![347, 523]\!]$, $b \in [\![1, 165]\!]$ et $q_i \leq M_n$, on constate que le plus grand quotient partiel est 1 817 451 obtenu pour $n = 349$, $b = 150$ et $i = 424$ (voir Annexe B).

Ainsi, il n'y a pas de solution non triviale de (F_n) si $b \in [\![1, 165]\!]$ et $n \in [\![349, 523]\!]$ ce qui achève la démonstration du théorème 4.1.2.

Pour terminer, remarquons que la valeur 347 du théorème 4.1.2 semble a priori assez arbitraire voire mystérieuse. On pourrait d'ailleurs reprendre toute l'étude de la partie 4.3 avec une valeur plus faible (par exemple 331 comme dans [6] [(2)]) en espérant ainsi obtenir un meilleur résultat que celui que nous avons énoncé. Cependant, l'essence de la démonstration, outre le théorème de Laurent, Mignotte et Nesterenko, réside dans le fait de pouvoir majorer y grâce à la relation (4.11). Or, il est clair que si $n < 347$ (tout en étant premier donc, en fait, $n \leq 337$) alors l'inégalité (4.12) n'est plus vraie et donc la fonction g est négative sur $]1\,;+\infty[$ de sorte que l'inégalité (4.11) n'apporte plus aucune information sur y. Ainsi, c'est essentiellement l'inégalité (4.12) qui nous permet de voir a posteriori qu'on ne peut pas, en suivant la méthode décrite ci-dessus, obtenir une meilleure valeur que 347. Il va donc falloir pour les valeurs de $n \leq 337$ aborder le problème avec un nouveau point de vue. C'est ce que nous allons faire dans le chapitre suivant en revenant aux approximants de Padé abordés dans le chapitre 2 et en étudiant de façon précise certaines propriétés arithmétiques des coefficients de ces polynômes dans le cas d'une famille de fonctions binomiales.

(2). Notons, cependant, que les auteurs de [6] ne choisissent pas 331 au hasard et que ce choix est motivé par le fait qu'il leur permet de montrer que (F_n) n'a pas de solution non triviale pour $b \geq 84$ et $n \geq 331$ ce qui, associé au tableau 3.2 p. 49 assure que l'équation (F_n) n'a pas de solution non triviale pour $b \geq 84$. Nous n'avons cependant pas besoin de ce raffinement ici et nous sommes donc partis directement de $n \geq 347$.

Chapitre 5

Le théorème de Bennett Les cas $a = b + 1$ et $17 \leq n \leq 337$

5.1 Introduction

Nous présentons dans ce dernier chapitre la démarche suivie par Bennett [5] pour traiter les derniers cas restants i.e. n premier entre 17 et 337 et $a - 1 = b \in [\![1, \lfloor c_n \rfloor - 1]\!]$.

Le théorème principal de Bennett est un résultat d'approximation diophantienne qui permet d'obtenir une mesure effective d'irrationalité des nombres $\sqrt[n]{\frac{a}{b}}$ pour les nombres premiers n compris entre 17 et 337. En voici l'énoncé :

Théorème 5.1.1. — *Soit $n \in [\![3, 337]\!]$ un nombre premier, $m = \left\lfloor \frac{n+1}{3} \right\rfloor$ et $a > b$ des entiers strictement positifs et premiers entre eux. Il existe des constantes explicites k_n et h_n telles que si*

$$\left(a^{\frac{1}{m}} - b^{\frac{1}{m}}\right)^m \mathrm{e}^{k_n} < 1$$

alors, pour tous entiers p et q tels que $q > 0$, on a

$$\left|\left(\frac{a}{b}\right)^{\frac{1}{n}} - \frac{p}{q}\right| > \frac{1}{Kq^{\lambda}}$$

où

$$K = K(n, a, b) = 1{,}56.10^{24} m(m-1) n^{m-1} \mathrm{e}^{k_n + h_n} \left(a^{\frac{1}{m}} + b^{\frac{1}{m}}\right)^m \text{ (1)}$$

et

$$\lambda = \lambda(n, a, b) = (m-1)\left(1 - \frac{\ln\left(\left(a^{\frac{1}{m}} + b^{\frac{1}{m}}\right)^m \mathrm{e}^{k_n + \frac{1}{20}}\right)}{\ln\left(\left(a^{\frac{1}{m}} - b^{\frac{1}{m}}\right)^m \mathrm{e}^{k_n}\right)}\right).$$

Pour résumer, la démonstration se scinde en 4 étapes. Tout d'abord, on établit un résultat classique d'approximation diophantienne (section 5.2). Pour s'appliquer, celui-ci nécessite de construire une suite $(P_{i,r})_{i \in \mathbb{N}}$ de polynômes de $\mathbb{Z}[X]$ de degré donné $\ell \in \mathbb{N}^*$ et dépendant d'un paramètre $r \in \mathbb{N}^*$. Ces polynômes doivent notamment avoir des coefficients ayant une croissance en r au plus exponentielle et doivent être tels que la suite $\left(P_{i,r}\left(\sqrt[n]{\frac{a}{b}}\right)\right)_{i \in \mathbb{N}}$ ait une décroissance en r au moins exponentielle. Ces polynômes vont être construits à partir des approximants de Padé d'un système de fonctions binomiales

(1). Nous donnons ici une constante K un peu meilleure que celle de [5], car d'une part, nous ne considérons pas ici le cas $n = 347$ et, d'autre part, nous n'avons pas majoré le terme $\frac{m(m-1)}{2}$ par $(m-1)^2$ comme le fait Bennett. Cette « amélioration » est cependant marginale car on reste dans le même ordre de grandeur.

étudiés dans le chapitre 2. On verra que la décroissance exponentielle de la suite $\left(P_{i,r}\left(\sqrt[n]{\frac{a}{b}}\right)\right)_{i\in\mathbb{N}}$ sera une conséquence d'une majoration de la fonction reste (section 5.3). En revanche, la croissance contrôlée des coefficients nécessitera, d'une part, de majorer les approximants de Padé (section 5.3) mais surtout, d'autre part, de mener une étude approfondie d'un rationnel $\Delta_{m,n,r}$ nécessaire pour rendre entiers les coefficients de la famille d'approximants (section 5.4). Une fois ces hypothèses vérifiées, le théorème pourra être démontré (section 5.5). Pour finir, nous verrons comment nous pourrons utiliser ce théorème pour achever la démonstration du théorème 1 en raisonnant sur les développements en fractions continuées (section 5.6) à l'image de ce qui a été fait dans la section 4.4.

5.2 Un lemme d'approximation diophantienne

La démonstration du théorème 5.1.1 est basé sur le lemme suivant.

Lemme 5.2.1. — *Soit θ, c, d, C et D des nombres réels strictement positifs tels que $C > 1$ et $D > 1$ et soit ℓ un entier naturel non nul. Supposons que, pour tout entier naturel $r \geq 1$, il existe une suite de polynômes de $\mathbb{Z}[X]$*

$$P_{i,r} = \sum_{j=0}^{\ell} a_{ij}(r)X^j$$

avec $i \in [\![0, \ell]\!]$ tels que

$$\text{la matrice } A_r := (a_{ij}(r))_{(i,j)\in[\![0,\ell]\!]^2} \text{ est inversible} \tag{5.1}$$

$$\forall (i,j) \in [\![0,\ell]\!]^2, \quad |a_{ij}(r)| \leq cC^r \tag{5.2}$$

$$\forall i \in [\![0,\ell]\!], \quad |P_{i,r}(\theta)| \leq dD^{-r} \tag{5.3}$$

Soit t un nombre réel tel que $t > 1$ et $td \geq 1$ et soit p et q des entiers naturels non nuls tels que $q \geq (td)^{-\frac{1}{\ell}}$. Alors, en posant $\delta = \max\left\{|\theta|, \left|\frac{p}{q}\right|, 1\right\}$, on a

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{Kq^{\lambda}}$$

où

$$K := \frac{t}{t-1}\frac{\ell(\ell+1)}{2}\delta^{\ell-1}cC(td)^{\frac{\ln C}{\ln D}}$$

et

$$\lambda := \ell\left(1 + \frac{\ln C}{\ln D}\right).$$

Preuve. — Etant donné que $q \geq (td)^{-\frac{1}{\ell}}$, on est assuré que $tdq^{\ell} \geq 1$ et donc, comme $D > 1$, il existe un unique entier $r \geq 1$ tel que $D^{r-1} \leq tdq^{\ell} < D^r$. On a alors $D^r \leq tdDq^{\ell}$ et donc

$$C^r = D^{r\frac{\ln C}{\ln D}} \leq C(td)^{\frac{\ln C}{\ln D}}q^{\ell\frac{\ln C}{\ln D}}. \tag{5.4}$$

Comme la matrice A_r est inversible, il existe un entier $i \in [\![0,\ell]\!]$ tel que $P_{i,r}\left(\frac{p}{q}\right) \neq 0$ car sinon, le vecteur de composantes 1, $\frac{p}{q}$, $\frac{p^2}{q^2}$, …, $\frac{p^{\ell}}{q^{\ell}}$ serait un vecteur non nul du noyau de A_r. Dès lors, $P_{i,r}\left(\frac{p}{q}\right)$ est de la forme $\frac{N}{q^{\ell}}$ avec $N \in \mathbb{Z}^*$ et donc

$$\frac{1}{q^{\ell}} \leq \left|P_{i,r}\left(\frac{p}{q}\right)\right| \leq \left|P_{i,r}\left(\frac{p}{q}\right) - P_{i,r}(\theta)\right| + |P_{i,r}(\theta)|.$$

Or, par hypothèse, $|P_{i,r}(\theta)| \leq dD^{-r}$ et $D^r > tdq^\ell$ donc

$$\frac{1}{q^\ell} < \left|P_{i,r}\left(\frac{p}{q}\right) - P_{i,r}(\theta)\right| + \frac{1}{tq^\ell}.$$

et ainsi

$$\left|P_{i,r}\left(\frac{p}{q}\right) - P_{i,r}(\theta)\right| > \left(1 - \frac{1}{t}\right)\frac{1}{q^\ell}.$$

Par ailleurs, en utilisant (5.2),

$$\left|P_{i,r}\left(\frac{p}{q}\right) - P_{i,r}(\theta)\right| = \left|\int_{\frac{p}{q}}^{\theta} P'_{i,r}(x)\,\mathrm{d}x\right| = \left|\int_{\frac{p}{q}}^{\theta} \sum_{j=1}^{\ell} j a_{ij}(r) x^{j-1}\,\mathrm{d}x\right| \leq \left|\theta - \frac{p}{q}\right| \sum_{j=1}^{\ell} j c C^r \delta^{j-1}$$

et donc, comme $\delta \geq 1$,

$$\left|P_{i,r}\left(\frac{p}{q}\right) - P_{i,r}(\theta)\right| \leq \frac{\ell(\ell+1)}{2}\delta^{\ell-1} c C^r \left|\theta - \frac{p}{q}\right|.$$

Il s'ensuit que

$$\left|\theta - \frac{p}{q}\right| > \frac{1}{\frac{t}{t-1}\frac{\ell(\ell+1)}{2}\delta^{\ell-1} c C^r q^\ell}.$$

Or, d'après (5.4), $C^r \leq C(td)^{\frac{\ln C}{\ln D}} q^{\ell\frac{\ln C}{\ln D}}$ donc

$$\frac{1}{C^r q^\ell} \geq \frac{1}{C(td)^{\frac{\ln C}{\ln D}} q^{\ell\left(\frac{\ln C}{\ln D}\right)} q^\ell} = \frac{1}{C(td)^{\frac{\ln C}{\ln D}} q^{\ell\left(1+\frac{\ln C}{\ln D}\right)}}$$

ce qui permet de conclure. ■

Pour construire les polynômes $P_{i,r}$ adéquats, nous allons définir les coefficients $a_{ij}(r)$ en fonction d'une certaine famille d'approximants de Padé d'un système de fonctions binomiales.

Plus précisément, dans toute la suite, m et n désignent des entiers naturels tels que $n > m \geq 2$ et $A_1, ..., A_m$ sont les $[\rho_1, ..., \rho_m]$ approximants de Padé du système de fonctions binomiales $(f_{\omega_1}, ..., f_{\omega_m})$ (où $f_\omega : z \mapsto (1-z)^\omega$) qui ont été construits dans le chapitre 2. Nous allons cependant nous restreindre au cas où

$$\forall k \in [\![1, m]\!], \qquad \omega_k = \frac{k-1}{n} \quad \text{et} \quad \rho_k = r + 1$$

où $r \in \mathbb{N}^*$.

Nous considérons, comme en (2.11), la famille de polynômes (A_{ij}) définis par

$$\forall (i,j) \in [\![1, m]\!]^2 \qquad A_{ij}(z) = A_j\left(z \,\middle|\, \begin{matrix} \omega_1 & \cdots & \omega_m \\ \rho_1 + \delta_{i1} & \cdots & \rho_m + \delta_{im} \end{matrix}\right)$$

i.e. dans notre cas

$$A_{ij}(z) = A_j\left(z \,\middle|\, \begin{matrix} 0 & \frac{1}{n} & \cdots & \frac{m-1}{n} \\ r+1+\delta_{i1} & r+1+\delta_{i2} & \cdots & r+1+\delta_{im} \end{matrix}\right). \tag{5.5}$$

Afin d'insister sur la dépendance par rapport au paramètre r, nous noterons, pour tout $r \in \mathbb{N}^*$, ces polynômes $A_{ij}(z, r)$ et, comme dans (2.12), $R_i(z, r)$ la fonction reste associée.

Nous verrons que la condition d'indépendance linéaire exigée par (5.1) sera une conséquence de la proposition 2.3.1.

Pour remplir les conditions (5.2) et (5.3), nous allons à présent borner pour chaque réel $z \in]-\infty\,;0[$, les nombres $R_i(z, r)$ et $A_{ij}(z, r)$.

5.3 Majoration de $|R_i(z,r)|$ et $|A_{ij}(z,r)|$ en fonction de $z<0$

5.3.1 Majoration de $|R_i(z,r)|$

L'expression sous forme intégrale de la fonction reste obtenue dans la proposition 2.2.6 permet d'en déduire une majoration de $|R_i(z,r)|$. On reprend ici le raisonnement de Bennett [5] qui s'appuie sur les propriétés établies par Chudnovsky [7].

Lemme 5.3.1. — *Soit z un réel strictement négatif fixé. Soit*

$$D := \left\{(t_1,t_2,...,t_{m-1}) \in \mathbb{R}^{m-1} \,\middle|\, z \leq t_1 \leq ... \leq t_{m-1} \leq 0\right\}.$$

Alors, en posant $t_0 = z$ et $t_m = 0$,

$$\max_{(t_1,t_2,...,t_{m-1})\in D} \left(\prod_{h=1}^{m} \frac{t_h - t_{h-1}}{1-t_h}\right) = \left((1-z)^{\frac{1}{m}} - 1\right)^m.$$

Preuve. — Soit f la fonction définie sur D par $f(t_1,...,t_{m-1}) = \prod_{h=1}^{m} \frac{t_h - t_{h-1}}{1-t_h}$. Comme f est continue sur le compact D, la fonction f est bornée et atteint ses bornes. Par définition, le minimum de f est 0 atteint sur le bord de D (et seulement sur le bord de D). Dès lors, f atteint son maximum à l'intérieur de D. Or, la fonction f est de classe $\mathcal{C}^1$ sur $\mathring{D}$ donc f atteint son maximum en un point critique de f. Pour tout $(t_1,...,t_{m-1}) \in D$,

$$\begin{aligned}
\frac{\partial f}{\partial t_j}(t_1,...,t_{m-1}) &= \frac{1-t_{j-1}}{(1-t_j)^2} \prod_{\substack{h=1\\h\neq j}}^{m} \frac{t_h - t_{h-1}}{1-t_h} + \frac{-1}{1-t_{j+1}} \prod_{\substack{h=1\\h\neq j+1}}^{m} \frac{t_h - t_{h-1}}{1-t_h} \\
&= \left[\frac{1-t_j}{t_j - t_{j-1}} \times \frac{1-t_{j-1}}{(1-t_j)^2} - \frac{1-t_{j+1}}{t_{j+1}-t_j} \times \frac{1}{1-t_{j+1}}\right] f(t_1,...,t_{m-1}) \\
&= \frac{(1-t_{j-1})(t_{j+1}-t_j) - (t_j - t_{j-1})(1-t_j)}{(t_j - t_{j-1})(1-t_j)(t_{j+1}-t_j)} f(t_1,...,t_{m-1})
\end{aligned}$$

Supposons que f admette en $(t_1,...,t_{m-1}) \in \mathring{D}$ un point critique. Alors, comme f ne s'annule pas sur $\mathring{D}$,

$$\forall j \in [\![1, m-1]\!] \quad (1-t_{j-1})(t_{j+1}-t_j) - (t_j - t_{j-1})(1-t_j) = 0.$$

En posant, pour tout $j \in [\![0,m]\!]$, $x_j = 1 - t_j$, ce qui précède implique que, pour tout $j \in [\![1, m-1]\!]$,

$$x_{j-1}(x_j - x_{j+1}) - (x_{j-1} - x_j)x_j = 0 \quad \text{donc} \quad x_{j-1}x_{j+1} = x_j^2 \quad \text{i.e.} \quad \frac{x_{j+1}}{x_j} = \frac{x_j}{x_{j-1}}.$$

Il s'ensuit que, pour tout $j \in [\![0,m]\!]$, $x_j = x_0 \left(\frac{x_1}{x_0}\right)^j$. En particulier, pour $j = m$, on obtient $1 = x_m = x_0 \left(\frac{x_1}{x_0}\right)^m$ i.e. $\frac{x_1}{x_0} = x_0^{-\frac{1}{m}}$ donc, pour tout $j \in [\![0,m]\!]$, $x_j = x_0^{1-\frac{j}{m}}$ i.e. $t_j = 1 - (1-z)^{-\frac{j}{m}}$.

Ainsi, f admet au plus un point critique dans $\mathring{D}$ donc, comme f admet au moins un point critique, f admet exactement un point critique en $\left(1-(1-z)^{-\frac{j}{m}}\right)_{1\leq j\leq m-1}$ et en ce point f atteint son maximum

sur D. On en déduit que

$$\begin{aligned}\max_{(t_1,t_2,\dots,t_{m-1})\in D}\left(\prod_{h=1}^{m}\frac{t_h-t_{h-1}}{1-t_h}\right) &= f\left(1-(1-z)^{-\frac{1}{m}},\dots,1-(1-z)^{-\frac{m-1}{m}}\right)\\ &= \prod_{h=1}^{m}\frac{(1-z)^{-\frac{h-1}{m}}-(1-z)^{-\frac{h}{m}}}{(1-z)^{-\frac{h}{m}}}\\ &= \prod_{h=1}^{m}\left((1-z)^{\frac{1}{m}}-1\right)\\ &= \left((1-z)^{\frac{1}{m}}-1\right)^m\end{aligned}$$

comme annoncé. ■

On va pouvoir déduire de ce lemme une majoration de la fonction reste en fonction de z.

Proposition 5.3.2. — *Soit $r\in\mathbb{N}^*$. Alors, pour tout $z<0$ et tout $i\in[\![1,m]\!]$,*

$$|R_i(z,r)|\leq\frac{|z|^m}{(m-1)!}\left|1-(1-z)^{\frac{1}{m}}\right|^{mr}.$$

Preuve. — Soit $i\in[\![1,m]\!]$ et $z<0$. Alors, d'après la proposition 2.2.6,

$$R_i(z,r)=R_i\left(z\,\middle|\,\begin{array}{ccc}0 & \cdots & \frac{m-1}{n}\\ r+1+\delta_{i1} & \cdots & r+1+\delta_{im}\end{array}\right)=\int_0^z\int_0^{t_1}\cdots\int_0^{t_{m-2}}R(z\mid t_1\,t_2\cdots t_{m-1})\,\mathrm{d}t_{m-1}\cdots\mathrm{d}t_2\,\mathrm{d}t_1$$

avec

$$\begin{aligned}R(z\mid t_1,t_2,\cdots t_{m-1})=(z-t_1)^{r+\delta_{i1}}(t_1-t_2)^{r+\delta_{i2}}\dots(t_{m-2}-t_{m-1})^{r+\delta_{i(m-1)}}t_{m-1}^{r+\delta_{im}}(1-z)^0(1-t_1)^{\frac{1}{n}-r-1-\delta_{i1}}\dots\\ (1-t_{m-2})^{\frac{1}{n}-r-1-\delta_{i(m-2)}}(1-t_{m-1})^{\frac{1}{n}-r-1-\delta_{i(m-1)}}.\end{aligned}$$

c'est-à-dire, en posant, comme dans le lemme précédent, $t_0=z$ et $t_m=0$

$$\begin{aligned}R(z\mid t_1,t_2,\cdots,t_{m-1}) &= \prod_{h=1}^{m}\left(\frac{t_{h-1}-t_h}{1-t_h}\right)^{r+\delta_{ih}}\prod_{h=2}^{m}(1-t_{h-1})^{\frac{1}{n}-1}\\ &= \frac{t_{i-1}-t_i}{1-t_i}\left[\prod_{h=1}^{m}\left(\frac{t_{h-1}-t_h}{1-t_h}\right)\right]^r\prod_{h=2}^{m}(1-t_{h-1})^{\frac{1}{n}-1}\\ &\leq |z|\left[\prod_{h=1}^{m}\left(\frac{t_{h-1}-t_h}{1-t_h}\right)\right]^r\prod_{h=2}^{m}(1-t_{h-1})^{\frac{1}{n}-1}\end{aligned}$$

car $t_{i-1}-t_i\leq 0-z=|z|$ et $1-t_i\geq 1$.

On déduit alors du lemme 5.3.1 que, pour tous réels t_1, t_2, ..., t_{m-1} tels que $z\leq t_1\leq t_2\leq\cdots\leq t_{m-1}\leq 0$, on a

$$|R(z\mid t_1\,t_2\cdots t_{m-1})|\leq|z|\left((1-z)^{\frac{1}{m}}-1\right)^{mr}\prod_{h=2}^{m}(1-t_{h-1})^{\frac{1}{n}-1}$$

et donc, puisque $\frac{1}{n}-1<0$ et $1-t_{h-1}\geq 1$ pour tout $h\in[\![2,m]\!]$,

$$|R(z\mid t_1\,t_2\cdots t_{m-1})|\leq|z|\left((1-z)^{\frac{1}{m}}-1\right)^{mr}=|z|\left|1-(1-z)^{\frac{1}{m}}\right|^{mr}.$$

Il s'ensuit que

$$|R_i(z)|\leq|z|\left|1-(1-z)^{\frac{1}{m}}\right|^{mr}\left|\int_0^z\int_0^{t_1}\cdots\int_0^{t_{m-2}}\mathrm{d}t_{m-1}\cdots\mathrm{d}t_2\,\mathrm{d}t_1\right|=\left|1-(1-z)^{\frac{1}{m}}\right|^m\frac{|z|^m}{(m-1)!}$$

qui est bien la majoration voulue. ■

5.3.2 Majoration de $|A_{ij}(z,r)|$

La majoration des polynômes A_{ij} est un peu moins immédiate. On va dans ce cas utiliser l'expression des approximants de Padé obtenue à l'aide de la formule des résidus. Rappelons que, d'après (2.8), si ϕ est définie pour tout complexe u, par

$$\phi(u) := \prod_{k=1}^{m} \prod_{h=0}^{\rho_k - 1} (u - \omega_k - h),$$

alors

$$A_k \left(z \,\middle|\, \begin{array}{ccc} \omega_1 & \cdots & \omega_m \\ \rho_1 & \cdots & \rho_m \end{array} \right) = (-1)^{\sigma-1} \Gamma(\rho_1) \cdots \Gamma(\rho_m) \sum_{h=0}^{\rho_k - 1} \frac{(1-z)^h}{\phi'(\omega_k + h)}$$

Ainsi, dans notre cas, on a

$$\forall (i,j) \in [\![1,m]\!]^2 \qquad A_{ij}(z,r) = (-1)^{m(r+1)+1} (r+\delta_{i1})! \cdots (r+\delta_{im})! \sum_{h=0}^{r+\delta_{ij}} \frac{(1-z)^h}{\phi' \left(\frac{j-1}{n} + h \right)}$$

Si on note, pour tout réel ω et tout entier $\rho > 0$,

$$F \left(z \,\middle|\, \begin{array}{c} \omega \\ \rho \end{array} \right) = \prod_{h=0}^{\rho-1} (z - \omega - h)$$

alors il vient que

$$\phi(z) = \prod_{k=1}^{m} F \left(z \,\middle|\, \begin{array}{c} \frac{k-1}{n} \\ r+1+\delta_{ik} \end{array} \right)$$

et

$$\phi'(z) = \sum_{k=1}^{m} F' \left(z \,\middle|\, \begin{array}{c} \frac{k-1}{n} \\ r+1+\delta_{ik} \end{array} \right) \prod_{\substack{\ell=1 \\ \ell \neq k}}^{m} F \left(z \,\middle|\, \begin{array}{c} \frac{\ell-1}{n} \\ r+1+\delta_{i\ell} \end{array} \right).$$

Or, pour tout $h \in [\![0, r+\delta_{ij}]\!]$, tout $\ell \in [\![1,m]\!]$ et tout $k \in [\![1,m]\!]$,

$$F \left(\frac{j-1}{n} + h \,\middle|\, \begin{array}{c} \frac{\ell-1}{n} \\ r+1+\delta_{i\ell} \end{array} \right) = \prod_{s=0}^{r+\delta_{i\ell}} \left(\frac{j-\ell}{n} + h - s \right) = \begin{cases} 0 & \text{si } j = \ell \\ \dfrac{\Gamma\left(\frac{j-\ell}{n} + h + 1 \right)}{\Gamma\left(\frac{j-\ell}{n} + h - r - \delta_{i\ell} \right)} & \text{sinon.} \end{cases}$$

donc

$$\phi' \left(\frac{j-1}{n} + h \right) = F' \left(\frac{j-1}{n} + h \,\middle|\, \begin{array}{c} \frac{j-1}{n} \\ r+1+\delta_{ij} \end{array} \right) \prod_{\substack{\ell=1 \\ \ell \neq j}}^{m} \frac{\Gamma\left(\frac{j-\ell}{n} + h + 1 \right)}{\Gamma\left(\frac{j-\ell}{n} + h - r - \delta_{i\ell} \right)}.$$

De plus,

$$F' \left(\frac{j-1}{n} + h \,\middle|\, \begin{array}{c} \frac{j-1}{n} \\ r+1+\delta_{ij} \end{array} \right) = \sum_{t=0}^{r+\delta_{ij}} \prod_{\substack{s=0 \\ s \neq t}}^{r+\delta_{ij}} (h-s) = \prod_{\substack{s=0 \\ s \neq h}}^{r+\delta_{ij}} (h-s) = (-1)^{r+\delta_{ij}-h} h! (r+\delta_{ij}-h)!$$

donc

$$\phi' \left(\frac{j-1}{n} + h \right) = (-1)^{r+\delta_{ij}-h} h! (r+\delta_{ij}-h)! \prod_{\substack{\ell=1 \\ \ell \neq j}}^{m} \frac{\Gamma\left(\frac{j-\ell}{n} + h + 1 \right)}{\Gamma\left(\frac{j-\ell}{n} + h - r - \delta_{i\ell} \right)}.$$

Il s'ensuit que

$$A_{ij}(z,r) = (-1)^{(m+1)(r+1)+\delta_{ij}} \sum_{h=0}^{r+\delta_{ij}} \alpha_{i,j,h,r}(1-z)^h$$

où

$$\alpha_{i,j,h,r} := (-1)^h \frac{(r+\delta_{i1})! \cdots (r+\delta_{im})!}{h!(r+\delta_{ij}-h)!} \prod_{\substack{\ell=1 \\ \ell \neq j}}^{m} \frac{\Gamma\left(\frac{j-\ell}{n} + h - r - \delta_{i\ell}\right)}{\Gamma\left(\frac{j-\ell}{n} + h + 1\right)} = (-1)^h \binom{r+\delta_{ij}}{h} \prod_{\substack{\ell=1 \\ \ell \neq j}}^{m} \beta_{i,j,h,\ell} \quad (5.6)$$

avec

$$\beta_{i,j,h,\ell} := \frac{\Gamma(r+1+\delta_{i\ell})\Gamma\left(\frac{j-\ell}{n} + h - r - \delta_{i\ell}\right)}{\Gamma\left(\frac{j-\ell}{n} + h + 1\right)}. \quad (5.7)$$

Afin de majorer $A_{ij}(z,r)$ pour $z < 0$, on va montrer que $\beta_{i,j,h,\ell}$ est de l'ordre de grandeur de $\binom{r+\delta_{i\ell}}{h}$. Pour cela, considérons pour tout entier $t \geq 1$, pour tout entier $h \in [\![0,t]\!]$, pour tout $(j,\ell) \in [\![1,m]\!]^2$,

$$K_{j,\ell,h,t} = \left| \frac{\Gamma\left(\frac{j-\ell}{n} + h - t\right)\Gamma(h+1)\Gamma(t-h+1)}{\Gamma\left(\frac{j-\ell}{n} + h + 1\right)} \right|$$

de telle sorte que $|\beta_{i,j,h,\ell}| = \binom{r+\delta_{i\ell}}{h} K_{j,\ell,h,r+\delta_{i\ell}}$.

En utilisant l'égalité

$$\forall z \in \mathbb{C} \setminus \mathbb{Z} \quad \frac{\Gamma(z-n)}{\Gamma(z)} = (-1)^n \frac{\Gamma(-z+1)}{\Gamma(-z+n+1)} \text{ (2)}$$

avec $z = \frac{j-\ell}{n} + h + 1$ et $n = t+1$, on obtient

$$\left| \frac{\Gamma\left(\frac{j-\ell}{n} + h - t\right)}{\Gamma\left(\frac{j-\ell}{n} + h + 1\right)} \right| = \left| \frac{\Gamma\left(\frac{\ell-j}{n} - h\right)}{\Gamma\left(\frac{\ell-j}{n} + t - h + 1\right)} \right|$$

ce qui implique que $K_{j,\ell,h,t} = K_{\ell,j,t-h,t}$. On peut, dès lors, supposer que $\frac{j-\ell}{n} > 0$ c'est-à-dire que $j - \ell = a \in [\![1, m-1]\!]$.

De plus, pour tout $h \in [\![0, t-1]\!]$,

$$\frac{K_{j,\ell,h,t}}{K_{j,\ell,h+1,t}} = \frac{t-h}{t-h-\frac{a}{n}} \times \frac{h+1+\frac{a}{n}}{h+1} > 1$$

et donc

$$\max_{0 \leq h \leq t} K_{j,\ell,h,t} = K_{j,\ell,0,t} = \left| \frac{\Gamma\left(\frac{a}{n} - t\right)\Gamma(t+1)}{\Gamma\left(\frac{a}{n} + 1\right)} \right| := K\left(\frac{a}{n}, t\right). \quad (5.8)$$

Considérons la fonction $g_t := x \mapsto \left|\frac{\Gamma(x-t)}{\Gamma(x+1)}\right| = \frac{1}{x} \prod_{j=1}^{t} \frac{1}{j-x}$. Alors, pour tout $x \in]0\,;1[$,

$$(\ln \circ g_t)''(x) = \frac{1}{x^2} + \sum_{j=1}^{t} \frac{1}{(j-x)^2} > 0$$

(2). Voir, par exemple, [3], identité (3) p. 3.

ce qui assure que g_t est log-convexe et donc convexe sur $]0\,;1[$. Il s'ensuit que

$$\max_{1\le a\le m-1} K\left(\frac{a}{n},t\right)=\max\left\{K\left(\frac{1}{n},t\right),K\left(\frac{m-1}{n},t\right)\right\}. \tag{5.9}$$

De plus, $\frac{K\left(\frac{a}{n},t+1\right)}{K\left(\frac{a}{n},t\right)}=\frac{t+1}{t+1-\frac{a}{n}}$ et l'étude de la fonction $h_t:=x\mapsto x\ln\left(\frac{t+1}{t}\right)-\ln\left(\frac{t+1}{t+1-x}\right)$ sur $[0\,;1]$ montre qu'elle est strictement croissante puis strictement décroissante. Sachant que $h_t(0)=h_t(1)=0$, on en déduit que $h_t(x)>0$ pour tout $x\in]0\,;1[$ et donc, étant donné que $0<\frac{a}{n}<\frac{m}{n}<1$,

$$\frac{K\left(\frac{a}{n},t+1\right)}{K\left(\frac{a}{n},t\right)}<\left(\frac{t+1}{t}\right)^{\frac{a}{n}}.$$

En utilisant le fait que $K\left(\frac{a}{n},1\right)=g_1\left(\frac{a}{n}\right)=\frac{n^2}{a(n-a)}$, on peut alors conclure que

$$K\left(\frac{a}{n},t\right)\le K\left(\frac{a}{n},t-1\right)\left(\frac{t}{t-1}\right)^{\frac{a}{n}}\le K\left(\frac{a}{n},t-2\right)\left(\frac{t}{t-2}\right)^{\frac{a}{n}}\le ...\le\frac{n^2}{a(n-a)}t^{\frac{a}{n}}. \tag{5.10}$$

En posant

$$\Phi_{m,n,t}:=\max\left\{\frac{n^2}{n-1}t^{\frac{1}{n}},\frac{n^2}{(m-1)(n-m+1)}t^{\frac{m-1}{n}}\right\},$$

on déduit de (5.8), (5.9) et (5.10) que

$$\forall h\in[\![0,t]\!],\quad K_{j,\ell,h,t}\le\Phi_{m,n,t}.$$

Par définition de $K_{j,\ell,h,t}$, il s'ensuit que

$$\forall h\in[\![0,r+\delta_{i\ell}]\!],\quad|\beta_{i,j,h,\ell}|\le\Phi_{m,n,r+\delta_{i\ell}}\binom{r+\delta_{i\ell}}{h}. \tag{5.11}$$

Si $i\neq j$ alors

$$|\alpha_{i,j,h,r}|=\binom{r}{h}\prod_{\substack{\ell=1\\\ell\neq j}}^{m}|\beta_{i,j,h,\ell}|\le\binom{r}{h}\prod_{\substack{\ell=1\\\ell\neq j}}^{m}\binom{r+\delta_{i\ell}}{h}\Phi_{m,n,r+\delta_{i\ell}}=\binom{r}{h}^{m-1}\Phi_{m,n,r}^{m-2}\binom{r+1}{h}\Phi_{m,n,r+1}.$$

Or, $\Phi_{m,n,r+1}\le\Phi_{m,n,2r}\le 2^{\frac{m-1}{n}}\Phi_{m,n,r}<2\Phi_{m,n,r}$ et $\binom{r+1}{h}\le(r+1)\binom{r}{h}$ donc

$$|\alpha_{i,j,h,r}|<2(r+1)\binom{r}{h}^{m}\Phi_{m,n,r}^{m-1}$$

et, par suite, pour tout $z<0$,

$$|A_{ij}(z)|\le\sum_{h=0}^{r}|\alpha_{i,j,h,r}|\,(1-z)^h\le 2(r+1)\Phi_{m,n,r}^{m-1}\sum_{h=0}^{r}\binom{r}{h}^{m}(1-z)^h\le 2(r+1)\Phi_{m,n,r}^{m-1}\left[\sum_{h=0}^{r}\binom{r}{h}(1-z)^{\frac{h}{m}}\right]^m$$

c'est-à-dire

$$|A_{ij}(z,r)|\le 2(r+1)\Phi_{m,n,r}^{m-1}\left(1+(1-z)^{\frac{1}{m}}\right)^{mr}. \tag{5.12}$$

Supposons à présent que $i=j$. Alors, pour tout $h\in[\![0,r]\!]$,

$$|\alpha_{i,i,h,r}|=\binom{r+1}{h}\prod_{\substack{\ell=1\\\ell\neq i}}^{m}|\beta_{i,i,h,\ell}|\le\binom{r+1}{h}\prod_{\substack{\ell=1\\\ell\neq i}}^{m}\Phi_{m,n,r+\delta_{i\ell}}\binom{r+\delta_{i\ell}}{h}\le(r+1)\binom{r}{h}^{m}\Phi_{m,n,r}^{m-1}. \tag{5.13}$$

En revanche, pour $h = r + \delta_{ii} = r + 1$, il faut raisonner autrement car (5.11) n'est plus valable puisque $\ell \neq i$ donc $\delta_{i\ell} = 0$.

On écrit alors

$$|\alpha_{i,i,r+1,r}| = \left| \prod_{\substack{\ell=1 \\ \ell \neq i}}^{m} \frac{\Gamma(r+1)\Gamma\left(\frac{i-\ell}{n}+1\right)}{\Gamma\left(\frac{i-\ell}{n}+r+2\right)} \right| = \prod_{\substack{\ell=1 \\ \ell \neq i}}^{m} \frac{\Gamma(r+1)\Gamma\left(\frac{i-\ell}{n}+1\right)}{\Gamma\left(\frac{i-\ell}{n}+r+2\right)}$$

car $\frac{i-\ell}{n} > -\frac{m}{n} > -1$ et, pour tout $x > 0$, $\Gamma(x) > 0$. Ainsi,

$$|\alpha_{i,i,r+1,r}| = \prod_{\substack{\ell=1 \\ \ell \neq i}}^{m} \frac{\Gamma(r+1)}{\Gamma\left(r+1+\frac{i-\ell}{n}+1\right)} \prod_{1 \leq \ell < i} \Gamma\left(\frac{i-\ell}{n}+1\right) \prod_{i < \ell \leq m} \Gamma\left(\frac{i-\ell}{n}+1\right)$$

Comme $r + 1 \geq 2$, la croissance de Γ sur $]2\,;+\infty[$ assure que le premier produit est inférieur à 1 car $\frac{i-\ell}{n} + 1 > 0$. Dans le deuxième produit, pour tout $\ell \in [\![1, i-1]\!]$, $1 < \frac{i-\ell}{n} + 1 < 2$ donc $\Gamma\left(\frac{i-\ell}{n}+1\right) < 1$. Dans le troisième produit, pour tout $\ell \in [\![i+1, m]\!]$, $0 < \frac{i-\ell}{n} + 1 < 1$. Or, pour tout $x \in]0\,;1[$, $\Gamma(x) = \frac{1}{x}\Gamma(x+1)$ et $0 < \Gamma(x+1) < 1$ donc $\Gamma(x) < \frac{1}{x}$. Il s'ensuit que, pour tout $\ell \in [\![i+1, m]\!]$, $\Gamma\left(\frac{i-\ell}{n}+1\right) < \frac{1}{\frac{i-\ell}{n}+1}$. On peut donc dire que

$$|\alpha_{i,i,r+1,r}| < \prod_{i < \ell \leq m} \frac{1}{\frac{i-\ell}{n}+1} \leq \prod_{i < \ell \leq m} \frac{n}{1-m+n} = \left(\frac{n}{n-m+1}\right)^{m-i} \leq \left(\frac{n}{n-m+1}\right)^{m-1}$$

car $\frac{n}{n-m+1} > 1$.

Ainsi, pour tout $z < 0$, en utilisant le fait que $1 - z = \left((1-z)^{\frac{1}{m}}\right)^m \leq \left(1 + (1-z)^{\frac{1}{m}}\right)^m$,

$$|\alpha_{i,i,r+1,r}|\,(1-z)^{r+1} < \left(\frac{n}{n-m+1}\right)^{m-1} (1-z)\left(1+(1-z)^{\frac{1}{m}}\right)^{mr}. \tag{5.14}$$

On déduit alors de (5.13) et (5.14) que

$$\begin{aligned}
|A_{ii}(z,r)| &\leq \sum_{h=0}^{r+1} |\alpha_{i,i,h,r}|\,(1-z)^h \\
&\leq (r+1)\Phi_{m,n,r}^{m-1} \sum_{h=0}^{r} \binom{r}{h}^m (1-z)^h + \left(\frac{n}{n-m+1}\right)^{m-1} (1-z)\left(1+(1-z)^{\frac{1}{m}}\right)^{mr} \\
&\leq (r+1)\Phi_{m,n,r}^{m-1} \left[\sum_{h=0}^{r} \binom{r}{h} (1-z)^{\frac{h}{m}}\right]^m + \left(\frac{n}{n-m+1}\right)^{m-1} (1-z)\left(1+(1-z)^{\frac{1}{m}}\right)^{mr} \\
&\leq \left[(r+1)\Phi_{m,n,r}^{m-1} + \left(\frac{n}{n-m+1}\right)^{m-1} (1-z)\right]\left(1+(1-z)^{\frac{1}{m}}\right)^{mr}
\end{aligned}$$

En remarquant que $r \geq 1$ et $m < n$, on peut dire que

$$\begin{aligned}
\left(\frac{n}{n-m+1}\right)^{m-1} &= \left(\frac{m-1}{n}\right)^{m-1} \left(\frac{n^2}{(m-1)(n-m+1)}\right)^{m-1} \\
&\leq \left(\frac{m-1}{m+1}\right)^{m-1} \Phi_{m,n,r}^{m-1}.
\end{aligned}$$

Or, l'étude de la fonction de la fonction $x \mapsto \left(\frac{x-1}{x+1}\right)^{x-1}$ montre qu'elle est décroissante sur $[2\,;+\infty[$ donc

$$\left(\frac{n}{n-m+1}\right)^{m-1} \leq \frac{1}{3}\Phi_{m,n,r}^{m-1}.$$

et ainsi,

$$|A_{ii}(z,r)| \leq \left[(r+1)+\frac{1-z}{3}\right]\Phi_{m,n,r}^{m-1}\left(1+(1-z)^{\frac{1}{m}}\right)^{mr} \leq \left[1+\frac{1-z}{3(r+1)}\right](r+1)\Phi_{m,n,r}^{m-1}\left(1+(1-z)^{\frac{1}{m}}\right)^{mr}$$

soit encore, comme $r+1 \geq 2$,

$$|A_{ii}(z,r)| \leq \left[1+\frac{1-z}{6}\right](r+1)\Phi_{m,n,r}^{m-1}\left(1+(1-z)^{\frac{1}{m}}\right)^{mr}. \tag{5.15}$$

Les inégalités (5.12) et (5.15) conduisent à la proposition suivante.

Proposition 5.3.3. — *Soit $r \in \mathbb{N}^*$. Si on note*

$$\Phi_{m,n,r} := \max\left\{\frac{n^2}{n-1}r^{\frac{1}{n}}, \frac{n^2}{(m-1)(n-m+1)}r^{\frac{m-1}{n}}\right\}$$

alors

$$\forall (i,j) \in [\![1,m]\!]^2 \quad \forall z<0 \quad |A_{ij}(z,r)| \leq \left(1+\max\left\{1,\frac{1-z}{6}\right\}\right)(r+1)\Phi_{m,n,r}^{m-1}\left(1+(1-z)^{\frac{1}{m}}\right)^{mr}.$$

Après avoir majoré les nombres $|R_i(z,r)|$ et $|A_{ij}(z,r)|$, il reste, pour pouvoir appliquer le lemme 5.2.1, à majorer le plus petit rationnel $\Delta_{m,n,r}$ tel que, pour tout $(i,j) \in [\![1,m]\!]^2$, $\Delta_{m,n,r}A_{ij}$ soit à coefficients non plus rationnels mais entiers. Autrement dit, $\Delta_{m,n,r}$ est le quotient du P.P.C.M. des dénominateurs des coefficients de tous les A_{ij} par le P.G.C.D. des numérateurs de ces mêmes coefficients.

On va voir qu'il s'agit là de la partie la plus délicate de la démonstration de Bennett.

5.4 Majoration de $\Delta_{m,n,r}$

5.4.1 Propriétés arithmétiques des coefficients des A_{ij}

Avant de procéder à la majoration de $\Delta_{m,n,r}$, nous allons étudier certaines propriétés arithmétiques des coefficients des polynômes A_{ij}. Plus précisément, pour tout nombre premier p, nous allons établir une estimation de la valuation $p-$adique des coefficients du polynôme $A_{ij}(z,r)$.

Pour ce faire, nous aurons besoin du lemme suivant dû à Chudnovsky (Lemme 4.5 de [7]).

Lemme 5.4.1. — *Soit u, v et s des entiers tels que $u<v$ et $1 \leq |s| < n$ et soit p un nombre premier ne divisant pas n et tel que $p^2 > \max\{|nu-s|, |nv-s|\}$. Soit $k \in \mathbb{N}$ tel que $kn \equiv s\ [p]$ et $k \leq p$. Alors,*

$$v_p\left((nu-s)(n(u+1)-s)\cdots(nv-s)\right) = \left\lfloor\frac{v-k}{p}\right\rfloor - \left\lfloor\frac{u-1-k}{p}\right\rfloor.$$

Preuve. — Comme aucun des facteurs du produit $(nu-s)(n(u+1)-s)\cdots(nv-s)$ n'est divisible par p^2, il nous faut compter le nombre d'entiers j tels que $u \leq j \leq v$ et $nj - s \equiv 0 \pmod p$ i.e. $nj \equiv s \pmod p \equiv nk \pmod p$. Comme n est premier avec p, ceci équivaut à $j \equiv k \pmod p$. Ainsi, j est de la forme $j = k + p\ell$ avec $\ell \in \mathbb{Z}$ et vérifie $u \leq j \leq v$ i.e. $u - 1 < k + p\ell \leq v$ soit encore $\frac{u-1-k}{p} < \ell \leq \frac{v-k}{p}$. De tels entiers ℓ sont au nombre de $\left\lfloor \frac{v-k}{p} \right\rfloor - \left\lfloor \frac{u-1-k}{p} \right\rfloor$ ce qui permet de conclure. ■

Si $r \in \mathbb{N}^*$, nous noterons désormais

$$\Omega_{m,n,r} = \max\{\sqrt{nr+n+m}, 2n\} \tag{5.16}$$

et nous supposerons jusqu'à la fin de ce paragraphe que p est un nombre premier tel que $p > \Omega_{m,n,r}$. Nous définissons, pour un entier fixé $j \in \{1, 2, ..., m\}$,

$$S_j = \{j - \ell \,|\, 1 \leq \ell \leq m, \ell \neq j\}\,.$$

Comme p est premier avec n, l'application $\bar{x} \mapsto \overline{xp+s}$ est une bijection de $\mathbb{Z}/n\mathbb{Z}$ dans lui-même pour tout $s \in S_j$. De plus, si $s \in S_j$, $s \not\equiv 0\ [n]$ (car $m < n$) donc il existe un unique entier $t(s) \in [\![1, n-1]\!]$ tel que $t(s)p + s \equiv 0\ [n]$ i.e. $t(s)p + s = nu(s)$ pour un certain entier $u(s)$. En outre, si $t(s) = t(s')$ alors comme $t(s)p + s \equiv t(s')p + s'\ [n]$, on a $s \equiv s'[n]$ et ainsi $s = s'$ car $|s - s'| \leq m - 1 < n - 1$. Ainsi, $s \mapsto t(s)$ est une injection de S_j dans $[\![1, n-1]\!]$.

Ainsi, on peut numéroter les éléments de S_j sous la forme s_1, s_2, ..., s_{m-1} de telle sorte que

$$1 \leq t(s_1) < t(s_2) < \cdots < t(s_{m-1}) \leq n - 1.$$

Dans toute la suite, nous adoptons cette numérotation des éléments de S_j et nous notons $t_k := t(s_k)$ et $u_k := u(s_k)$ de telle sorte que

$$u_k = \frac{t_k p + s_k}{n} \quad \text{et} \quad 1 \leq t_1 < t_2 < \cdots < t_{m-1} \leq n - 1. \tag{5.17}$$

On note, de plus, pour tout $(j,k) \in [\![1,m]\!]^2$, tout $r \in \mathbb{N}^*$ et tout $h \in [\![1, r]\!]$,

$$g_{j,k,h,r} := \frac{r!}{\prod_{v=-h}^{r-h} (nv - j + k)} \tag{5.18}$$

et $\psi(j,k)$ l'unique entier de $[\![1, m-1]\!]$ tel que $s_{\psi(j,k)} = j - k$.

Lemme 5.4.2. — *Soit j et k deux entiers de $[\![1,m]\!]$. Alors, pour tout $r \in \mathbb{N}^*$ et tout $h \in [\![1,r]\!]$,*

$$v_p(g_{j,k,h,r}) = \begin{cases} -1 & si\ \left\{\frac{r}{p}\right\} \geq \left\{\frac{h + u_{\psi(j,k)}}{p}\right\}, \\ 0 & sinon. \end{cases}$$

Preuve. — Etant donné que $p^2 > (\Omega_{m,n,r})^2 > r$,

$$v_p(g_{j,k,h,r}) = \sum_{\ell \geq 1} \left\lfloor \frac{r}{p^\ell} \right\rfloor - v_p\left(\prod_{v=-h}^{r-h} (nv - j + k)\right) = \left\lfloor \frac{r}{p} \right\rfloor - v_p\left(\prod_{v=-h}^{r-h} (nv - s_{\psi(j,k)})\right).$$

De plus, p ne divise pas n car $p > \Omega_{m,n,r} \geq 2n$ et, étant donné que $0 \leq h \leq r$,

$$\max\{\left|-nh - s_{\psi(j,k)}\right|, \left|n(r-h) - s_{\psi(j,k)}\right|\} \leq nr + m - 1 < (\Omega_{m,n,r})^2 < p^2.$$

Enfin, par définition, $u_{\psi(j,k)}n = t_{\psi(j,k)}p + s_{\psi(j,k)} \equiv s_{\psi(j,k)}\ [p]$ avec

$$u_{\psi(j,k)} = \frac{t_{\psi(j,k)}p + s_{\psi(j,k)}}{n} \leq \frac{(n-1)p + (m-1)}{n} = p - \frac{p-(m-1)}{n} < p$$

car $p > \Omega_{m,n,r} > n > m$. Ainsi, on peut appliquer le lemme 5.4.1 qui assure que

$$v_p(g_{j,k,h,r}) = \left\lfloor \frac{r}{p} \right\rfloor - \left\lfloor \frac{r-h-u_{\psi(j,k)}}{p} \right\rfloor + \left\lfloor \frac{-h-1-u_{\psi(j,k)}}{p} \right\rfloor.$$

Si p divise $h+1+u_{\psi(j,k)}$ alors

$$\begin{aligned} v_p(g_{j,k,h,r}) &= \frac{r}{p} - \left\{\frac{r}{p}\right\} - \frac{r-h-u_{\psi(j,k)}}{p} + \left\{\frac{r-h-u_{\psi(j,k)}}{p}\right\} - \frac{h+1+u_{\psi(j,k)}}{p} \\ &= \left\{\frac{r-h-u_{\psi(j,k)}}{p}\right\} - \left\{\frac{r}{p}\right\} - \frac{1}{p} \end{aligned}$$

En utilisant le fait que, pour tous réels x et y,

$$\{x-y\} = \begin{cases} \{x\} - \{y\} & \text{si } \{x\} \geq \{y\}, \\ 1 + \{x\} - \{y\} & \text{si } \{x\} < \{y\}. \end{cases} \tag{5.19}$$

on en déduit que, si $\left\{\frac{r}{p}\right\} \geq \left\{\frac{h+u_{\psi(j,k)}}{p}\right\}$ alors

$$v_p(g_{j,k,h,r}) = \left\{\frac{r}{p}\right\} - \left\{\frac{h+u_{\psi(j,k)}}{p}\right\} - \left\{\frac{r}{p}\right\} - \frac{1}{p} = -\left\{\frac{h+u_{\psi(j,k)}}{p}\right\} - \frac{1}{p} \in \left]-2\,;0\right[$$

donc $v_p(g_{j,k,h,r}) = -1$ tandis que si $\left\{\frac{r}{p}\right\} > \left\{\frac{h+u_{\psi(j,k)}}{p}\right\}$ alors

$$v_p(g_{j,k,h,r}) = 1 + \left\{\frac{r}{p}\right\} - \left\{\frac{h+u_{\psi(j,k)}}{p}\right\} - \left\{\frac{r}{p}\right\} - \frac{1}{p} = 1 - \left\{\frac{h+u_{\psi(j,k)}}{p}\right\} - \frac{1}{p} \in \left]-1\,;1\right[$$

et ainsi $v_p(g_{j,k,h,r}) = 0$.

Si p ne divise pas $h+1+u_{\psi(j,k)}$ alors, en utilisant le fait que, pour tout $x \in \mathbb{R}\setminus\mathbb{Z}$, $\{-x\} = 1-\{x\}$,

$$\begin{aligned} v_p(g_{j,k,h,r}) &= \frac{r}{p} - \left\{\frac{r}{p}\right\} - \frac{r-h-u_{\psi(j,k)}}{p} + \left\{\frac{r-h-u_{\psi(j,k)}}{p}\right\} - \frac{h+1+u_{\psi(j,k)}}{p} - \left\{\frac{-h-1-u_{\psi(j,k)}}{p}\right\} \\ &= \left\{\frac{r-h-u_{\psi(j,k)}}{p}\right\} + \left\{\frac{h+1+u_{\psi(j,k)}}{p}\right\} - \frac{1}{p} - \left\{\frac{r}{p}\right\} - 1. \end{aligned}$$

Comme p ne divise pas $h+1+u_{\psi(j,k)}$, on peut écrire $h+1+u_{\psi(j,k)} = Qp+R$ avec $1 \leq R \leq p-1$ et alors

$$\left\{\frac{h+1+u_{\psi(j,k)}}{p}\right\} - \frac{1}{p} = \frac{R}{p} - \frac{1}{p} = \frac{R-1}{p} = \left\{\frac{h+u_{\psi(j,k)}}{p}\right\}$$

car $R-1 \geq 0$. Ainsi,

$$v_p(g_{j,k,h,r}) = \left\{\frac{r-h-u_{\psi(j,k)}}{p}\right\} + \left\{\frac{h+u_{\psi(j,k)}}{p}\right\} - \left\{\frac{r}{p}\right\} - 1$$

et la conclusion est une conséquence directe de (5.19). ■

On prolonge la définition des nombres s_k, $\psi(j,k)$, t_k et u_k en posant

$$s_0 = t_0 = u_0 = \psi(j,j) = 0 \quad \text{pour tout } 1 \leq j \leq m \tag{5.20}$$

$$s_{\ell+m} = s_\ell \quad \text{et} \quad t_{\ell+m} = t_\ell + n \quad \text{pour tout } \ell \in [\![0, m-1]\!] \tag{5.21}$$

$$u_{\ell+m} = \frac{(t_\ell + n)p + s_\ell}{n} = u_\ell + p \quad \text{pour tout } \ell \in [\![0, m-1]\!] \tag{5.22}$$

On définit, de plus, pour tout $k \in [\![1, m]\!]$, l'intervalle $I_k = \left[1 - \frac{u_k}{p},\ 1 - \frac{u_{k-1}}{p}\right[$.

Lemme 5.4.3. — *La famille $(I_k)_{k\in[\![1,m]\!]}$ forme un recouvrement disjoint de $[0,\ 1[$.*

Preuve. — Remarquons que

$$\forall k \in [\![1, m]\!] \quad u_{k+1} - u_k = \frac{t_{k+1}p + s_{k+1}}{n} - \frac{t_k p + s_k}{n} = \frac{(t_{k+1} - t_k)p + s_{k+1} - s_k}{n}.$$

Or, d'après (5.17) et (5.22), pour tout $k \in [\![1, m]\!]$, $t_{k+1} - t_k \geq 1$ et, de plus, $|s_{k+1} - s_k| \leq m - 1$ donc

$$u_{k+1} - u_k > \frac{p-m}{n} > \frac{2n-m}{n} > 1 \tag{5.23}$$

car $m < n$. Ainsi,

$$0 = u_0 < u_1 < \cdots < u_{m-1} < u_m = p$$

donc

$$0 = 1 - \frac{u_m}{p} < 1 - \frac{u_{m-1}}{p} < \cdots < 1 - \frac{u_1}{p} < 1 - \frac{u_0}{p} = 1 \tag{5.24}$$

ce qui achève la démonstration. ■

Lemme 5.4.4. — *Soit $(i,j) \in [\![1,m]\!]^2$, $r \in \mathbb{N}^*$ et $h \in [\![0, r + \delta_{ij}]\!]$. Si $\alpha_{i,j,h,r}$ est défini comme en (5.6) alors, pour tout nombre premier $p > \Omega_{m,n,r}$*

$$v_p(\alpha_{i,j,h,r}) = 1 - N_{i,j,h,p}$$

où

$$N_{i,j,h,p} = \text{Card}\left\{\ell \in [\![1,m]\!] \;\middle|\; \left\{\frac{r+\delta_{i\ell}}{p}\right\} \geq \left\{\frac{h + u_{\psi(j,\ell)}}{p}\right\}\right\}.$$

En particulier, $v_p(\alpha_{i,j,h,r}) \geq 1 - m$.

Preuve. — Soit $\ell \in [\![1,m]\!]$. En appliquant l'égalité

$$\forall k \in \mathbb{N} \quad \forall z \in \mathbb{C} \setminus \{-\mathbb{N}\} \quad \Gamma(z+k) = \left[\prod_{w=0}^{k-1}(z+w)\right]\Gamma(z)\ ^{(3)},$$

à $z = \frac{j-\ell}{n} + h - r - \delta_{i\ell}$ et $k = r + 1 + \delta_{i\ell}$, on obtient

$$\begin{aligned}
\Gamma\left(\frac{j-\ell}{n} + h + 1\right) &= \left[\prod_{w=0}^{r+\delta_{i\ell}}\left(\frac{j-\ell}{n} + h - r - \delta_{i\ell} + w\right)\right]\Gamma\left(\frac{j-\ell}{n} + h - r - \delta_{i\ell}\right) \\
&= \frac{1}{n^{r+1+\delta_{i\ell}}}\left[\prod_{w=0}^{r+\delta_{i\ell}}(j - \ell + (h - r - \delta_{i\ell} + w)n)\right]\Gamma\left(\frac{j-\ell}{n} + h - r - \delta_{i\ell}\right) \\
&= \frac{1}{n^{r+1+\delta_{i\ell}}}\left[\prod_{v=-h}^{r+\delta_{i\ell}-h}(j - \ell - nv)]\right]\Gamma\left(\frac{j-\ell}{n} + h - r - \delta_{i\ell}\right)
\end{aligned}$$

(3). Voir, par exemple, [3] formule (2) p. 3.

On déduit alors de (5.7) que

$$\beta_{i,j,h,\ell} = \frac{\Gamma(r+1+\delta_{i\ell})n^{r+1+\delta_{i\ell}}}{\prod\limits_{v=-h}^{r+\delta_{i\ell}-h}(j-\ell-nv)} = (-n)^{r+1+\delta_{i\ell}}\frac{(r+\delta_{i\ell})!}{\prod\limits_{v=-h}^{r+\delta_{i\ell}-h}(nv-j+\ell)}$$

i.e. avec la notation (5.18)

$$\beta_{i,j,h,\ell} = (-n)^{r+1+\delta_{i\ell}} g_{j,\ell,h,r+\delta_{i\ell}}.$$

Il suit alors de (5.6) que

$$\begin{aligned}\alpha_{i,j,h,r} &= (-1)^h\binom{r+\delta_{ij}}{h}(-n)^{\left(\sum\limits_{\substack{\ell=1\\ \ell\neq j}}^{m} r+1+\delta_{i\ell}\right)}\prod_{\substack{\ell=1\\ \ell\neq j}}^{m} g_{j,\ell,h,r+\delta_{i\ell}}\\ &= (-1)^h\binom{r+\delta_{ij}}{h}(-n)^{(m-1)(r+1)+1-\delta_{ij}}\prod_{\substack{\ell=1\\ \ell\neq j}}^{m} g_{j,\ell,h,r+\delta_{i\ell}}\end{aligned}$$

soit finalement

$$\alpha_{i,j,h,r} = \pm\binom{r+\delta_{ij}}{h}n^{mr+m-r-\delta_{ij}}\prod_{\substack{\ell=1\\ \ell\neq j}}^{m} g_{j,\ell,h,r+\delta_{i\ell}}. \tag{5.25}$$

Etant donné que $p > \Omega_{m,n,r} \geq 2n$, p ne divise pas n ce qui implique que

$$v_p(\alpha_{i,j,h,r}) = v_p\left(\binom{r+\delta_{ij}}{h}\right) + \sum_{\substack{\ell=1\\ \ell\neq j}}^{m} v_p(g_{j,\ell,h,r+\delta_{i\ell}}). \tag{5.26}$$

Or, comme $p^2 > nr+n+m > r+1 \geq h$, p^2 ne divise ni $r+\delta_{ij}$, ni h, ni $r+\delta_{ij}-h$ donc

$$v_p\left(\binom{r+\delta_{ij}}{h}\right) = \left\lfloor\frac{r+\delta_{ij}}{p}\right\rfloor - \left\lfloor\frac{h}{p}\right\rfloor - \left\lfloor\frac{r+\delta_{ij}-h}{p}\right\rfloor = -\left\{\frac{r+\delta_{ij}}{p}\right\} + \left\{\frac{h}{p}\right\} + \left\{\frac{r+\delta_{ij}-h}{p}\right\}$$

et ainsi, en utilisant (5.19),

$$v_p\left(\binom{r+\delta_{ij}}{h}\right) = \begin{cases} 0 & \text{si } \left\{\dfrac{r+\delta_{ij}}{p}\right\} \geq \left\{\dfrac{h}{p}\right\},\\ 1 & \text{sinon.}\end{cases} \tag{5.27}$$

Supposons que $\left\{\dfrac{r+\delta_{ij}}{p}\right\} \geq \left\{\dfrac{h}{p}\right\}$. On déduit alors du lemme 5.4.2, de (5.26) et de (5.27) que

$$v_p(\alpha_{i,j,h,r}) = -\text{Card}\left\{\ell\in[\![1,m]\!]\;\middle|\;\ell\neq j \text{ et } \left\{\frac{r+\delta_{i\ell}}{p}\right\} \geq \left\{\frac{h+u_{\psi(j,\ell)}}{p}\right\}\right\}$$

De plus, étant donné que, d'après (5.20), $u_{\psi(j,j)} = u_0 = 0$, $\left\{\dfrac{r+\delta_{ij}}{p}\right\} \geq \left\{\dfrac{h+u_{\psi(j,j)}}{p}\right\}$ donc

$$v_p(\alpha_{i,j,h,r}) = 1 - \text{Card}\left\{\ell\in[\![1,m]\!]\;\middle|\;\left\{\frac{r+\delta_{i\ell}}{p}\right\} \geq \left\{\frac{h+u_{\psi(j,\ell)}}{p}\right\}\right\}$$

Supposons ensuite que $\left\{\frac{r+\delta_{ij}}{p}\right\} < \left\{\frac{h}{p}\right\}$. Dans ce cas, le lemme 5.4.2, (5.26) et (5.27) conduisent à

$$v_p(\alpha_{i,j,h,r}) = 1 - \mathrm{Card}\left\{\ell \in [\![1,m]\!] \;\middle|\; \ell \neq j \text{ et } \left\{\frac{r+\delta_{i\ell}}{p}\right\} \geq \left\{\frac{h+u_{\psi(j,\ell)}}{p}\right\}\right\}$$

et, comme $\left\{\frac{r+\delta_{ij}}{p}\right\} < \left\{\frac{h+u_{\psi(j,j)}}{p}\right\}$,

$$v_p(\alpha_{i,j,h,r}) = 1 - \mathrm{Card}\left\{\ell \in [\![1,m]\!] \;\middle|\; \left\{\frac{r+\delta_{i\ell}}{p}\right\} \geq \left\{\frac{h+u_{\psi(j,\ell)}}{p}\right\}\right\}$$

Ainsi, dans tous les cas, $v_p(\alpha_{i,j,h,r}) = 1 - N_{i,j,h,p}$ où $N_{i,j,h,p}$ est tel qu'annoncé. ■

Ces différents lemmes techniques étant démontrés, nous sommes en mesure de prouver le principal résultat de ce paragraphe qui est la proposition suivante.

Proposition 5.4.5. — *Soit μ et r des entiers strictement positifs tels que $m > \mu$ et soit p un nombre premier tel que $p > \Omega_{m,n,r}$. S'il existe trois entiers i, j et h tels que $(i,j) \in [\![1,m]\!]^2$, $h \in [\![0, r+\delta_{ij}]\!]$ et $v_p(\alpha_{i,j,h,r}) = -\mu$ où $\alpha_{i,j,h,r}$ est défini en (5.6) alors*

$$\left\{\frac{r}{p}\right\} \geq \min_{1\leq\ell\leq m}\left(\frac{u_{\ell+\mu} - u_\ell - 1}{p}\right).$$

Preuve. — Supposons qu'il existe trois entiers i, j et h tels que $(i,j) \in [\![1,m]\!]^2$, $h \in [\![0, r+\delta_{ij}]\!]$ et $v_p(\alpha_{i,j,h,r}) = -\mu$. D'après le lemme 5.4.3, il existe un unique $\kappa \in [\![1,m]\!]$ tel que $\left\{\frac{h}{p}\right\} \in I_\kappa = \left[1 - \frac{u_\kappa}{p}\,;1 - \frac{u_{\kappa-1}}{p}\right[$. Montrons que

$$\left\{\frac{h+u_\kappa}{p}\right\} < \left\{\frac{h+u_{\kappa+1}}{p}\right\} < \cdots < \left\{\frac{h+u_{m-1}}{p}\right\} < \left\{\frac{h+u_0}{p}\right\} < \left\{\frac{h+u_1}{p}\right\} < \cdots < \left\{\frac{h+u_{\kappa-1}}{p}\right\} \tag{5.28}$$

En effet, étant donné que $\left\{\frac{h}{p}\right\} < 1 - \frac{u_{\kappa-1}}{p}$, on déduit de (5.24) que, pour tout entier $\ell \in [\![0, \kappa-1]\!]$, $\left\{\frac{h}{p}\right\} < 1 - \frac{u_\ell}{p}$ et donc $\left\{\frac{h}{p}\right\} + \left\{\frac{u_\ell}{p}\right\} = \left\{\frac{h}{p}\right\} + \frac{u_\ell}{p} < 1$. Dès lors, pour tout entier $\ell \in [\![0, \kappa-1]\!]$,

$$\left\{\frac{h+u_\ell}{p}\right\} = \left\{\frac{h}{p}\right\} + \frac{u_\ell}{p} \tag{5.29}$$

et, comme la suite (u_ℓ) est strictement croissante,

$$\left\{\frac{h+u_0}{p}\right\} < \left\{\frac{h+u_1}{p}\right\} < \cdots < \left\{\frac{h+u_{\kappa-1}}{p}\right\} \tag{5.30}$$

ce qui démontre (5.28) dans le cas où $\kappa = m$. Par ailleurs, si $\kappa < m$, étant donné que $\left\{\frac{h}{p}\right\} \geq 1 - \frac{u_\kappa}{p}$, on a d'après (5.24), pour tout $\ell \in [\![\kappa, m-1]\!]$,

$$\left\{\frac{h}{p}\right\} + \left\{\frac{u_\ell}{p}\right\} = \left\{\frac{h}{p}\right\} + \frac{u_\ell}{p} \geq 1 - \frac{u_\kappa}{p} + \frac{u_\ell}{p} \geq 1$$

et donc

$$\left\{\frac{h}{p}+\frac{u_\ell}{p}\right\}=\left\{\frac{h}{p}\right\}+\left\{\frac{u_\ell}{p}\right\}-1=\left\{\frac{h}{p}\right\}+\frac{u_\ell}{p}-1. \tag{5.31}$$

Ainsi, comme précédemment,

$$\left\{\frac{h+u_\kappa}{p}\right\}<\left\{\frac{h+u_{\kappa+1}}{p}\right\}<\cdots<\left\{\frac{h+u_{m-1}}{p}\right\}. \tag{5.32}$$

De plus,

$$\left\{\frac{h+u_{m-1}}{p}\right\}=\left\{\frac{h}{p}\right\}+\frac{u_{m-1}}{p}-1<\left\{\frac{h}{p}\right\}=\left\{\frac{h+u_0}{p}\right\}$$

car $u_0=0$ ce qui, combiné avec (5.30) et (5.32), achève de démontrer (5.28).

Par hypothèse, $v_p(\alpha_{i,j,h,\ell})=-\mu$ donc, d'après le lemme 5.4.4, $N_{i,j,h,p}=\mu+1$ i.e. il y a exactement $\mu+1$ entiers $\ell\in[\![1,m]\!]$ tels que $\left\{\frac{h+u_{\psi(j,\ell)}}{p}\right\}\leq\left\{\frac{r+\delta_{i\ell}}{p}\right\}$. Si on note $\bar{x}$ le reste d'un entier x modulo m et ℓ_0 l'unique entier de $[\![1,m]\!]$ tel que $\psi(j,\ell_0)=\overline{\kappa+\mu}$, on déduit de (5.28) que

$$\left\{\frac{r+\delta_{i\ell_0}}{p}\right\}\geq\left\{\frac{h+u_{\overline{\kappa+\mu}}}{p}\right\}$$

Si $\overline{\kappa+\mu}\in[\![0,\kappa-1]\!]$ alors $\kappa+\mu=m+\overline{\kappa+\mu}$ car $\mu\in[\![0,m-1]\!]$ et on déduit de (5.29) que

$$\left\{\frac{h+u_{\overline{\kappa+\mu}}}{p}\right\}=\left\{\frac{h}{p}\right\}+\frac{u_{\overline{\kappa+\mu}}}{p}=\left\{\frac{h}{p}\right\}+\frac{u_{\kappa+\mu}}{p}-1$$

car $u_{\kappa+\mu}=u_{\overline{\kappa+\mu}+m}=u_{\overline{\kappa+\mu}}+p$ d'après (5.22).

Si $\overline{\kappa+\mu}\in[\![\kappa,m-1]\!]$ alors $\overline{\kappa+\mu}=\kappa+\mu$ car $\mu<m$ et on déduit de (5.31) que

$$\left\{\frac{h+u_{\overline{\kappa+\mu}}}{p}\right\}=\left\{\frac{h}{p}\right\}+\frac{u_{\overline{\kappa+\mu}}}{p}-1=\left\{\frac{h}{p}\right\}+\frac{u_{\kappa+\mu}}{p}-1.$$

Ainsi, dans tous les cas,

$$\left\{\frac{r+\delta_{i\ell_0}}{p}\right\}\geq\left\{\frac{h}{p}\right\}+\frac{u_{\kappa+\mu}}{p}-1$$

et, comme $\left\{\frac{h}{p}\right\}\in I_\kappa$, $\left\{\frac{h}{p}\right\}\geq 1-\frac{u_\kappa}{p}$ donc

$$\left\{\frac{r}{p}\right\}+\frac{1}{p}\geq\left\{\frac{r+\delta_{i\ell_0}}{p}\right\}\geq\frac{u_{\kappa+\mu}-u_\kappa}{p}$$

i.e.

$$\left\{\frac{r}{p}\right\}\geq\frac{u_{\kappa+\mu}-u_\kappa-1}{p}\geq\min_{\ell\in[\![1,m]\!]}\left(\frac{u_{\ell+\mu}-u_\ell-1}{p}\right)$$

ce qui achève la démonstration. ■

Si $k\in[\![1,m-1]\!]$, t_k est défini comme l'unique entier appartenant à $[\![1,n-1]\!]$ tel que $t_kp+s_k\equiv 0\ [n]$. Si p' est un nombre premier tel que $p'\equiv p\ [n]$ alors on a aussi $t_kp'+s_k\equiv 0\ [n]$. Ceci restant vrai pour toutes les valeurs de $k\in[\![0,2m-1]\!]$ d'après (5.21), on en déduit que les nombres t_k restent inchangés lorsque p décrit une même classe modulo n. On peut donc définir, pour tout $a\in[\![1,n-1]\!]$,

$$d_{a,\mu}:=\min_{1\leq k\leq m}(t_{k+\mu}-t_k) \tag{5.33}$$

les t_k étant choisis pour une valeur quelconque du nombre premier p tel que $p \equiv a\ [n]$. De plus, d'après la preuve de la proposition précédente, si $v_p(\alpha_{i,j,h,r}) = -\mu$ alors

$$\left\{\frac{r+\delta_{i\ell_0}}{p}\right\} \geq \frac{u_{\kappa+\mu}-u_\kappa}{p} = \frac{t_{\kappa+\mu}-t_\kappa}{n} + \frac{s_{\kappa+\mu}-s_\kappa}{pn}$$

et comme $|s_{\kappa+\mu} - s_\kappa| < m$ et $m < n$, il s'ensuit que

$$\left\{\frac{r+\delta_{i\ell_0}}{p}\right\} > \frac{d_{a,\mu}}{n} - \frac{1}{p}.$$

En particulier, si p ne divise ni $r+1$ ni $r+2$ alors $\left\{\frac{r+2}{p}\right\} = \left\{\frac{r+1}{p}\right\} + \frac{1}{p} = \left\{\frac{r}{p}\right\} + \frac{2}{p}$ donc, si $i = \ell_0$ alors $\left\{\frac{r+2}{p}\right\} > \frac{d_{a,\mu}}{n}$ et, si $i \neq \ell_0$ alors $\left\{\frac{r+2}{p}\right\} > \frac{d_{a,\mu}}{n} + \frac{1}{p}$. On en déduit le corollaire suivant.

Corollaire 5.4.6. — *Soit μ et r des entiers strictement positifs tels que $m > \mu$. Soit p un nombre premier tel que $p > \Omega_{m,n,r}$ et $p \equiv a\ [n]$ avec $a \in [\![1, n-1]\!]$. Si $v_p(\alpha_{i,j,h,r}) = -\mu$ pour un certain $h \in [\![0, r+\delta_{ij}]\!]$ alors ou bien p divise $(r+1)(r+2)$ ou bien*

$$\left\{\frac{r+2}{p}\right\} > \frac{d_{a,\mu}}{n}.$$

Par la suite, nous allons avoir besoin de calculer les nombres $d_{a,\mu}$ pour $a \in [\![1, n-1]\!]$ et $\mu \in [\![1, m-1]\!]$. Pour simplifier ces calculs, nous pouvons faire deux remarques.

Tout d'abord, pour μ et a fixés, l'entier $d_{a,\mu}$ ne dépend pas du paramètre j. Pour le voir, notons provisoirement $t_{k,j}$ les nombres t_k qui dépendent du paramètre j et $d_{a,\mu,j} = \min\limits_{1\leq k\leq m}(t_{k+\mu,j} - t_{k,j})$. Posons

$$\widetilde{S_j} = \{j - \ell \,|\, \ell \in [\![1, m]\!]\} = S_j \cup \{0\}$$

et, pour p un nombre premier tel que $p \equiv a\ [n]$,

$$T_{j,p} = \left\{\theta \in \mathbb{Z} \,\middle|\, \text{ il existe } s \in \widetilde{S_j} \text{ tel que } \theta p + s \equiv 0\ [n]\right\}.$$

Ecrivons $T_{j,p}$ comme une suite ordonnée indexée par $\mathbb{Z}$: $T_{j,p} = (\theta_{k,j})_{k\in\mathbb{Z}}$. Par définition, si $k \in [\![0, m]\!]$ alors $\theta_{k,j} = t_{k,j}$. En se souvenant que l'application $s_k \in S_j \mapsto t_k \in [\![1, n-1]\!]$ est injective, il est clair que l'application $s_k \in \widetilde{S_j} \mapsto t_k \in [\![1, n]\!]$ est également injective. Ainsi, si $k \in \mathbb{Z}$ s'écrit $k = Qm + R$ avec $R \in [\![1, m]\!]$ alors $\theta_{k,j} = t_{R,j} + Qn$. Il s'ensuit que

$$\{t_{k+\mu,j} - t_{k,j} \,|\, k \in [\![1, m]\!]\} = \{\theta_{k+\mu,j} - \theta_{k,j} \,|\, k \in \mathbb{Z}\}. \tag{5.34}$$

Comme le nombre premier p ne divise pas n, p est inversible modulo n. Notons $\tilde{p} \in [\![1, n-1]\!]$ l'entier tel que $p\tilde{p} \equiv 1\ [n]$. Alors,

$$\begin{aligned}\theta \in T_{j+1,p} &\Leftrightarrow \exists s \in \widetilde{S_{j+1}}\ \ \theta p + s \equiv 0\ [n] \Leftrightarrow \exists \ell \in [\![1, m]\!]\ \ \theta p + j + 1 - \ell \equiv 0\ [n] \\ &\Leftrightarrow \exists \ell \in [\![1, m]\!]\ \ (\theta + \tilde{p})p + j - \ell \equiv 0\ [n] \Leftrightarrow \exists s' \in \widetilde{S_j}\ \ (\theta + \tilde{p})p + s' \equiv 0\ [n] \\ &\Leftrightarrow \theta + \tilde{p} \in T_{j,p}.\end{aligned}$$

Ainsi, $T_{j+1,p} = T_{j,p} - \tilde{p}$ donc

$$\{\theta_{k+\mu,j+1} - \theta_{k,j+1} \,|\, k \in \mathbb{Z}\} = \{\theta_{k+\mu,j} - \theta_{k,j} \,|\, k \in \mathbb{Z}\} \tag{5.35}$$

On déduit alors de (5.34) et (5.35) que $\{t_{k+\mu,j} - t_{k,j} \,|\, k \in [\![1,m]\!]\} = \{t_{k+\mu,j+1} - t_{k,j+1} \,|\, k \in [\![1,m]\!]\}$ et donc $d_{a,\mu,j} = d_{a,\mu,j+1}$ ce qui montre, par récurrence, l'indépendance de $d_{a,\mu,j}$ par rapport à j.

La seconde remarque est la suivante. Si $(a_1, a_2) \in [\![1, n-1]\!]^2$ sont tels que $a_1 \equiv -a_2\ [n]$ alors $d_{a_1,\mu} = d_{a_2,\mu}$.

En effet, considérons deux nombres premiers p_1 et p_2 tels que $p_1 \equiv a_1\ [n]$ et $p_2 \equiv a_2\ [n]$. Alors,

$$\theta \in T_{j,p_1} \Leftrightarrow \exists s \in \widetilde{S_j}\ \ \theta p_1 + s \equiv 0\ [n] \Leftrightarrow \exists s \in \widetilde{S_j}\ \ (-\theta)p_2 + s \equiv 0\ [n] \Leftrightarrow -\theta \in T_{j,p_2}$$

donc $T_{j,p_1} = -T_{j,p_2}$ et ainsi, en faisant apparaître cette fois la dépendance des $t_k = t_{k,p}$ par rapport à p,

$$d_{a_1,\mu} = \min_{k\in\mathbb{Z}}(\theta_{k+\mu,p_1} - \theta_{k,p_1}) = \min_{k\in\mathbb{Z}}(-\theta_{k,p_1} - (-\theta_{k+\mu,p_1})) = \min_{k'\in\mathbb{Z}}(\theta_{k'+\mu,p_2} - \theta_{k',p_2}) = d_{a_2,\mu}.$$

Ces deux observations nous permettent de calculer $d_{a,\mu}$ en ne considérant que les valeurs de $a \in \left[\!\left[1, \dfrac{n-1}{2}\right]\!\right]$. De plus si on note $\tilde{a} \in [\![1, n-1]\!]$ l'inverse de a modulo n alors, pour le choix $j = 1$, on peut définir les nombres $t'_k \in [\![1, n-1]\!]$ tels que $t'_k \equiv \tilde{a}k\ [n]$ pour $1 \leq k \leq m-1$ et les t_k sont alors les t'_k ordonnés par ordre croissant (avec, comme auparavant, $t_0 = 0$ et $t_{\ell+m} = t_\ell + n$ pour $\ell \in [\![0, m-1]\!]$).

A titre d'exemple, donnons les valeurs de $d_{a,\mu}$ pour $n = 17$ et $m = \left\lfloor \dfrac{m-1}{3} \right\rfloor = 6$. On a alors $a \in [\![1, 8]\!]$ et $\mu \in [\![1, 5]\!]$. Détaillons les calculs pour $a = 1$ et $a = 2$.

Pour $a = 1$, $\tilde{a} = 1$ et donc $t_k = k$ pour tout $k \in [\![1, 5]\!]$ et, ainsi, pour tout $\mu \in [\![1, 5]\!]$, $d_{1,\mu} = \mu$.

Pour $a = 2$, $\tilde{a} = 9$ et donc t'_k est le reste de $9k$ modulo 17 ce qui donne la liste suivante pour les t_k $(0 \leq k \leq 10)$:

$$0 \quad 1 \quad 2 \quad 9 \quad 10 \quad 11 \quad 17 \quad 18 \quad 19 \quad 26 \quad 27.$$

Il s'ensuit que $d_{2,1} = 1 - 0 = 1$, $d_{2,2} = 2 - 0 = 2$, $d_{2,3} = 17 - 9 = 8$, $d_{2,4} = 18 - 9 = 9$, $d_{2,5} = 19 - 9 = 10$.

On raisonne de même pour les autres valeurs de a et on aboutit au tableau suivant.

	$d_{1,\alpha}$	$d_{2,\alpha}$	$d_{3,\alpha}$	$d_{4,\alpha}$	$d_{5,\alpha}$	$d_{6,\alpha}$	$d_{7,\alpha}$	$d_{8,\alpha}$
$\alpha = 1$	1	1	1	1	1	1	1	1
$\alpha = 2$	2	2	5	4	4	5	5	4
$\alpha = 3$	3	8	6	5	7	8	7	6
$\alpha = 4$	4	9	11	9	10	11	10	8
$\alpha = 5$	5	10	12	13	13	14	12	10

Remarquons, pour finir ce paragraphe, que, quelles que soient les valeurs de a et μ, $d_{a,\mu} < n$ donc $0 < \dfrac{d_{a,\mu}}{n} < 1$ et ainsi, pour tout $r \in \mathbb{N}^*$, en notant $N = \left\lfloor \frac{r+2}{p} \right\rfloor$

$$\frac{d_{a,\mu}}{n} < \left\{\frac{r+2}{p}\right\} \Leftrightarrow N + \frac{d_{a,\mu}}{n} < \frac{r+2}{p} < N+1 \Leftrightarrow \frac{r+2}{N+1} < p < \frac{r+2}{N + \frac{d_{a,\mu}}{n}}. \tag{5.36}$$

Il s'ensuit, grâce au corollaire 5.4.6 que le produit des nombres premiers $p > \Omega_{m,n,r}$ qui divisent le dénominateur d'un $a_{i,j,h,r}$ donné mais ne divise pas $(r+1)(r+2)$, en tenant compte des multiplicités, divise

$$\exp\left(\sum_{a=1}^{n-1}\sum_{\mu=1}^{m-1}\sum_{N=0}^{N_0}\left(\theta\left(\frac{r+2}{N + \frac{d_{a,\mu}}{n}}, n, a\right) - \theta\left(\frac{r+2}{N+1}, n, a\right)\right)\right) \tag{5.37}$$

où

$$\theta(x,n,a)=\sum_{\substack{p\leq x\\ p\equiv a\ [n]}}\ln p$$

et N_0 désigne le plus petit entier strictement positif tel que $\dfrac{r+2}{N_0+1}<\sqrt{nr+n+m}$ car, si $N>N_0$ alors, d'après (5.36), $p<\dfrac{r+2}{N+\frac{d_{a,\mu}}{n}}<\dfrac{r+2}{N_0+1}<\sqrt{nr+n+1}<\Omega_{m,n,r}$.

5.4.2 Une première majoration de $\Delta_{m,n,r}$

Les propriétés arithmétiques étudiées précédemment vont nous permettre de majorer $\Delta_{m,n,r}$. Rappelons que, d'après (5.25),

$$\alpha_{i,j,h,r}=\pm\binom{r+\delta_{ij}}{h}n^{mr+m-r-\delta_{ij}}\prod_{\substack{\ell=1\\ \ell\neq j}}^{m}g_{j,\ell,h,r+\delta_{i\ell}}$$

où

$$g_{j,\ell,h,r}=\frac{r!}{\prod\limits_{v=-h}^{r-h}(nv-j+\ell)}$$

donc

$$\alpha_{i,j,h,r}=\pm\binom{r+\delta_{ij}}{h}\frac{n^{mr+m-r-\delta_{ij}}\prod\limits_{\substack{\ell=1\\ \ell\neq j}}^{m}(r+\delta_{i\ell})!}{\prod\limits_{\substack{\ell=1\\ \ell\neq j}}^{m}\prod\limits_{v=-h}^{r+\delta_{i\ell}-h}(nv-j+\ell)}.$$

Si on note $s_{n,r}=n^{v_n(r!)}$, le numérateur de la fraction est divisible par $(n^{r+1}s_{n,r})^{m-1}$ et le dénominateur n'est pas divisible par n car sinon, n étant premier, n diviserait l'un des $nv-j+\ell$ donc n diviserait un certain $\ell-j$ ce qui impossible car $|\ell-j|<m<n$.

Notons $D_{i,j,h,r}$ le dénominateur dans l'écriture sous forme irréductible de $\alpha_{i,j,h,r}$ et, oubliant la dépendance en n, m et r, $\Delta_0\Delta_1$ le plus petit commun multiple des $D_{i,j,h,r}$ pour $(i,j)\in[\![1,m]\!]^2$ et $h\in[\![0,r+\delta_{ij}]\!]$ de telle sorte que Δ_0 contienne les nombres premiers $p\leq\Omega_{m,n,r}$ et que Δ_1 contienne les nombres premiers $p>\Omega_{m,n,r}$. Ainsi, on peut affirmer que

$$\Delta_{m,n,r}\leq(n^{r+1}s_{n,r})^{1-m}\Delta_0\Delta_1. \tag{5.38}$$

Déterminons tout d'abord un minorant de $s_{n,r}$. En rappelant que $v_n(r!)=\sum\limits_{t=1}^{\rho}\left\lfloor\dfrac{r}{n^t}\right\rfloor$ où $\rho=\left\lfloor\dfrac{\ln r}{\ln n}\right\rfloor$, on obtient $\dfrac{\ln s_{n,r}}{\ln n}=\sum\limits_{t=1}^{\rho}\left(\dfrac{r}{n^t}-\left\{\dfrac{r}{n^t}\right\}\right)$. Or, en écrivant la division euclidienne de r par n^t, on a $r=Qn^t+R$ avec $0\leq R\leq n^t-1$ donc $\left\{\dfrac{r}{n^t}\right\}=\dfrac{R}{n^t}\leq 1-\dfrac{1}{n^t}$. Il s'ensuit que

$$\frac{\ln s_{n,r}}{\ln n}\geq\sum_{t=1}^{\rho}\left(\frac{r+1}{n^t}-1\right)=\frac{(r+1)(1-n^{-\rho})}{n-1}-\rho.$$

Posons $\gamma = \left\{ \dfrac{\ln r}{\ln n} \right\}$ de telle sorte que $\rho = \dfrac{\ln r}{\ln n} - \gamma$. Alors,

$$\frac{\ln s_{n,r}}{\ln n} \geq \frac{(r+1)(1-n^{\gamma-\frac{\ln r}{\ln n}})}{n-1} + \gamma - \frac{\ln r}{\ln n} = \frac{r+1-\frac{r+1}{r}n^{\gamma}+\gamma(n-1)}{n-1} - \frac{\ln r}{\ln n}.$$

Si on définit la fonction f sur $[0\,;1]$ par $f(x) = 1 - \dfrac{r+1}{r}n^x + x(n-1)$ alors $f''(x) = -\dfrac{r+1}{r}(\ln n)^2 n^x$ donc f est concave et ainsi f atteint son minimum en 0 ou en 1. Comme $f(0) = -\dfrac{1}{r}$ et $f(1) = -\dfrac{n}{r}$, f atteint son minimum en $x = 1$ (et seulement en $x = 1$) donc

$$\frac{1-\frac{r+1}{r}n^{\gamma}+\gamma(n-1)}{n-1} > \frac{-\frac{n}{r}}{n-1}$$

et ainsi, si $n \leq r$

$$\frac{\ln s_{n,r}}{\ln n} \geq \frac{r-\frac{n}{r}}{n-1} - \frac{\ln r}{\ln n} \geq \frac{r-1}{n-1} - \frac{\ln r}{\ln n}.$$

On en déduit que

$$s_{n,r} \geq \begin{cases} r^{-1}n^{\frac{r-1}{n-1}} & \text{si } n \leq r, \\ 1 & \text{si } n > r \end{cases} \tag{5.39}$$

(La seconde minoration découlant simplement du fait que $s_{n,r}$ est un entier naturel non nul.)

Intéressons-nous ensuite à Δ_0. Supposons que p divise le dénominateur d'un certain $g_{j,\ell,h,r+\delta_{i\ell}}$. Alors, comme on l'a déjà vu, n ne divise pas le dénominateur de $g_{j,\ell,h,r+\delta_{i\ell}}$ donc, comme n est premier, $\mathrm{PGCD}(p,n) = 1$. Soit $t \in \mathbb{N}^*$. En raisonnant comme dans la démonstration du lemme 3.2.2, si on note $\tilde{n}$ l'inverse de n modulo p^t et $k_{j,\ell}$ le reste de $(j-\ell)\tilde{n}$ modulo p^t alors p^t divise $nv - j + \ell$ si et seulement si $v \equiv k_{j,\ell}\ [p^t]$ et ainsi le nombre d'entiers de la forme $nv - j + \ell$ divisible par p^t avec $v \in [\![-h, r+\delta_{i\ell}-h]\!]$ est égal au nombre d'entiers u compris entre $\dfrac{-h-k_{j,\ell}}{p^t}$ et $\dfrac{r+\delta_{i\ell}-h-k_{j,\ell}}{p^t}$. Ce nombre est donc au plus égal $\left\lfloor \dfrac{r+\delta_{i\ell}}{p^t} \right\rfloor + 1$. Ainsi, la valuation $p-$adique du dénominateur de $g_{j,\ell,h,r+\delta_{i\ell}}$ est majorée par

$$\sum_{t=1}^{T} \left(\left\lfloor \frac{r+\delta_{i\ell}}{p^t} \right\rfloor + 1 \right)$$

où T est le plus grand entier tel que $p^T \leq \max\{|nv - j + \ell| \,|\, v \in [\![-h, r+\delta_{i\ell}-h]\!]\} \leq n(r+1)+m$. On en déduit donc que la valuation $p-$adique du dénominateur de $g_{j,\ell,h,r+\delta_{i\ell}}$ est majorée par

$$\left\lfloor \frac{\ln(nr+n+m)}{\ln p} \right\rfloor + \sum_{t=1}^{T} \left\lfloor \frac{r+\delta_{i\ell}}{p^t} \right\rfloor.$$

Comme, par ailleurs,

$$v_p((r+\delta_{i\ell})!) = \sum_{t=1}^{+\infty} \left\lfloor \frac{r+\delta_{i\ell}}{p^t} \right\rfloor$$

on peut conclure que, si $G_{j,\ell,h,r+\delta_{i\ell}}$ désigne le dénominateur dans l'écriture irréductible de $g_{j,\ell,h,r+\delta_{i\ell}}$ alors

$$v_p(G_{j,\ell,h,r+\delta_{i\ell}}) \leq \left\lfloor \frac{\ln(nr+n+m)}{\ln p} \right\rfloor$$

Comme cette majoration ne dépend pas de ℓ, on en déduit que

$$v_p(D_{i,j,h,r}) \leq (m-1)\left\lfloor \frac{\ln(nr+n+m)}{\ln p} \right\rfloor \leq (m-1)\frac{\ln(nr+n+m)}{\ln p}$$

où, rappelons-le, $D_{i,j,h,r}$ désigne le dénominateur dans l'écriture irréductible de $\alpha_{i,j,h,r}$. Ainsi, étant donné que $\Delta_0 = \prod_{p \leq \Omega_{m,n,r}} p^{\max v_p(D_{i,j,h,r})}$, on peut conclure que

$$\ln \Delta_0 \leq (m-1)\pi(\Omega_{m,n,r}) \ln(nr+n+m)$$

où $\pi(x)$ désigne le nombre de nombres premiers p tels que $p \leq x$. Or, d'après le corollaire 1 de Rosser et Schœnfeld [36], pour tout $x > 1$,

$$\pi(x) < \frac{1{,}25506x}{\ln x}$$

donc, en se souvenant du fait que $\ln \Omega_{m,n,r} \geq \frac{1}{2}\ln(nr+n+m)$

$$\ln \Delta_0 \leq (m-1)\frac{1{,}25506\Omega_{m,n,r}}{\ln \Omega_{m,n,r}} \ln(nr+n+m) \leq 2{,}52(m-1)\Omega_{m,n,r}. \tag{5.40}$$

Pour les « grands » nombres premiers i.e. pour les nombres premiers $p > \Omega_{m,n,r}$, nous utilisons le corollaire 5.4.6. On sait, d'après le lemme 5.4.4, que

$$v_p(\Delta_1) \leq m-1$$

donc, d'après (5.37), (5.38), (5.40),

$$\Delta_{m,n,r} \leq \left(\frac{(r+2)(r+1)\mathrm{e}^{2{,}52\Omega_{m,n,r}}}{n^{r+1}s_{n,r}}\right)^{m-1} \Delta_2 \tag{5.41}$$

où $\Delta_2 = \Delta_2(m,n,r)$ vérifie

$$\ln \Delta_2 = \sum_{a=1}^{n-1}\sum_{\mu=1}^{m-1}\sum_{N=0}^{N_0}\left(\theta\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right) - \theta\left(\frac{r+2}{N+1},n,a\right)\right). \tag{5.42}$$

Il reste alors à majorer Δ_2. Pour cela, remarquons que

$$\sum_{N=0}^{N_0}\left(\theta\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right) - \theta\left(\frac{r+2}{N+1},n,a\right)\right)$$

est majoré par

$$\sum_{N=0}^{N_1}\theta\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right) - \sum_{N=0}^{N_1-1}\theta\left(\frac{r+2}{N+1},n,a\right)$$

pour tout entier naturel non nul N_1.

En effet, notons pour simplifier $f(x) = \theta(x,n,a)$ et $t = \frac{d_{a,\mu}}{n}$. Comme la fonction f est croissante et comme $0 < t < 1$, $\sum_{N=0}^{N_0}\left[f\left(\frac{r+2}{N+t}\right) - f\left(\frac{r+2}{N+1}\right)\right] \leq \sum_{N=0}^{+\infty}\left[f\left(\frac{r+2}{N+t}\right) - f\left(\frac{r+2}{N+1}\right)\right]$ (la somme étant en fait finie car, pour $0 < x < 2$, $f(x) = 0$). Or,

$$\begin{aligned}
&\sum_{N=0}^{+\infty}\left[f\left(\frac{r+2}{N+t}\right) - f\left(\frac{r+2}{N+1}\right)\right] \\
&\quad= \sum_{N=0}^{N_1} f\left(\frac{r+2}{N+t}\right) - \sum_{N=0}^{N_1-1} f\left(\frac{r+2}{N+1}\right) - f\left(\frac{r+2}{N_1+1}\right) + \sum_{N=N_1+1}^{+\infty}\left[f\left(\frac{r+2}{N+t}\right) - f\left(\frac{r+2}{N+1}\right)\right] \\
&\quad= \sum_{N=0}^{N_1} f\left(\frac{r+2}{N+t}\right) - \sum_{N=0}^{N_1-1} f\left(\frac{r+2}{N+1}\right) - \sum_{N=N_1}^{+\infty}\left[f\left(\frac{r+2}{N+1}\right) - f\left(\frac{r+2}{N+1+t}\right)\right] \\
&\quad\leq \sum_{N=0}^{N_1} f\left(\frac{r+2}{N+t}\right) - \sum_{N=0}^{N_1-1} f\left(\frac{r+2}{N+1}\right)
\end{aligned}$$

car, par croissante de f, $f\left(\frac{r+2}{N+1}\right) - f\left(\frac{r+2}{N+1+t}\right) \geq 0$ pour tout entier N.

Pour terminer ce paragraphe, remarquons que si δ_n est une fonction à valeurs positives telle que

$$\max_{1\leq a\leq n-1} \frac{n-1}{x}\left|\theta(x,n,a) - \frac{x}{n-1}\right| < \delta_n(x),$$

alors

$$\theta\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right) - \frac{r+2}{\left(N+\frac{d_{a,\mu}}{n}\right)(n-1)} < \frac{r+2}{\left(N+\frac{d_{a,\mu}}{n}\right)(n-1)}\delta_n\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}}\right)$$

donc

$$\theta\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right) < \frac{r+2}{n-1}\times\frac{1+\delta_n\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}}\right)}{N+\frac{d_{a,\mu}}{n}}$$

et

$$\frac{r+2}{(N+1)(n-1)} - \theta\left(\frac{r+2}{N+1},n,a\right) < \frac{r+2}{(N+1)(n-1)}\delta_n\left(\frac{r+2}{N+1}\right)$$

donc

$$\theta\left(\frac{r+2}{N+1},n,a\right) > \frac{r+2}{n-1}\times\frac{1-\delta_n\left(\frac{r+2}{N+1}\right)}{N+1}$$

ce qui permet de conclure que

$$\ln\Delta_2 \leq \frac{r+2}{n-1}\sum_{a=1}^{n-1}\sum_{\mu=1}^{m-1}\left(\sum_{N=0}^{N_1}\frac{1+\delta_n\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}}\right)}{N+\frac{d_{a,\mu}}{n}} - \sum_{N=0}^{N_1-1}\frac{1-\delta_n\left(\frac{r+2}{N+1}\right)}{N+1}\right). \tag{5.43}$$

Il nous reste donc à déterminer une telle fonction δ_n. C'est l'objet du prochain paragraphe.

5.4.3 Estimation « à la Tchebychev » pour les nombres premiers en progression arithmétiques

Pour définir la fonction δ_n, il est nécessaire d'obtenir une estimation précise de la fonction $\theta(x,n,a)$. Pour ce faire, on va distinguer les « grandes » valeurs de x des « petites ».

Pour les « grandes » valeurs de x, on utilise un théorème dû à Ramaré et Rumely [35].

Rappelons qu'étant donné un entier naturel non nul k, un caractère de Dirichlet χ modulo k est un caractère du groupe $(\mathbb{Z}/k\mathbb{Z})^*$ i.e. un morphisme de $(\mathbb{Z}/k\mathbb{Z})^*$ dans $\mathbb{C}^*$. On note $\mathrm{Dir}(k)$ l'ensemble des caractères de Dirichlet modulo k.

Si $\chi \in \mathrm{Dir}(k)$ alors χ se prolonge naturellement à $\mathbb{Z}/k\mathbb{Z}$ en posant $\chi(x) = 0$ si x est un élément non inversible de $\mathbb{Z}/k\mathbb{Z}$ puis χ se prolonge à $\mathbb{N}$ tout entier en posant, pour tout $u \in \mathbb{N}$, $\chi(u) = \chi(\bar{u})$ où $\bar{u}$ est la classe de u modulo n. Un tel prolongement définit une suite $(\chi(u))_{u\in\mathbb{N}}$ strictement multiplicative i.e. telle que, pour tous entiers naturels u et v, $\chi(uv) = \chi(u)\chi(v)$.

Si k' est un diviseur strict de k, on a une projection naturelle $\pi' : \mathbb{Z}/k\mathbb{Z} \to \mathbb{Z}/k'\mathbb{Z}$ et, pour tout $\chi_{k'} \in \mathrm{Dir}(k')$, on définit $\chi_k \in \mathrm{Dir}(k)$ par $\chi_k = \chi_{k'} \circ \pi'$.

On dit qu'un caractère $\chi \in \mathrm{Dir}(k)$ est primitif s'il n'existe pas de diviseur strict k' de k tel que $\chi = \chi_k$ pour un certain $\chi_{k'} \in \mathrm{Dir}(k')$ i.e. si χ ne se factorise pas à travers $\mathbb{Z}/k'\mathbb{Z}$.

Si $\chi \in \mathrm{Dir}(k)$ est primitif, on dit que k est le conducteur de χ.

On remarquera que, par définition, si k est un nombre premier alors un caractère de Dirichlet modulo k est primitif de conducteur k.

A tout $\chi \in \mathrm{Dir}(k)$, on peut associer la série L de Dirichlet définie par

$$L(s,\chi) = \sum_{u=1}^{+\infty} \frac{\chi(u)}{u^s}.$$

Comme χ est borné, cette égalité formelle définie une fonction sur $\{s \in \mathbb{C} \,|\, \mathrm{Re}\, s > 1\}$ appelée fonction L de Dirichlet. Cette fonction se prolonge de façon unique en une fonction méromorphe sur $\mathbb{C}$.

Si χ est le caractère trivial constant égal à 1 alors $L(s,\chi)$ n'est autre que la fonction ζ de Riemann. A l'image de ζ, les fonctions L sont l'objet d'une conjecture dite *hypothèse de Riemann généralisée* (en anglais *Generalized Riemann hypothesis* abrégé GRH) qui s'énonce ainsi :

Conjecture. (GRH) — Pour tout caractère de Dirichlet χ, si $s \in \mathbb{C}$ est un nombre complexe tel que $L(s,\chi) = 0$ et $\mathrm{Re}(s) \in [0\,;1]$ alors $\mathrm{Re}(s) = \frac{1}{2}$.

Autrement dit, tout zéro de $L(s,\chi)$ situé dans la bande critique $\{0 \leq \mathrm{Re}(s) \leq 1\}$ se trouve sur la droite critique $\mathrm{Re}(s) = \frac{1}{2}$.

Cette conjecture, comme celle de Riemann, semble pour l'instant loin d'être démontrée. On sait, en revanche, dans certain cas, la prouver en bornant la hauteur des nombres s i.e. la valeur absolue de leur partie imaginaire. Si H est un réel strictement positif, on appelle *hypothèse de Riemann généralisée de hauteur H* (en abrégé GRH(H)) la conjecture suivante :

Conjecture. (GRH(H)) — Soit χ un caractère de Dirichlet. Si $s \in \mathbb{C}$ est un nombre complexe tel que $L(s,\chi) = 0$, $\mathrm{Re}(s) \in [0\,;1]$ et $|\mathrm{Im}(s)| \leq H$ alors $\mathrm{Re}(s) = \dfrac{1}{2}$.

Le théorème 4.3.2 de [35] assure que si tout caractère de Dirichlet modulo k vérifie GRH(H) pour une hauteur $H \geq 1000$ alors il existe un réel x_0 et une constante $C(x_0)$ explicitement calculables tels que, pour tout $x \geq x_0$

$$\frac{\varphi(k)}{x} \max_{1 \leq y \leq x} \left| \theta(x,k,a) - \frac{y}{\varphi(k)} \right| \leq C(x_0).$$

Etant donné que n est premier, on en déduit que si tout caractère de Dirichlet primitif de conducteur n vérifie GRH(H) avec $H \geq 1000$ alors il existe un réel x_0 et une constante $C(x_0)$ explicitement calculables tels que, pour tout $x \geq x_0$

$$\frac{n-1}{x} \max_{1 \leq y \leq x} \left| \theta(x,n,a) - \frac{y}{n-1} \right| \leq C(x_0).$$

Afin d'utiliser ce théorème, il est donc nécessaire de montrer GRH(H) pour H au moins égal à 1000. Pour cela, on utilise la méthode décrite par Rumely dans [37]. Dans cette article, Rumely a prouvé GRH(10 000) pour tout caractère primitif de conducteur $n \leq 13$ et GRH(2 500) pour tout caractère de conducteur $n \leq 72$. Il suffit donc de prouver GRH(1 000) pour tout caractère primitif de conducteur $n \in [\![73, 337]\!]$. C'est ce qu'a fait Bennett dans son article [5]. La méthode de Rumely se divise en trois étape dont nous donnons une description très sommaire. (Pour plus de précision, on pourra se reporter à [37]).

Etape 1. — Recherche des zéros sur la droite critique.

Si on définit $\xi(s,\chi) = \left(\dfrac{n}{\pi}\right)^{\frac{s}{2}} \Gamma\left(\dfrac{s+\delta}{2}\right) L(s,\chi)$ où $\delta = \dfrac{1-\chi(n-1)}{2}$ alors ξ vérifie l'équation fonctionnelle

$$\xi(s,\chi) = W_\chi \xi(1-s,\bar{\chi}) \tag{5.44}$$

où $W_\chi = \dfrac{1}{\mathrm{i}^\delta\sqrt{n}} \sum_{a=1}^{n} \chi(a)\mathrm{e}^{\frac{2\mathrm{i}\pi a}{n}}$. On montre que $|W_\chi| = 1$ donc on peut écrire $W_\chi = \mathrm{e}^{\mathrm{i}\alpha_\chi}$ et, en posant $s = \frac{1}{2} + \mathrm{i}t$ et $\alpha(t,\chi) = \frac{t}{2}\ln\left(\frac{n}{\pi}\right) + \mathrm{Im}\left(\ln\left(\Gamma\left(\frac{s+\delta}{2}\right)\right)\right) - \frac{\alpha_\chi}{2}$ il suit de (5.44) que $Z(t,\chi) := \mathrm{e}^{\mathrm{i}\alpha(t,\chi)}L(s,\chi)$ est une fonction réelle à valeurs réelle qui a même module que L. Ainsi, on peut ramener le problème de la recherche des zéros de L à l'étude d'une fonction réelle d'une variable réelle.

On calcule alors (une approximation) du développement de Taylor de L au point $s_\ell = \frac{1}{2} + \frac{\ell}{2}$ avec une précision suffisante pour être sûr que l'erreur commise sur le disque de centre s_ℓ et de rayon $\frac{1}{4}$ est inférieure à 10^{-20} puis on recherche les zéros de la fonction Z définie précédemment.

Etape 2. — Validation de la liste des zéros obtenue

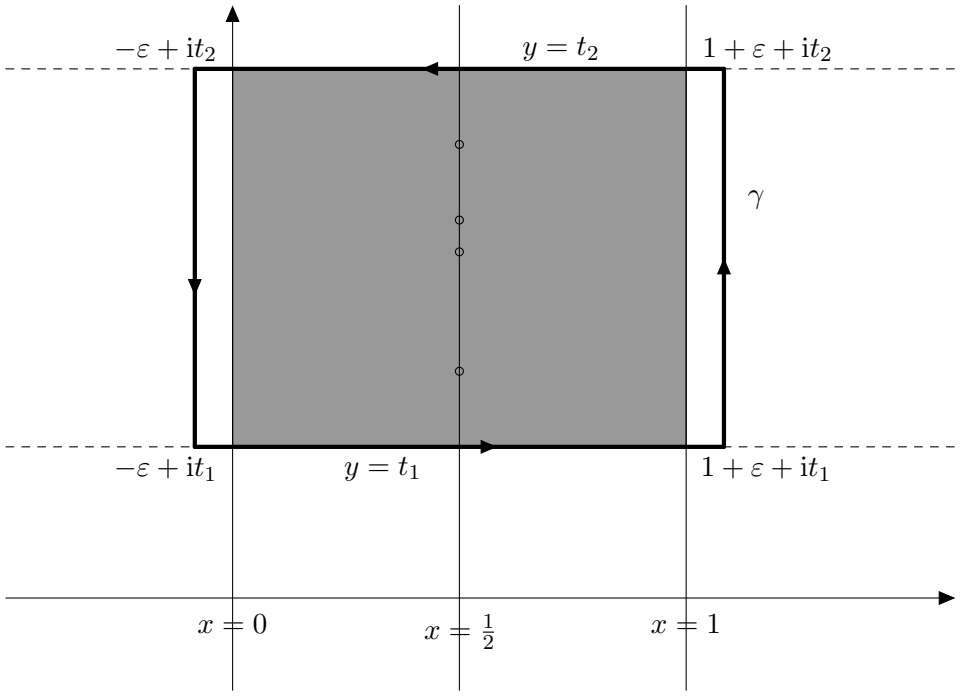
La liste de zéros établie lors de la première étape est ensuite validée. Pour ce faire, on ordonne les zéros (potentiels) obtenus et on choisit entre chacun une valeur, appelée point de validation. On utilise ensuite la formule sommatoire d'Euler-MacLaurin pour approcher L puis Z et on vérifie qu'entre deux points de validation successifs, la fonction Z change de signe ce qui atteste de la présence d'un zéro.

Etape 3. — Vérification que la liste obtenue est exhaustive

Pour vérifier que la liste obtenue est exhaustive i.e. qu'il n'y a pas de zéros de L dans la bande critique autres que ceux trouvés sur la droite critique $\mathrm{Re}(s) = \frac{1}{2}$, il suffit de montrer que le nombre de zéros de L contenue dans la bande critique ne dépasse pas le nombre de zéros déjà trouvés. Pour ce faire, Rumely utilise une généralisation pour les fonctions L de la méthode de Turing pour la fonction ζ dont le principe est le suivant. On considère deux ordonnées t_1 et t_2 en lesquelles L ne s'annule pas. On souhaite déterminer le nombre $N(t_1,t_2)$ de zéros contenus dans le rectangle dont les sommets sont $\mathrm{i}t_1$, $1+\mathrm{i}t_1$, $1+\mathrm{i}t_2$ et $\mathrm{i}t_2$. Si on sait qu'il y a N zéros de L sur la droite critique entre les ordonnées t_1 et t_2, il suffit de montrer que $N(t_1,t_2) \leq N + \alpha$ avec $\alpha < 1$ pour en déduire que $N(t_1,t_2) = N$ et qu'il n'y a donc pas d'autres zéros que ceux situés sur la droite critique entre les ordonnées t_1 et t_2. Pour obtenir une telle majoration, on utilise le fait que L et ξ ont les mêmes zéros et on utilise le théorème des résidus pour écrire que

$$N(t_1,t_2) = \int_\gamma \frac{\xi'}{\xi}$$

où γ est le contour orienté suivant ($\varepsilon > 0$) :



Il faut ensuite par des arguments à la fois techniques et numériques réussir à majorer suffisamment précisément cette intégrale pour pouvoir conclure.

Une fois montrée GRH(1 000) pour les caractères primitifs de conducteur $n \in [\![3, 337]\!]$, en appliquant le théorème 4.3.2 de [35], Bennett aboutit au théorème suivant.

Théorème 5.4.7. — *Si* $3 \leq n \leq 337$ *est un nombre premier et si on définit*

$$\varepsilon_n = \max_{x \geq 10^{11}} \max_{1 \leq a \leq n-1} \max_{1 \leq y \leq x} \frac{n-1}{x} \left| \theta(y, n, a) - \frac{y}{n-1} \right|$$

alors $\varepsilon_n < \widetilde{\varepsilon_n}$ *où* $\widetilde{\varepsilon_n}$ *est donnée par le tableau suivant :*

n	$\widetilde{\varepsilon_n}$	n	$\widetilde{\varepsilon_n}$	n	$\widetilde{\varepsilon_n}$	n	$\widetilde{\varepsilon_n}$
3	0,002238	67	0,018873	151	0,046304	241	0,060570
5	0,002686	71	0,019435	157	0,047254	251	0,062161
7	0,003007	73	0,033698	163	0,048204	257	0,063116
11	0,003606	79	0,034706	167	0,048837	263	0,064073
13	0,003893	83	0,035374	173	0,049787	269	0,065030
17	0,010746	89	0,036369	179	0,050737	271	0,065349
19	0,011296	97	0,037686	181	0,051054	277	0,066307
23	0,011980	101	0,038341	191	0,052637	281	0,066943
29	0,012968	103	0,038664	193	0,052954	283	0,067261
31	0,013290	107	0,039305	197	0,053587	293	0,068851
37	0,014244	109	0,039625	199	0,053904	307	0,071081
41	0,014869	113	0,040265	211	0,055806	311	0,071719
43	0,015176	127	0,042496	223	0,057710	313	0,072038
47	0,015788	131	0,043132	227	0,058345	317	0,072677
53	0,016702	137	0,044084	229	0,058663	331	0,074915
59	0,017613	139	0,044402	233	0,059298	337	0,075876
61	0,017917	149	0,045987	239	0,060252		

Ce théorème nous permet de voir qu'on peut donc choisir $\delta_n(x) = \widetilde{\varepsilon_n}$ pour les valeurs de $x \geq 10^{11}$.

Intéressons-nous à présent aux valeurs de $x < 10^{11}$. Pour cela, nous définissons

$$\theta_n := \max_{1 \leq a \leq n-1} \max_{0 < x < 10^{11}} \frac{1}{\sqrt{x}} \left| \theta(x, n, a) - \frac{x}{n-1} \right|.$$

Entre deux nombres premiers, la fonction $x \mapsto \theta(x, n, a)$ est constante donc $f := x \mapsto \dfrac{\theta(x, n, a) - \frac{x}{n-1}}{\sqrt{x}}$ est décroissante. De plus, en chaque nombre premier, elle présente un saut. Ainsi, pour connaître la valeur de θ_n, il suffit de déterminer $f(2)$, $f(10^{11})$ ainsi que $\lim\limits_{x \to p^-} f(x)$ et $\lim\limits_{x \to p^+} f(x)$ pour tout nombre premier p compris entre 2 et 10^{11}. En suivant ce procédé, Bennett obtient les valeurs rassemblées dans le tableau de la page suivante. Dans ce tableau, les valeurs de θ_n sont arrondies pas excès à la sixième décimale. De plus, on précise la valeur de a en laquelle le maximum est atteint et la valeur correspondante $\tilde{x}$. Celle-ci est toujours de la forme $\tilde{x} = p_j$ (i.e. x est le $j-$ème nombre premier) et, selon les cas,

$$\theta_n = \frac{1}{\sqrt{p_{j-1}}} \left| \theta(p_{j-1}, n, a) - \frac{p_{j-1}}{n-1} \right| \quad \text{ou} \quad \theta_n = \lim_{x \to p_j^-} \frac{1}{\sqrt{x}} \left| \theta(x, n, a) - \frac{x}{n-1} \right|.$$

n	θ_n	a	$\tilde{x}$
2	2,071993	1	1423
3	1,798158	1	69991
5	1,412480	4	349
7	1,116838	4	24470870029
11	0,976421	5	726270803
13	1,017317	10	65095932067
17	1,001057	8	6395663
19	1,001556	6	461687
23	0,973114	12	793489
29	0,793283	9	2039
31	0,853475	8	16773763751
37	0,867916	26	4058619751
41	0,818620	29	30239497
43	0,832936	25	6547405001
47	0,744386	34	2000700217
53	0,829958	36	5813
59	0,710444	58	25841
61	0,719386	1	9212953
67	0,728237	24	48679198759
71	0,750488	11	41333
73	0,759154	72	4817
79	0,730952	26	38932253
83	0,703220	7	173
89	0,705420	7	541
97	0,713661	79	2206247
101	0,709028	7	613
103	0,709547	7	419
107	0,710525	7	863
109	0,710988	7	443
113	0,711863	7	233
127	0,714487	7	769
131	0,715133	7	269
137	0,716031	7	281
139	0,716619	121	90124089259
149	0,717609	7	2689
151	0,717847	7	2423
157	0,718525	7	2833

n	θ_n	a	$\tilde{x}$
163	0,719154	7	659
167	0,719547	7	1009
149	0,717609	7	2689
151	0,717847	7	2423
157	0,718525	7	2833
163	0,719154	7	659
167	0,719547	7	1009
173	0,720103	7	353
179	0,720622	7	1439
181	0,720787	7	1093
191	0,721560	7	389
193	0,721705	7	4253
197	0,721987	7	401
199	0,722123	7	1201
211	0,722887	7	2539
223	0,723568	7	2237
227	0,723779	7	461
229	0,723881	7	1381
233	0,724081	7	1871
239	0,724369	7	4787
241	0,724461	7	971
251	0,724902	7	509
257	0,725150	7	521
263	0,725387	7	2111
269	0,725613	7	1621
271	0,725686	7	1091
277	0,725899	7	1669
281	0,726036	7	569
283	0,726103	7	2837
293	0,726425	7	593
307	0,726839	7	3691
311	0,726951	7	1873
313	0,727005	7	1259
317	0,727113	7	641
331	0,727468	7	1993
337	0,727611	7	2029

Nous concluons que nous pouvons définir la fonction δ_n nécessaire pour avoir l'inégalité (5.43) par

$$\delta_n(x) = \begin{cases} \widetilde{\varepsilon_n} & \text{si } x \geq 10^{11} \\ \dfrac{(n-1)\theta_n}{\sqrt{x}} & \text{si } x < 10^{11} \end{cases} \tag{5.45}$$

5.4.4 Majoration de $\Delta_{m,n,r}$

Nous pouvons à présent obtenir la majoration de $\Delta_{m,n,r}$ voulue en prenant $m = \left\lfloor \dfrac{n+1}{3} \right\rfloor$. On va en effet démontrer la proposition suivante.

Proposition 5.4.8. — *Si les constantes k_n et h_n sont définies par le tableau ci-dessous et si on pose $m = \left\lfloor \frac{n+1}{3} \right\rfloor$ alors, pour tout $r \in \mathbb{N}^*$,*

$$\ln \Delta_{m,n,r} < k_n r + h_n.$$

n	k_n	h_n
17	8,93	13,06
19	9,40	15,46
23	13,03	17,66
29	17,39	29,95
31	17,92	30,55
37	21,92	31,51
41	25,83	36,08
43	26,62	33,95
47	30,46	40,16
53	34,78	35,37
59	39,18	48,34
61	39,96	55,93
67	44,76	43,56
71	48,36	54,80
73	52,83	48,11
79	58,27	54,65

n	k_n	h_n
83	62,70	49,64
89	67,56	60,29
97	73,71	62,14
101	78,29	50,36
103	79,16	60,85
107	83,55	50,84
109	84,18	58,97
113	89,22	77,93
127	100,47	72,61
131	105,34	71,51
137	111,44	79,94
139	112,15	77,27
149	122,53	85,82
157	129,07	81,61
163	134,80	93,63
167	139,95	82,87

n	k_n	h_n
173	146,07	87,71
179	151,40	83,92
181	152,20	91,69
191	163,78	84,40
193	164,81	91,51
197	170,17	104,53
199	170,80	110,41
211	183,12	124,02
223	195,74	112,93
227	201,15	116,91
229	202,11	100,61
233	207,50	102,49
239	213,74	105,66
241	214,95	95,14
251	226,83	115,64
257	233,75	113,23

n	k_n	h_n
263	240,15	119,49
269	246,54	124,75
271	247,72	134,21
277	254,62	119,17
281	260,46	116,79
283	261,67	118,21
293	274,23	129,73
307	289,00	124,89
311	294,70	130,14
313	296,38	130,18
317	302,73	134,63
331	317,41	147,69
337	324,63	139,95

Preuve. — Si on admet l'idée que les constantes k_n et h_n existent i.e. que la fonction $r \mapsto \ln \Delta_{m,n,r}$ peut être majorée par une fonction affine, il est naturel de prendre pour valeur de k_n un majorant de la limite de $\dfrac{\Delta_{m,n,r}}{r}$ lorsque r rend vers $+\infty$.

Pour de très grandes valeurs de r, $x_{a,\mu} := \dfrac{r+2}{N + \frac{d_{a,\mu}}{n}}$ et $x_1 := \dfrac{r+2}{N+1}$ sont très grands donc, d'après (5.45), $\delta_n(x_{a,\mu}) = \delta_n(x_1) = \widetilde{\varepsilon_n}$. Ainsi, d'après (5.43),

$$\ln \Delta_2 \leq \frac{r+2}{n-1} \sum_{a=1}^{n-1} \sum_{\mu=1}^{m-1} \left(\sum_{N=0}^{N_1} \frac{1+\widetilde{\varepsilon_n}}{N + \dfrac{d_{a,\mu}}{n}} - \sum_{N=0}^{N_1-1} \frac{1-\widetilde{\varepsilon_n}}{N+1} \right).$$

Nous détaillons le raisonnement pour $n = 17$. Un calcul montre que le majorant est minimum pour le choix $N_1 = 16$ et on trouve alors

$$\ln \Delta_2 \leq 23{,}9792(r+2) \underset{r \to +\infty}{\sim} 23{,}9792r$$

Intéressons-nous ensuite au logarithme du terme $\Delta_3 := \left(\dfrac{(r+2)(r+1)\mathrm{e}^{2{,}52\Omega_{m,n,r}}}{n^{r+1} s_{n,r}} \right)^{m-1}$ qui apparait dans (5.41). Etant donné que $n \leq r$, d'une part, $\sqrt{nr+n+m} > 2n$ et, d'autre part, d'après (5.39), $s_{n,r} \geq r^{-1} n^{\frac{r-1}{n-1}}$ donc

$$\ln \Delta_3 \leq (m-1) \ln \left(\frac{r(r+1)(r+2)\mathrm{e}^{2{,}52\sqrt{nr+n+m}}}{n^{r+1+\frac{r-1}{n-1}}} \right) \underset{r \to +\infty}{\sim} -(m-1) \frac{n \ln n}{n-1} r.$$

Pour $n = 17$, on trouve donc que ce logarithme est majoré par une quantité asymptotiquement équivalente à $-5\frac{17\ln 17}{16}r < -15{,}0514r$. Etant donné que $23{,}9792r - 15{,}0514r = 8{,}9278r < 8{,}93r$, pour r suffisamment grand, $\ln\Delta_{m,n,r} < 8{,}93r$. Montrons qu'en fait, ceci est vrai pour tout $r > 3.10^6$.

Pour cela, distinguons deux cas.

Si $r \geq 10^9$ alors, pour tout a, tout μ et tout $N \in [\![0,16]\!]$, $\dfrac{(n-1)\theta_n}{\sqrt{\frac{r+2}{N+\frac{d_{a,\mu}}{n}}}} \leq \dfrac{16\times 1{,}001057}{\sqrt{\frac{10^9+2}{17}}} < \widetilde{\varepsilon_n}$ donc $\delta_n(x) \leq \widetilde{\varepsilon_n}$ et on peut dès lors, comme ci-dessus, majorer $\ln\Delta_2$ par $23{,}9792(r+2)$.

Par ailleurs, pour tout réel $\eta > 0$,

$$\ln\Delta_3 \leq 5\ln\left(\frac{(r+2)^3 \mathrm{e}^{2{,}52\sqrt{17r+23}}}{17^{\frac{17}{16}r+\frac{15}{16}}}\right) = 5\ln\left(\frac{(r+2)^3 \mathrm{e}^{2{,}52\sqrt{17r+23}}}{17^{\frac{\eta}{16}r+\frac{15}{16}}}\right) - 5\frac{17-\eta}{16}\ln(17)r.$$

Reste à choisir η tel que $23{,}979 - 5\frac{17-\eta}{16}\ln(17) < 8{,}93$ et $23{,}979\times 2 + 5\ln\left(\dfrac{(r+2)^3 \mathrm{e}^{2{,}52\sqrt{17r+23}}}{17^{\frac{\eta}{16}r+\frac{15}{16}}}\right) \leq 0$ pour $r \geq 10^9$. Un simple calcul montre que $\eta = 0{,}002$ satisfait la première inéquation et une étude de fonction montre que $h : r \mapsto 23{,}979\times 2 + 5\ln\left(\dfrac{(r+2)^3 \mathrm{e}^{2{,}52\sqrt{17r+23}}}{17^{\frac{0{,}002}{16}r+\frac{15}{16}}}\right)$ est décroissante sur $\left[10^9\,;+\infty\right[$. Etant donné que $h(10^9) < 0$, on peut conclure que $\ln\Delta_{m,n,r} < 8{,}93r$ pour $r \geq 10^9$.

Si $3.10^6 \leq r < 10^9$ alors pour, tout a, tout μ et tout $N \in [\![0,16]\!]$, $\frac{r+2}{N+\frac{d_{a,\mu}}{n}} < \frac{10^9+2}{\frac{1}{17}} < 10^{11}$ donc $\delta_n\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}}\right) = \frac{(n-1)\theta_n}{\sqrt{\frac{r+2}{N+\frac{d_{a,\mu}}{n}}}} \leq \frac{(n-1)\theta_n}{\sqrt{\frac{3.10^6+2}{N+\frac{d_{a,\mu}}{n}}}} = \delta_n\left(\frac{3.10^6+2}{N+\frac{d_{a,\mu}}{n}}\right)$. Il s'ensuit que

$$\ln\Delta_2 \leq \frac{r+2}{n-1}\sum_{a=1}^{n-1}\sum_{\mu=1}^{m-1}\left(\sum_{N=0}^{N_1}\frac{1+\delta_n\left(\frac{3.10^6+2}{N+\frac{d_{a,\mu}}{n}}\right)}{N+\frac{d_{a,\mu}}{n}} - \sum_{N=0}^{N_1-1}\frac{1-\delta_n\left(\frac{3.10^6+2}{N+\frac{d_{a,\mu}}{n}}\right)}{N+1}\right).$$

Un calcul montre que la double-somme est minimale pour le choix $N_1 = 7$ et on a alors

$$\ln\Delta_2 \leq 23{,}9468(r+2).$$

En raisonnant alors ci-dessus avec $\eta = 0{,}039$, on a

$$\ln\Delta_{m,n,r} \leq 8{,}93r + 2\times 23{,}9468 + 5\ln\left(\frac{(r+2)^3 \mathrm{e}^{2{,}52\sqrt{17r+23}}}{17^{\frac{0{,}039}{16}r+\frac{15}{16}}}\right).$$

Comme précédemment, une étude de fonction montre que $k : r \mapsto 2\times 23{,}9468 + 5\ln\left(\dfrac{(r+2)^3 \mathrm{e}^{2{,}52\sqrt{17r+23}}}{17^{\frac{0{,}039}{16}r+\frac{15}{16}}}\right)$ est décroissante sur $\left[3.10^6\,;10^9\right[$ avec $k(3.10^6) < 0$ ce qui permet de conclure.

Ces calculs se mènent de la même façon pour tout $n \geq 17$ et fournissent les différentes valeurs de k_n du tableau.

Les valeurs de $r < 3.10^6$ demandent un travail plus approfondi. Pour traiter ces cas, on commence par établir, par une méthode de crible, la liste des nombres premiers inférieurs à 2×10^9 (car on ne s'intéresse qu'aux nombres premiers inférieurs à $\dfrac{r+2}{N+\frac{1}{n}} < 337\times 3.10^6 < 2.10^9$) puis on organise ces nombres par progressions arithmétiques.

Tout d'abord, si $50\,000 \leq r < 3 \times 10^6$, on applique l'inégalité (5.41) et on calcule Δ_2 à partir de l'égalité (5.42). Pour ce faire, pour chacune des valeurs de N comprises entre 0 et N_0, il suffit de considèrer les nombres premiers de la liste compris entre $\frac{r+2}{N+1}$ et $\frac{r+2}{N+\frac{1}{n}}$ et d'ajouter les logarithmes de tels nombres appartenant aux intervalles $\left]\frac{r+2}{N+1}\,;\,\frac{r+2}{N+\frac{d_{a,\mu}}{n}}\right]$. Une remarque importante à faire est que lorsqu'on augmente r de 1, le terme $\theta\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right)-\theta\left(\frac{r+2}{N+1},n,a\right)$ n'est modifié que par, au plus, l'addition du logarithme d'un unique nombre premier de la table s'il y a un nombre premier $p \equiv a\ [n]$ dans l'intervalle $\left]\frac{r+2}{N+\frac{d_{a,\mu}}{n}}\,;\,\frac{r+3}{N+\frac{d_{a,\mu}}{n}}\right[$ et la soustraction d'un tel logarithme s'il y a nombre premier $p \equiv a\ [n]$ dans l'intervalle $\left]\frac{r+2}{N+1}\,;\,\frac{r+3}{N+1}\right[$.

Ceci nous permet d'obtenir les valeurs de Δ_2 correspondant à $r+1$ à partir de celles correspondant à r sans avoir à tout recalculer.

De façon plus générale, si $\delta \in \mathbb{N}$ et $s \in \{r, r+1, \cdots, r+\delta\}$ alors, par croissance de θ,

$$\begin{aligned}
&\sum_{a=1}^{n-1}\sum_{\mu=1}^{m-1}\sum_{N=0}^{N_0}\left[\theta\left(\frac{s+2}{N+\frac{d_{a,\mu}}{n}},n,a\right)-\theta\left(\frac{s+2}{N+1},n,a\right)\right]\\
&\quad=\sum_{a=1}^{n-1}\sum_{\mu=1}^{m-1}\sum_{N=0}^{N_0}\left[\theta\left(\frac{s+2}{N+\frac{d_{a,\mu}}{n}},n,a\right)-\theta\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right)+\theta\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right)-\theta\left(\frac{s+2}{N+1},n,a\right)\right]\\
&\quad\leq\sum_{a=1}^{n-1}\sum_{\mu=1}^{m-1}\sum_{N=0}^{N_0}\left[\theta\left(\frac{r+\delta+2}{N+\frac{d_{a,\mu}}{n}},n,a\right)-\theta\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right)+\theta\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right)-\theta\left(\frac{r+2}{N+1},n,a\right)\right]
\end{aligned}$$

et donc

$$\ln\Delta_2(m,n,s) \leq \ln\Delta_2(m,n,r)+\sum_{a=1}^{n-1}\sum_{\mu=1}^{m-1}\sum_{N=0}^{N_0}\chi(a,\mu,N,n,r,\delta)$$

où

$$\chi(a,\mu,N,n,r,\delta)=\theta\left(\frac{r+2+\delta}{N+\frac{d_{a,\mu}}{n}},n,a\right)-\theta\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right).$$

En supposant qu'on montre que, pour un certain $\varepsilon_n > 0$,

$$\ln\Delta_{m,n,r} < (k_n-\varepsilon_n)r$$

et, pour un certain $\delta \in \mathbb{N}^*$,

$$S := \sum_{a=1}^{n-1}\sum_{\mu=1}^{m-1}\sum_{N=0}^{N_0}\chi(a,\mu,N,n,r,\delta) < \varepsilon_n r, \tag{5.46}$$

alors, comme la fonction $f : r \mapsto (m-1)\ln\left(\frac{r(r+1)(r+2)\mathrm{e}^{2,52\sqrt{nr+n+m}}}{n^{r+1}n^{\frac{r-1}{n-1}}}\right)$ est décroissante sur $\left[50\,000\,;3.10^6\right]$,

$$\ln\Delta_{m,n,s} \leq f(s)+\ln\Delta_2(m,n,s) \leq f(r)+\ln\Delta_2(m,n,r)+S < \ln\Delta_{m,n,r}+\varepsilon_n r < k_n r \leq k_n s.$$

dont la proposition 5.4.8 est vraie pour tout $s \in [\![r, r+\delta]\!]$.

Pour mettre en œuvre cette observation, on suppose que $\delta > n$ et on écrit

$$S = S_1 + S_2 + S_3$$

avec

$$S_1 = \sum_{a=1}^{n-1}\sum_{\mu=1}^{m-1}\sum_{\frac{\delta}{2}\leq N\leq N_0}\chi(a,\mu,N,n,r,\delta), \qquad S_2 = \sum_{a=1}^{n-1}\sum_{\mu=1}^{m-1}\sum_{1\leq N<\frac{\delta}{2}}\chi(a,\mu,N,n,r,\delta)$$

$$\text{et} \qquad S_3 = \sum_{a=1}^{n-1}\sum_{\mu=1}^{m-1}\chi(a,\mu,0,n,r,\delta).$$

Pour majorer ces sommes, on utilise l'inégalité grossière suivante : si A et B sont des réels tels que $B > A > 0$,

$$\theta(B,n,a) - \theta(A,n,a) = \sum_{\substack{A<p\leq B\\ p\equiv a\ [n]}} \ln p \leq \ln(B) \sum_{\substack{A<p\leq B\\ p\equiv a\ [n]}} 1 = \ln(B)(\pi(B,n,a) - \pi(A,n,a))$$

où $\pi(x,n,a)$ désigne le nombre de nombres premiers $p \equiv a\ [n]$ tels que $p \leq x$.

Or, pour tout $a \in [\![1, n-1]\!]$ et tout $\mu \in [\![1, m-1]\!]$, $d_{a,\mu} \geq 1$ donc $\frac{r+2+\delta}{N+\frac{d_{a,\mu}}{n}} \leq \frac{r+2+\delta}{N+\frac{1}{n}}$. De là, on déduit que

$$\begin{aligned}\chi(a,\mu,N,n,r,\delta) &\leq \ln\left(\frac{r+2+\delta}{N+\frac{d_{a,\mu}}{n}}\right)\left[\pi\left(\frac{r+2+\delta}{N+\frac{d_{a,\mu}}{n}},n,a\right) - \pi\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right)\right]\\ &\leq \ln\left(\frac{r+2+\delta}{N+\frac{1}{n}}\right)\left[\pi\left(\frac{r+2+\delta}{N+\frac{d_{a,\mu}}{n}},n,a\right) - \pi\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right)\right].\end{aligned}$$

Ainsi,

$$S_1 \leq \sum_{\frac{\delta}{2}\leq N\leq N_0}\ln\left(\frac{r+2+\delta}{N+\frac{1}{n}}\right)\sum_{\mu=1}^{m-1}\sum_{a=1}^{n-1}\left[\pi\left(\frac{r+2+\delta}{N+\frac{d_{a,\mu}}{n}},n,a\right) - \pi\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right)\right].$$

Si $N \geq \frac{\delta}{2}$ alors, pour un $d \in \mathbb{N}^*$ fixé, $\dfrac{\delta}{N+\frac{d}{n}} < 2$ donc il y au plus un nombre premier dans l'intervalle $\left]\frac{r+2}{N+\frac{d}{n}}\,;\frac{r+2+\delta}{N+\frac{d}{n}}\right]$ et il existe un unique $a \in [\![0, n-1]\!]$ tel que $p \equiv a\ [n]$ car $p \geq \Omega_{m,n,r} > n$. Dès lors,

$$\sum_{a=1}^{n-1}\left(\pi\left(\frac{r+2+\delta}{N+\frac{d}{n}},n,a\right) - \pi\left(\frac{r+2}{N+\frac{d}{n}},n,a\right)\right) \leq 1.$$

Comme les valeurs prises par $d_{a,\mu}$ appartiennent à $[\![1, n-1]\!]$ et comme les valeurs sommées sont positives,

$$\begin{aligned}\sum_{\mu=1}^{m-1}\sum_{a=1}^{n-1}\left[\pi\left(\frac{r+2+\delta}{N+\frac{d_{a,\mu}}{n}},n,a\right) - \pi\left(\frac{r+2}{N+\frac{d_{a,\mu}}{n}},n,a\right)\right] &\leq \sum_{d=1}^{n-1}\sum_{a=1}^{n-1}\left[\pi\left(\frac{r+2+\delta}{N+\frac{d}{n}},n,a\right) - \pi\left(\frac{r+2}{N+\frac{d}{n}},n,a\right)\right]\\ &\leq n-1\end{aligned}$$

et donc $S_1 \leq (n-1)\sum_{\frac{\delta}{2}\leq N\leq N_0}\ln\left(\frac{r+2+\delta}{N+\frac{1}{n}}\right)$ (4).

(4). Nous aboutissons ici à une majoration légèrement différente de celle obtenue par Bennett ([5] p. 30) mais son raisonnement, et notamment l'utilisation du fait que, pour tout a, $d_{a,\mu} \leq d_{a,m-1}$ nous échappe.

Comme $r \geq 50\,000$, une étude de fonction montre que $\frac{r+2}{\sqrt{n(r+1)}} < \frac{r}{2n}$ et donc, par définition de N_0,

$$N \leq N_0 \leq \frac{r+2}{\sqrt{nr+n+m}} \leq \frac{r+2}{\sqrt{n(r+1)}} < \frac{r}{2n}.$$

Ainsi,

$$\frac{r+\delta}{N} - \frac{r+2+\delta}{N+\frac{1}{n}} = \frac{2\left(\frac{r}{2n} - N\right) + \frac{\delta}{n}}{N\left(N+\frac{1}{n}\right)} > 0 \quad \text{donc} \quad \frac{r+2+\delta}{N+\frac{1}{n}} < \frac{r+\delta}{N}$$

ce qui permet de conclure que

$$S_1 < (n-1) \sum_{\frac{\delta}{2} \leq N \leq N_0} \ln\left(\frac{r+\delta}{N}\right). \tag{5.47}$$

De la même façon, on commence par majorer S_2 par

$$(m-1)(n-1) \sum_{1 \leq N < \frac{\delta}{2}} \ln\left(\frac{r+2+\delta}{N+\frac{1}{n}}\right) \max_{a \in [\![1,n-1]\!]} \max_{d \in [\![1,n-1]\!]} \left[\pi\left(\frac{r+2+\delta}{N+\frac{d}{n}}, n, a\right) - \pi\left(\frac{r+2}{N+\frac{d}{n}}, n, a\right)\right]$$

Or, pour tout $d \geq 1$, l'intervalle $\left]\frac{r+2}{N+\frac{d}{n}} ; \frac{r+2+\delta}{N+\frac{d}{n}}\right]$ a une amplitude strictement inférieure à $\left(\left\lfloor\frac{\delta}{nN}\right\rfloor + 1\right) n$ donc contient, pour tout a fixé, au plus $\left\lfloor\frac{\delta}{nN}\right\rfloor + 1$ nombres (premiers) congrus à a modulo n. On en déduit que

$$S_2 \leq (m-1)(n-1) \sum_{1 \leq N < \frac{\delta}{2}} \left(\left\lfloor\frac{\delta}{nN}\right\rfloor + 1\right) \ln\left(\frac{r+2+\delta}{N+\frac{1}{n}}\right) \leq (m-1)(n-1) \sum_{1 \leq N < \frac{\delta}{2}} \left(\left\lfloor\frac{\delta}{nN}\right\rfloor + 1\right) \ln\left(\frac{r+\delta}{N}\right)$$

et donc

$$S_2 \leq (n-1)(m-1)\left(\sum_{1 \leq N < \frac{\delta}{2}} \ln\left(\frac{r+\delta}{N}\right) + \sum_{1 \leq N < \frac{\delta}{2}} \left\lfloor\frac{\delta}{nN}\right\rfloor \ln\left(\frac{r+\delta}{N}\right)\right). \tag{5.48}$$

La majoration de S_3 demande d'utiliser un argument un peu moins élémentaire. Pour cela, on utilise le théorème de type Brun-Titschmarsh suivant dû à Montgomery et Vaughan [28] :

Si x et y sont deux nombres réels positifs et si a et n sont deux entiers premiers entre eux tels que $1 \leq n < y \leq x$ alors

$$\pi(x+y, n, a) - \pi(x, n, a) < \frac{2y}{\varphi(n) \ln\left(\frac{y}{n}\right)}.$$

Il s'ensuit que

$$\chi(a, \mu, 0, n, r, \delta) \leq \ln\left(\frac{r+2+\delta}{\frac{d_{a,\mu}}{n}}\right)\left[\pi\left(\frac{r+2+\delta}{\frac{d_{a,\mu}}{n}}, n, a\right) - \pi\left(\frac{r+2}{\frac{d_{a,\mu}}{n}}, n, a\right)\right] \leq \frac{2n\delta \ln\left((r+2+\delta)\frac{n}{d_{a,\mu}}\right)}{(n-1)d_{a,\mu} \ln\left(\frac{\delta}{d_{a,\mu}}\right)}$$

et donc

$$S_3 \leq \sum_{a=1}^{n-1} \sum_{\mu=1}^{m-1} \frac{2n\delta \ln\left((r+2+\delta)\frac{n}{d_{a,\mu}}\right)}{(n-1)d_{a,\mu} \ln\left(\frac{\delta}{d_{a,\mu}}\right)}.$$

Le calcul de la dérivée seconde de $f : x \mapsto \dfrac{\ln\left((r+2+\delta)n\right)}{\ln\delta} x \ln\frac{\delta}{x} - \ln\left((r+2+\delta)\frac{n}{x}\right)$ montre qu'elle est concave donc, pour tout $x \in [1\,;n]$, $f(x) \geq \min\{0, f(n)\}$. Or, comme $\delta > n$,

$$f(n) = \frac{\ln\left((r+2+\delta)n\right)}{\ln\delta} n \ln\frac{\delta}{n} - \ln\left((r+2+\delta)\right) \geq \ln\left((r+2+\delta)\right)\left[\frac{n\ln\frac{\delta}{n}}{\ln\delta} - 1\right]$$

Pour que $f(n)$ soit positif, il suffit donc que $\delta \geq n^{\frac{n}{n-1}}$ et alors

$$\frac{\ln\left((r+2+\delta)\frac{n}{d_{a,\mu}}\right)}{d_{a,\mu}\ln\left(\frac{\delta}{d_{a,\mu}}\right)} \leq \frac{\ln((r+2+\delta)n)}{\ln(\delta)}.$$ (5)

Dès lors, comme $n \geq 17$ et comme la fonction $x \mapsto \frac{2x}{x-1}$ est décroissante sur $]1\,;+\infty[$

$$S_3 \leq (n-1)(m-1)\frac{17\delta}{8\ln\delta}\ln((r+2+\delta)n). \tag{5.49}$$

Pour finir, on utilise également la minoration $\ln N > \displaystyle\int_{N-1}^{N} \ln t\,\mathrm{d}t$ pour en déduire que, pour tous entiers $B > A \geq 2$, $\displaystyle\sum_{N=A}^{B} \ln N > \int_{A-1}^{B} \ln t\,\mathrm{d}t = B(\ln B - 1) + (A-1)(\ln(A-1) - 1)$ et donc

$$\sum_{N=A}^{B} \ln\left(\frac{r+\delta}{N}\right) < (B-A+1)\ln(r+\delta) - B(\ln B - 1) + (A-1)(\ln(A-1)-1) \tag{5.50}$$

Pour des valeurs données de r et δ, on peut alors facilement majorée S en utilisant (5.47), (5.48), (5.49) et (5.50). Illustrons cela dans le cas où $n = 17$ et $r = 10^5$ (et donc $m = 6$ et $N_0 = 76$). On calcule explicitement Δ_2 et on trouve

$$\ln\Delta_2 = 2\,321\,042{,}99325\ldots$$

et donc, de (5.39) et (5.41), on déduit que

$$\ln\Delta_{6,17,10^5} < 832\,485{,}44.$$

Ceci implique qu'on peut choisir $\varepsilon = 0{,}6$ et donc, en prenant $\delta = 50$ (6), on obtient

$$S = S_1 + S_2 + S_3 < 60\,000$$

et ainsi (5.46) est vérifiée. Ceci prouve que la proposition 5.4.8 est vraie pour $10^5 \leq r \leq 10^5 + 50$. En procédant de même pour les autres valeurs de $r \geq 50\,000$, on conclut que

$$\ln\Delta_{m,n,r} < k_n r$$

pour tout $r \geq 50\,000$.

Pour $1\,000 \leq r < 50\,000$, on calcule Δ_2 à partir de (5.42) comme précédemment. Pour les « petits » nombres premiers p, en revanche, i.e les nombres premiers p tels que

$$p \leq \Omega_{m,n,r} = \max\{\sqrt{nr+n+m}, 2n\}$$

(5). Nous avons donc besoin pour établir cette inégalité d'une condition sur δ plus forte que celle imposée par Bennett mais le cas $(n, \delta, d_{a,\mu}, r) = (17, 18, 16, 50000)$ montre que l'inégalité est fausse si on suppose seulement $\delta > n$.

(6). Ce qui est bien licite car $50 > 17^{\frac{17}{16}}$.

on n'utilise pas la majoration de Δ_0 mais on calcule ce nombre directement. On aboutit comme précédemment à

$$\ln \Delta_{m,n,r} < k_n r$$

pour $1\,000 \leq r < 50\,000$.

Finalement, si $1 \leq r \leq 1\,000$, on calcule directement

$$\frac{1}{r} \ln \Delta_{m,n,r}$$

et on vérifie qu'il ne dépasse pas k_n sauf pour un certain nombre de petites valeurs de r, la plus grande étant $r = 41$, correspondant à $n = 31$. On vérifie alors que, pour ces valeurs de r, on a

$$\frac{1}{r} \ln \Delta_{m,n,r} - k_n < \frac{1}{r} h_n.$$

Le maximum de

$$\frac{1}{r} \ln \Delta_{m,n,r} - k_n$$

correspond à $r = 1$ ou $r = 2$ sauf si $17 \leq n \leq 41$, $n = 47$ ou $59 \leq n \leq 73$. Dans tous les cas, le maximum est atteint pour $r \leq 23$.

Ceci achève la preuve de la proposition 5.4.8. ■

5.5 Démonstration du théorème 5.1.1

Nous pouvons à présent démontrer le théorème 5.1.1. Nous considérons, pour tout nombre premier $n \in [\![17, 337]\!]$, les constantes k_n et h_n définies par la proposition 5.4.8 et nous appliquons le lemme 5.2.1 en prenant $\theta = \left(\frac{a}{b}\right)^{\frac{1}{n}}$, $\ell = m - 1$ et

$$\forall r \in \mathbb{N}^* \quad \forall i \in [\![1, m]\!] \quad P_{i-1,r}(x) = \sum_{j=1}^{m} b^r \Delta_{m,n,r} A_{ij} \left(\frac{b-a}{b}, r\right) x^{j-1}.$$

Ainsi, avec les notations du lemme 5.2.1, pour tout $r \in \mathbb{N}^*$ et tout $(i, j) \in [\![0, m-1]\!]^2$, le nombre

$$a_{ij}(r) = b^r \Delta_{m,n,r} A_{i+1,j+1} \left(\frac{b-a}{b}, r\right)$$

est un entier par définition de $\Delta_{m,n,r}$.

Comme $\frac{b-a}{b} \neq 0$, la proposition 2.3.1 assure que la matrice $\left(A_{ij}\left(\frac{b-a}{a}, r\right)\right)_{(i,j)\in[\![1,m]\!]^2}$ est inversible et il en est donc de même de la matrice $(a_{ij}(r))_{(i,j)\in[\![0,m-1]\!]^2}$. Ainsi, l'hypothèse (5.1) est vérifiée.

Dans toute la suite, on pose $\tau = \frac{a}{b} > 1$.

Si $n = 17$, nous pouvons supposer, sans perte de généralité, que $\tau \leq 2$. En effet, par définition

$$\lambda = 5 \left(1 - \frac{\ln\left(\left(\tau^{\frac{1}{6}} + 1\right)^6 b\mathrm{e}^{8,98}\right)}{\ln\left(\left(\tau^{\frac{1}{6}} - 1\right)^6 b\mathrm{e}^{8,93}\right)}\right).$$

Or, pour tout réel $c > 0$, la dérivée de $f_b : x \mapsto 1 - \dfrac{\ln\left(\left(x^{\frac{1}{m}} + 1\right)^m b\mathrm{e}^{c+\frac{1}{20}}\right)}{\ln\left(\left(x^{\frac{1}{m}} - 1\right)^m b\mathrm{e}^{c}\right)}$ est du signe de

$$\begin{aligned} N(x) &= \ln\left(\left(\frac{x^{\frac{1}{m}}+1}{x^{\frac{1}{m}}-1}\right)^m \mathrm{e}^{\frac{1}{20}}\right) x^{\frac{1}{m}} + \ln\left(\left(x^{\frac{1}{m}}+1\right)^m b\mathrm{e}^{c+\frac{1}{20}}\right) + \ln\left(\left(x^{\frac{1}{m}}-1\right)^m b\mathrm{e}^{c}\right) \\ &\geq \ln\left(\left(\frac{x^{\frac{1}{m}}+1}{x^{\frac{1}{m}}-1}\right)^m \mathrm{e}^{\frac{1}{20}}\right) x^{\frac{1}{m}} \geq \frac{1}{20} x^{\frac{1}{m}} \end{aligned}$$

donc la fonction f_b est croissante et ainsi, pour tout $\tau > 2$, $f_b(\tau) > f_b(2)$. Par ailleurs, la dérivée de $g : b \mapsto 1 - \dfrac{\ln(\alpha b)}{\ln(\beta b)}$ est du signe de $\ln\alpha - \ln\beta$ donc $b \mapsto f_b(\frac{3}{2})$ est croissante. Il s'ensuit que $f_b(\tau) > f_1(2) > 4{,}6$ donc $\lambda = 5f_b(\tau) > 17$. Par ailleurs, pour $n \geq 17$,

$$nb(\theta+1)^{n-1} < nb(2\theta)^n = n2^n a < 5n^{m-1}a < K(n,a,b).$$

Dès lors, dans ce cas, le théorème 5.1.1 est une conséquence du théorème Liouville car

$$\left|\left(\frac{a}{b}\right)^{\frac{1}{n}} - \frac{p}{q}\right| > \frac{1}{nb(\theta+1)^{n-1}q^{17}} > \frac{1}{K(n,a,b)q^{\lambda(n,a,b)}}.$$

En généralisant cet argument pour de plus grandes valeurs de n, nous pouvons supposer que $\frac{a}{b}$ est majoré par 2 si $17 \leq n \leq 109$ et par 3 si $113 \leq n \leq 337$.

Par définition, pour tout $i \in [\![1, m]\!]$ et tout $z < 0$,

$$R_i(z,r) = \sum_{j=1}^{m} A_{ij}(z,r)(1-z)^{\frac{j-1}{n}}$$

donc, en remarquant que $\theta = \left(\frac{a}{b}\right)^{\frac{1}{n}} = \left(1 - \frac{b-a}{b}\right)^{\frac{1}{n}}$,

$$P_{i-1,r}(\theta) = \sum_{j=1}^{m} b^r \Delta_{m,n,r} A_{ij}\left(\frac{b-a}{b}, r\right)\theta^{j-1} = b^r \Delta_{m,n,r} R_i\left(\frac{b-a}{b}, r\right)$$

Dès lors, d'après le proposition 5.3.2 et la proposition 5.4.8, pour tout $i \in [\![1, m]\!]$,

$$|P_{i-1,r}(\theta)| \leq b^r \Delta_{m,n,r} \frac{\left|\frac{b-a}{b}\right|^m}{(m-1)!}\left|1 - \left(1 - \frac{b-a}{b}\right)^{\frac{1}{m}}\right|^{mr} \leq \frac{\left(\frac{a-b}{b}\right)^m}{(m-1)!} \mathrm{e}^{k_n r + h_n}\left(a^{\frac{1}{m}} - b^{\frac{1}{m}}\right)^{mr}$$

i.e. en posant $D = \left(\mathrm{e}^{k_n}\left(a^{\frac{1}{m}} - b^{\frac{1}{m}}\right)^m\right)^{-1} > 1$ par hypothèse,

$$\forall i \in [\![0, m-1]\!] \quad |P_{i,r}(\theta)| \leq \frac{(\tau-1)^m}{(m-1)!}\mathrm{e}^{h_n} D^{-r}.$$

En majorant, selon les cas, τ par 2 ou par 3, on vérifie que $\frac{(\tau-1)^m}{(m-1)!}\mathrm{e}^{h_n}$ est toujours inférieur $\mathrm{e}^{17{,}75}$ (le maximum étant atteint pour $n = 31$). Ainsi, en posant $d = \mathrm{e}^{17{,}75}$, on a, pour tout $i \in [\![0, m-1]\!]$ et tout $r \in \mathbb{N}^*$, $P_{i,r}(\theta) \leq dD^{-r}$ ce qui assure que l'hypothèse (5.3) est vérifiée.

D'après la proposition 5.3.3 et la proposition 5.4.8, pour tout $(i,j) \in [\![0, m-1]\!]^2$ et tout $r \in \mathbb{N}^*$,

$$|a_{ij}(r)| = \left|b^r \Delta_{m,n,r} A_{ij}\left(\frac{b-a}{b}, r\right)\right| \leq 2(r+1)\Phi_{m,n,r}^{m-1}\mathrm{e}^{k_n r + h_n}\left(a^{\frac{1}{m}} + b^{\frac{1}{m}}\right)^{mr}$$

car $\frac{1}{6}\left(1 - \frac{b-a}{b}\right) = \frac{\tau}{6} < 1$ puisque $\tau \leq 3$. En posant

$$C := \mathrm{e}^{k_n + \frac{1}{20}}\left(a^{\frac{1}{m}} + b^{\frac{1}{m}}\right)^m$$

on a donc pour tout $(i,j) \in [\![0, m-1]\!]^2$ et tout $r \in \mathbb{N}^*$,

$$|a_{ij}(r)| \leq 2(r+1)\Phi_{m,n,r}^{m-1}\mathrm{e}^{h_n - \frac{r}{20}} C^r$$

avec, rappelons-le,

$$\Phi_{m,n,r}^{m-1} = \max\left\{\frac{n^2}{n-1}r^{\frac{1}{n}}, \frac{n^2}{(m-1)(n-m+1)}r^{\frac{m-1}{n}}\right\}^{m-1}$$
$$= n^{m-1}\max\left\{\frac{n}{n-1}r^{\frac{1}{n}}, \frac{n}{(m-1)(n-m+1)}r^{\frac{m-1}{n}}\right\}^{m-1}.$$

Considérons les deux fonctions

$$f : r \mapsto \ln 2 + \ln(r+1) + (m-1)\ln\left(\frac{n}{n-1}\right) + \frac{m-1}{n}\ln r - \frac{1}{20}r$$

et

$$g : r \mapsto \ln 2 + \ln(r+1) + (m-1)\ln\left(\frac{n}{(m-1)(n-m+1)}\right) + \frac{(m-1)^2}{n}\ln r - \frac{1}{20}r.$$

Sur $[1\,;+\infty[$, la fonction f atteint son maximum en

$$r_f(n,m) := \frac{20(m-1) + 19n + \sqrt{40(m-1)(10m-10+21n) + 361n^2}}{2n}.$$

et, en calculant les valeurs correspondantes de f pour les différentes valeurs de n, on en déduit que, pour tout $r \in \mathbb{N}^*$, on peut majorer $f(r)$ par 4,092 (le maximum étant atteint pour $n = 337$ et $r = 26$).

De même, sur $[1\,;+\infty[$, la fonction g atteint son maximum en

$$r_g(n,m) := \frac{20(m-1)^2 + 19n + \sqrt{40(m-1)^2(10m^2-20m+10+21n) + 361n^2}}{2n}$$

et on vérifie que, pour tout $r \in \mathbb{N}^*$, $g(r) \leq 1{,}6$ (le maximum étant atteint pour $n = 17$ et $r = 49$).

On en déduit que

$$2(r+1)\Phi_{m,n,r}^{m-1}\mathrm{e}^{-\frac{r}{20}} \leq n^{m-1}\mathrm{e}^{4{,}092} < 59{,}86n^{m-1}.$$

Ainsi, si on pose

$$c := 59{,}86n^{m-1}\mathrm{e}^{h_n}$$

alors, pour tout $(i,j) \in [\![0, m-1]\!]^2$ et tout $r \in \mathbb{N}^*$,

$$|a_{ij}(r)| < cC^r$$

et donc l'hypothèse (5.2) est bien vérifiée.

Remarquons que, si on note $\delta = \max\left\{|\theta|, \left|\frac{p}{q}\right|\right\}$, alors on peut toujours supposer que

$$\max\left\{|\theta|, \left|\frac{p}{q}\right|\right\}^{m-2} < 3^{\frac{1}{3}}.$$

En effet, d'une part, comme $\frac{a}{b} \leq 3$, $\theta \leq 3^{\frac{1}{n}}$ donc $\theta^{m-2} \leq 3^{\frac{m-2}{n}} < 3^{\frac{1}{3}}$ car $m - 2 < \frac{n}{3}$. D'autre part, si $\left|\frac{p}{q}\right|^{m-2} \geq 3^{\frac{1}{3}}$ alors, pour toutes les valeurs de n considérées

$$\left|\theta - \frac{p}{q}\right| \geq \left|\frac{p}{q}\right| - \theta \geq 3^{\frac{1}{3(m-2)}} - 3^{\frac{1}{n}} > 5.10^{-5}$$

(le minimum étant atteint pour $n = 317$.) Or, dans l'expression de λ, le logarithme au numérateur est positif et supérieur au logarithme au dénominateur. Le quotient est donc inférieur à 1 et donc $\lambda \geq 0$. Ainsi, pour tout $q \geq 1$,

$$\frac{1}{Kq^\lambda} < \frac{1}{1{,}56 \times 10^{24}} < 5.10^{-5} < \left|\theta - \frac{p}{q}\right|$$

donc le théorème est vrai dans ce cas.

Pour le choix de t, prenons

$$t = \frac{n}{n-m+1}$$

Alors, pour tout n, on a bien $td > t > 1$ et, de plus, $(td)^{-\frac{1}{m-1}} \leq 0{,}85$ (le maximum étant atteint pour $n = 337$) donc le lemme est vrai pour tout $q \geq 1$. Enfin, remarquons que, si $\frac{\ln C}{\ln D} \geq \frac{n-m+1}{m-1}$, alors $\lambda \geq (m-1)\left(1 + \frac{n-m+1}{m-1}\right) = n$ donc le théorème est une nouvelle fois une conséquence du théorème de Liouville. Ainsi, on peut supposer que $\frac{\ln C}{\ln D} < \frac{n-m+1}{m-1}$ et donc on peut majorer $\frac{t}{t-1}\frac{(m-1)m}{2}\delta^{m-2}cC(td)^{\frac{\ln(C)}{\ln(D)}}$ par

$$\frac{n}{m-1} \times \frac{(m-1)m}{2} \times 3^{\frac{1}{3}} \times 59{,}86 \times n^{m-1} \times \mathrm{e}^{h_n}\mathrm{e}^{k_n+\frac{1}{20}}\left(a^{\frac{1}{m}} + b^{\frac{1}{m}}\right)^m \left(\frac{n}{n-m+1}\mathrm{e}^{17{,}75}\right)^{\frac{n-m+1}{m-1}}$$

Par conclure, il ne reste plus alors qu'à vérifier que

$$29{,}93 \times 3^{\frac{1}{3}} \times \mathrm{e}^{\frac{1}{20}}\frac{n}{m-1}\left(\frac{n}{n-m+1}\mathrm{e}^{17{,}75}\right)^{\frac{n-m+1}{m-1}}$$

est majoré par $1{,}56 \times 10^{24}$ pour les valeurs de n considérées (le maximum étant atteint pour $n = 19$). ■

5.6 Application à l'équation (F_n)

D'après les résultats du chapitre 4, pour $n \in [\![17, 337]\!]$, il nous reste à montrer que l'équation

$$(F_n) : (b+1)x^n - by^n = 1$$

n'a pas de solution non triviale (i.e. différente de $(1,1)$) pour $b \in [\![1, \lfloor c_n \rfloor - 1]\!]$ où c_n est définie par le tableau 3.2 p. 49. Pour cela, nous allons utiliser la même démarche que dans la section 4 du chapitre 4 en raisonnant sur les développements en fractions continuées.

On commence par montrer que le théorème (5.1.1) fournit des mesures effectives d'irrationalité des nombres $\sqrt[n]{1+\frac{1}{b}}$ qui permettent de borner les solutions de (F_n). Plus précisément, on a le lemme suivant.

Lemme 5.6.1. — *Si n est un nombre premier appartenant à $[\![17, 337]\!]$ et si b est un entier appartenant à $[\![1, \lfloor c_n \rfloor - 1]\!]$ avec $b \geq 2$ si $n \leq 47$ alors une solution (x, y) de l'équation (F_n) vérifie $x < 10^{728}$.*

Preuve. — Soit (x, y) une solution de (F_n). Alors, l'inégalité (1.7) établie dans la preuve du lemme 1.4.2 assure que

$$\left|\sqrt[n]{1+\frac{1}{b}} - \frac{y}{x}\right| < \frac{1}{nbx^n}$$

(autrement dit, $\frac{y}{x}$ est une très bonne approximation diophantienne de $\sqrt[n]{1+\frac{1}{b}}$). Or, d'après le théorème 5.1.1, pour tous entiers naturels non nuls x et y,

$$\left|\sqrt[n]{1+\frac{1}{b}} - \frac{y}{x}\right| > \frac{1}{Kx^\lambda}$$

donc,

$$\frac{1}{nbx^n} > \frac{1}{Kx^\lambda}$$

Si $\lambda < n$, on en déduit que

$$x < \left(\frac{K}{nb}\right)^{\frac{1}{n-\lambda}}.$$

Or, on vérifie que $\lambda < n$ pour tout n si $b \geq 2$ et pour tout $n \geq 53$ si $b = 1$ et que, pour ces valeurs, on a toujours $\left(\frac{K}{nb}\right)^{\frac{1}{n-\lambda}} < 10^{728}$, le maximum étant atteint pour $n = 79$ et $b = 1$. ■

La conclusion suit alors de la proposition suivante.

Proposition 5.6.2. — *Si b et n sont des entiers positifs avec $n \geq 17$ alors l'équation (F_n) n'a pas de solution $(x, y) \in \mathbb{N}^*$ telle que*

$$1 < x < 10^{728}.$$

Preuve. — Supposons que (F_n) admet une solution non triviale (x, y) telle que $x < 10^{728}$. Rappelons que, d'après le lemme (1.4.2), $\frac{y}{x}$ est une réduite $R_i = \frac{p_i}{q_i}$ (pour un certain $i \in \mathbb{N}^*$) dans le développement en fractions continuées de $\sqrt[n]{1 + \frac{1}{b}}$ et que, d'après (4.15), cette réduite correspond à un quotient partiel a_i vérifiant

$$a_i \geq nb(2nb)^{n-2} - 1$$

i.e. sachant que $n \geq 17$ et $b \geq 1$,

$$a_i > 10^{24}.$$

D'après le lemme 1.1.2, $x = q_i \geq \left(\frac{1+\sqrt{5}}{2}\right)^{i-1}$ donc $x < 10^{728}$ assure que $i \leq 3\,500$. Pour aboutir à une absurdité, il suffit donc d'examiner les 3 500 premiers quotients partiels de $\sqrt[n]{1 + \frac{1}{b}}$ pour les valeurs de n et b considérées et de vérifier qu'aucun d'eux ne dépasse 10^{24}. Le tableau donné en annexe C montre que le plus grand quotient partiel est $a_{2\,701} = 10\,564\,244$ obtenu pour $n = 193$ et $b = 21$ ce qui permet de conclure. ■

Ainsi, on peut conclure des deux résultats précédents que l'équation (F_n) n'a pas de solution non triviale si $b \geq 2$ et $n \in [\![17, 337]\!]$ ni si $b = 1$ et $n \in [\![53, 337]\!]$

Conclusion

Nous concluons par quelques remarques dans le cas $n \geq 3$. Tout d'abord, on a pu constater que la majorité des cas a été traitée grâce au théorème d'Evertse qui nous a permis de montrer que (E_n) admet au plus une solution non triviale sauf dans les cas suivants :

1. $a = b + 1$ avec $b \leq \lfloor c_n \rfloor - 1$ pour tout $n \geq 3$ (où c_n est défini par le tableau 3.2 p. 49) ;

2. pour $n = 3$,

$$x^3 - 26y^3 = 1 \qquad x^3 - 7y^3 = 1 \qquad 2x^3 - 15y^3 = 1 \qquad 3x^3 - 23y^3 = 1 \qquad 4x^3 - 31y^3 = 1$$
$$9x^3 - y^3 = 1 \qquad 17x^3 - 2y^3 = 1 \qquad 25x^3 - 3y^3 = 1 \qquad 28x^3 - y^3 = 1 \qquad 33x^3 - 4y^3 = 1$$

3. pour $n = 4$, $x^4 - 15y^4 = 1$ et $17x^4 - y^4 = 1$.

Ce résultat ne nécessitant pas de supposer que n soit premier, on en déduit qu'il permet de montrer le théorème 1 sauf dans les cas ci-dessus et ceci sans admettre les théorèmes de Nagell et Ljunggren (pour les cas $n = 3$ et $n = 4$) ni les résultats de Bennett et de Weger (pour $5 \leq n \leq 13$). Cela laisse donc un nombre fini de cas pour chaque valeur de n (mais, évidemment, un nombre total de cas infini).

L'utilisation des formes linéaires de logarithmes permet de borner n. Nous avons utilisé dans le chapitre 4 le fait que n est premier pour obtenir de meilleures constantes mais la démarche n'utilise pas cette hypothèse de façon déterminante et on pourrait reprendre l'étude, quitte à avoir une borne plus élevée, sans cette hypothèse et donc se ramener à un nombre fini de cas restants.

La démarche de Bennett, en revanche, utilise de façon essentielle la primalité de n notamment dans l'étude de la valuation $p-$adique des coefficients des approximants de Padé pour les grandes valeurs de p. Ainsi, avec ce que nous avons vu précédemment, nous ne pouvons pas espérer traiter complètement les cas $n \geq 17$ sans savoir que le théorème 1 est vrai pour les nombres premiers $n \leq 13$.

Les cas, pour $n = 4$ ou n premier, que nous n'avons pas traité par les méthodes décrites dans ce mémoire sont au final les suivants :

- pour $n = 3$, les équations de la forme $(b+1)x^3 - by^3 = 1$ avec $b \in [\![1, 36]\!]$ ainsi que les équations

$$x^3 - 26y^3 = 1 \qquad x^3 - 7y^3 = 1 \qquad 2x^3 - 15y^3 = 1 \qquad 3x^3 - 23y^3 = 1 \qquad 4x^3 - 31y^3 = 1$$
$$9x^3 - y^3 = 1 \qquad 17x^3 - 2y^3 = 1 \qquad 25x^3 - 3y^3 = 1 \qquad 28x^3 - y^3 = 1 \qquad 33x^3 - 4y^3 = 1$$

- pour $n = 4$, les équations de la forme $(b+1)x^4 - by^4 = 1$ avec $b \in [\![1, 16]\!]$ ainsi que les équations $x^4 - 15y^4 = 1$ et $17x^4 - y^4 = 1$;
- pour $n = 5$, les équations de la forme $(b+1)x^5 - by^5 = 1$ avec $b \in [\![1, 7]\!]$;
- pour $n = 7$, les équations de la forme $(b+1)x^7 - by^7 = 1$ avec $b \in [\![1, 6]\!]$;
- pour $n = 11$, les équations de la forme $(b+1)x^{11} - by^{11} = 1$ avec $b \in [\![1, 6]\!]$;
- pour $n = 13$, les équations de la forme $(b+1)x^{13} - by^{13} = 1$ avec $b \in [\![1, 6]\!]$;
- pour $n \in \{17, 19, 23, 29, 31, 37, 41, 43, 47\}$, l'équation $2x^n - y^n = 1$.

soit un total de 98 cas restants.

Il est peut-être possible de traiter ces cas avec des méthodes d'approximation diophantienne et notamment en obtenant des mesures effectives d'irrationalité. Par exemple, Bennett a montré dans [4] que, pour tous entiers naturels p et q avec $q > 0$,

$$\left| \sqrt[4]{17} - \frac{p}{q} \right| > \frac{3}{10q^{3,24}}.$$

Ainsi, en utilisant (1.7), une solution (x, y) de $17x^4 - y^4 = 1$ vérifie

$$\frac{3}{10x^{3,24}} < \left| \sqrt[4]{17} - \frac{y}{x} \right| < \frac{1}{4x^4}$$

ce qui impose $x \leq 16$. De plus, on sait que $\frac{y}{x}$ est une réduite dans le développement en fractions continuées de $\sqrt[4]{17}$. Or, la première réduite est $R_0 = \frac{2}{1}$ et, dès $R_1 = \frac{65}{32}$, on a un dénominateur supérieur à 16 ce qui permet de conclure que la seule solution de $17x^4 - y^4 = 1$ est $(1, 2)$.

Ainsi, soit en utilisant une méthode directe comme on vient de le faire quand on dispose d'une très bonne mesure d'irrationalité soit en étudiant les quotients partiels dans la suite des fractions continuées comme on l'a fait dans les paragraphes 4.4 et 5.6 (et en utilisant la remarque 1.4.3 dans le cas où $a < b$), on peut espérer traiter les cas restants par une méthode diophantienne et ainsi donner une démonstration du théorème 1 ne faisant pas du tout appel à des méthodes algébriques. Cela nécessite, bien sûr, de disposer de mesures effectives d'irrationalité pour les 97 nombres restants !

Annexe A

Sur une remarque de Mahler

Dans l'article [24], Mahler détermine les approximants de Hermite-Padé d'une famille de fonctions binomiales. Plus précisément, il montre que si ω_1, ..., ω_m sont des complexes tels que $\omega_i - \omega_j$ n'est jamais entier pour $i \neq j$ et si ρ_1, ..., ρ_m sont des entiers strictement positifs de somme $\sigma = \sum_{k=1}^{m} \rho_k$ alors, en posant, pour tout $j \in [\![1, m]\!]$,

$$A_j\left(z \left| \begin{array}{ccc} \omega_1 & \cdots & \omega_m \\ \rho_1 & \cdots & \rho_m \end{array} \right.\right) = (-1)^{\sigma-1}\Gamma(\rho_1)\ldots\Gamma(\rho_m) \sum_{h=0}^{\rho_j-1} \frac{(1-z)^h}{\Phi'(\omega_j+h)}$$

où

$$\Phi(z) = \prod_{k=1}^{m}\prod_{h=0}^{\rho_j-1}(z-\omega_j-h),$$

on définit m polynômes $A_j\left(z \left| \begin{array}{ccc} \omega_1 & \cdots & \omega_m \\ \rho_1 & \cdots & \rho_m \end{array} \right.\right)$ de degrés $\rho_j - 1$ tels que

$$R\left(z \left| \begin{array}{ccc} \omega_1 & \cdots & \omega_m \\ \rho_1 & \cdots & \rho_m \end{array} \right.\right) := \sum_{j=1}^{m} A_j\left(z \left| \begin{array}{ccc} \omega_1 & \cdots & \omega_m \\ \rho_1 & \cdots & \rho_m \end{array} \right.\right)(1-z)^{\omega_j}$$

admette en 0 une racine d'ordre exactement $\sigma - 1$.

Pour des valeurs de ω_1, ..., ω_m et ρ_1, ..., ρ_m fixées, Mahler définit ensuite la famille des polynômes $A_{ij}(z)$ en posant, pour tout $(i, j) \in [\![1, m]\!]^2$

$$A_{ij}(z) = A_j\left(z \left| \begin{array}{ccc} \omega_1 & \cdots & \omega_m \\ \rho_1+\delta_{i1} & \cdots & \rho_m+\delta_{im} \end{array} \right.\right)$$

où δ_{ij} est le symbole de Kronecker. Il définit également les fonctions R_i par

$$R_i(z) := \sum_{j=1}^{m} A_{ij}(z)(1-z)^{\omega_j}$$

qui, par définition, admettent en 0 une racine d'ordre σ.

Il démontre ensuite que la famille des polynômes $A_{ij}(z)$ est « indépendante » au sens où le déterminant $D(z) := \det_{1\leq i,j\leq m}(A_{ij}(z))$ n'est pas nul pour $z \neq 0$. Sa démonstration, qui est reprise dans la proposition 2.3.1, se fait sans calculer explicitement ce déterminant. Mahler ajoute, cependant, dans la note en bas de la page 272, qu'un calcul direct donne

$$D(z) = \pm \prod_{\substack{i,j=1 \\ i\neq j}}^{m} \frac{\Gamma(\omega_i-\omega_j)\Gamma(\rho_j)}{\Gamma(\rho_j+\omega_i-\omega_j)} z^{\sigma}.$$

Cette expression est erronée.

Prenons l'exemple simple $\omega_1 = 1$, $\omega_2 = \dfrac{1}{2}$, $\rho_1 = 2$ et $\rho_2 = 3$. Dans ce cas, on trouve

$$A_{11}(z) = -\frac{16}{15}z^2 + \frac{64}{5}z - \frac{256}{15} \qquad A_{12}(z) = \frac{16}{3}z^2 - \frac{64}{3}z + \frac{256}{15}$$
$$A_{21}(z) = \frac{32}{3}z - \frac{256}{15} \qquad A_{22}(z) = \frac{4}{15}z^3 + \frac{16}{5}z^2 - \frac{96}{5}z + \frac{256}{15}$$

ce qui donne

$$D(z) = -\frac{64}{225}z^5$$

Or,

$$\frac{\Gamma(\omega_1 - \omega_2)\Gamma(\rho_2)}{\Gamma(\rho_2 + \omega_1 - \omega_2)} \times \frac{\Gamma(\omega_2 - \omega_1)\Gamma(\rho_1)}{\Gamma(\rho_1 + \omega_2 - \omega_1)} = \frac{\Gamma(\frac{1}{2})\Gamma(3)}{\Gamma(\frac{7}{2})} \times \frac{\Gamma(-\frac{1}{2})\Gamma(2)}{\Gamma(\frac{3}{2})} = -\frac{64}{15} \neq -\frac{64}{225}.$$

En fait, on a plutôt

$$\det_{1\leq i,j\leq m}(A_{ij}(z)) = \prod_{\substack{i,j=1\\ i\neq j}}^{m} \frac{\Gamma(\omega_j - \omega_i - \rho_i)\Gamma(\rho_j)}{\Gamma(\omega_j + \rho_j - \omega_i - \rho_i)} z^{\sigma}.$$

Démontrons cette égalité. On a vu dans la proposition 2.3.1 qu'il existe une constante non nulle c telle que $D(z) = cz^{\sigma}$ et que, de plus, cette constante est le produit des coefficients dominants des polynômes A_{ii}. Explicitons cette constante c. Pour cela, nous utilisons le fait que

$$A_{ii}(z) = (-1)^{\sigma}\Gamma(\rho_1)\cdots\Gamma(\rho_i + 1)\cdots\Gamma(\rho_m)\sum_{h=0}^{\rho_i} \frac{(1-z)^h}{\phi'(\omega_i + h)}$$

où

$$\phi(z) = \prod_{k=1}^{m}\prod_{h=0}^{\rho_k + \delta_{ik} - 1}(z - \omega_k - h).$$

Si on note

$$F\left(z \,\middle|\, \begin{matrix}\omega\\ \rho\end{matrix}\right) = \prod_{h=0}^{\rho-1}(z - \omega - h)$$

alors il vient que

$$\phi(z) = \prod_{k=1}^{m} F\left(z \,\middle|\, \begin{matrix}\omega_k\\ \rho_k + \delta_{ik}\end{matrix}\right)$$

et

$$\phi'(z) = \sum_{k=1}^{m} F'\left(z \,\middle|\, \begin{matrix}\omega_k\\ \rho_k + \delta_{ik}\end{matrix}\right)\prod_{\substack{j=1\\ j\neq k}}^{m} F\left(z \,\middle|\, \begin{matrix}\omega_j\\ \rho_j + \delta_{ij}\end{matrix}\right).$$

Or,

$$F\left(\omega_i + \rho_i \,\middle|\, \begin{matrix}\omega_j\\ \rho_j + \delta_{i\ell}\end{matrix}\right) = \prod_{h=0}^{\rho_j + \delta_{ij} - 1}(\omega_i + \rho_i - \omega_j - h) = \begin{cases} 0 & \text{si } j = i \\ \dfrac{\Gamma(\omega_i + \rho_i - \omega_j + 1)}{\Gamma(\omega_i + \rho_i - \omega_j - \rho_j + 1)} & \text{sinon.}\end{cases}$$

et

$$F'\left(\omega_i + \rho_i \,\middle|\, \begin{matrix}\omega_i\\ \rho_i + \delta_{ii}\end{matrix}\right) = \sum_{h=0}^{\rho_i}\prod_{\substack{\ell=0\\ \ell\neq h}}^{\rho_i}(\omega_i + \rho_i - \omega_i - \ell) = \Gamma(\rho_i + 1)$$

donc

$$\phi'(\omega_i+\rho_i)=\Gamma(\rho_i+1)\prod_{\substack{j=1\\ j\neq i}}^{m}\frac{\Gamma(\omega_i+\rho_i-\omega_j+1)}{\Gamma(\omega_i+\rho_i-\omega_j-\rho_j+1)}.$$

Il s'ensuit que le coefficient dominant de $A_{ii}(z)$ est

$$(-1)^{\sigma+\rho_i}\Gamma(\rho_1)\cdots\Gamma(\rho_i+1)\cdots\Gamma(\rho_m)\frac{1}{\Gamma(\rho_i+1)}\prod_{\substack{j=1\\ \ell\neq i}}^{m}\frac{\Gamma(\omega_i+\rho_i-\omega_j-\rho_j+1)}{\Gamma(\omega_i+\rho_i-\omega_j+1)}$$

qui est égal à

$$(-1)^{\sigma+\rho_i}\prod_{\substack{j=1\\ j\neq i}}^{m}\frac{\Gamma(\rho_j)\Gamma(\omega_i+\rho_i-\omega_j-\rho_j+1)}{\Gamma(\omega_i+\rho_i-\omega_j+1)}$$

et donc

$$c=\prod_{i=1}^{m}(-1)^{\sigma+\rho_i}\prod_{\substack{j=1\\ j\neq i}}^{m}\frac{\Gamma(\rho_j)\Gamma(\omega_i+\rho_i-\omega_j-\rho_j+1)}{\Gamma(\omega_i+\rho_i-\omega_j+1)}=(-1)^{(m+1)\sigma}\prod_{i=1}^{m}\prod_{\substack{j=1\\ j\neq i}}^{m}\frac{\Gamma(\rho_j)\Gamma(\omega_i+\rho_i-\omega_j-\rho_j+1)}{\Gamma(\omega_i+\rho_i-\omega_j+1)}.$$

De plus, pour tout $z\in\mathbb{C}\setminus\mathbb{Z}$ et tout $n\in\mathbb{N}$, $\dfrac{\Gamma(z)}{\Gamma(z-n)}=(-1)^n\dfrac{\Gamma(-z+n+1)}{\Gamma(-z+1)}$ (voir, par exemple, [3] formule (3) p. 3) donc, en prenant $z=\omega_i+\rho_i-\omega_j+1$ et $n=\rho_j$, il vient

$$\frac{\Gamma(\omega_i+\rho_i-\omega_j+1)}{\Gamma(\omega_i+\rho_i-\omega_j-\rho_j+1)}=(-1)^{\rho_j}\frac{\Gamma(\omega_j-\omega_i-\rho_i+\rho_j)}{\Gamma(\omega_j-\omega_i-\rho_i)}.$$

Ainsi,

$$c=(-1)^{(m+1)\sigma}\prod_{i=1}^{m}\prod_{\substack{j=1\\ j\neq i}}^{m}(-1)^{\rho_j}\frac{\Gamma(\rho_j)\Gamma(\omega_j-\omega_i-\rho_i)}{\Gamma(\omega_j-\omega_i-\rho_i+\rho_j)}=(-1)^{(m+1)\sigma+(m-1)\sigma}\prod_{i=1}^{m}\prod_{\substack{j=1\\ j\neq i}}^{m}\frac{\Gamma(\rho_j)\Gamma(\omega_j-\omega_i-\rho_i)}{\Gamma(\omega_j-\omega_i-\rho_i+\rho_j)}$$

donc

$$c=\prod_{i=1}^{m}\prod_{\substack{j=1\\ j\neq i}}^{m}\frac{\Gamma(\rho_j)\Gamma(\omega_j-\omega_i-\rho_i)}{\Gamma(\omega_j-\omega_i-\rho_i+\rho_j)}.$$

■

Remarque. — On peut vérifier que cette égalité est cohérente avec l'exemple donné précédemment : si $\omega_1=1$, $\omega_2=\dfrac{1}{2}$, $\rho_1=2$ et $\rho_2=3$ alors

$$\frac{\Gamma(\rho_2)\Gamma(\omega_2-\omega_1-\rho_1)}{\Gamma(\omega_2-\omega_1-\rho_1+\rho_2)}\times\frac{\Gamma(\rho_1)\Gamma(\omega_1-\omega_2-\rho_2)}{\Gamma(\omega_1-\omega_2-\rho_2+\rho_1)}=\frac{\Gamma(3)\Gamma(-\frac{5}{2})}{\Gamma(\frac{1}{2})}\times\frac{\Gamma(2)\Gamma(-\frac{5}{2})}{\Gamma(-\frac{1}{2})}=-\frac{64}{225}.$$

Annexe B

Résultats numériques du chapitre 4

Le tableau suivant donne les résultats numériques issus de programmations sur Maple 16 et vérifiées ensuite sur Pari/GP. Les deuxième, troisième et quatrième colonnes indiquent respectivement la valeur de b pour laquelle le plus grand quotient partiel est rencontré, l'indice i de ce quotient partiel et la valeur a_i de celui-ci. La cinquième colonne, enfin, indique la valeur maximale du premier entier $k(b)$ tel que $q_{k(b)} > M_n$ pour les différentes valeurs de b. En d'autres termes, la dernière colonne donne, pour chaque valeur de n, le nombre maximal de réduite qu'il a été nécessaire de calculer pour l'ensemble de valeurs de $b \in [\![1, 165]\!]$.

n	b	i	a_i	$\max_{1\leq b\leq 165} k(b)$
347	10	1 196	203 417	1 839
349	150	484	1 817 451	1 121
353	165	2	58 420	598
359	118	78	146 902	403
367	165	2	60 737	252
373	165	2	61 730	185
379	165	2	62 723	149
383	165	2	63 385	131
389	165	2	64 378	106
397	165	2	65 702	85
401	165	2	66 364	72
409	165	2	67 688	64
419	165	2	69 343	50
421	165	2	69 674	46
431	165	2	71 329	42
433	165	2	71 660	41

n	b	i	a_i	$\max_{1\leq b\leq 165} k(b)$
439	165	2	72 653	34
443	165	2	73 315	29
449	165	2	74 308	27
457	165	2	75 632	25
461	165	2	76 294	22
463	165	2	76 625	22
467	165	2	77 287	19
479	165	2	79 273	16
487	165	2	80 597	14
491	165	2	81 259	12
499	165	2	82 583	11
503	165	2	83 245	11
509	165	2	84 238	9
521	165	2	86 224	6
523	165	2	86 555	6

Annexe C

Résultats numériques du chapitre 5

Le tableau suivant donne le plus grand quotient complet $a_k = a_k(n, b)$ rencontré dans le développement en fractions continuées de $\sqrt[n]{1 + \frac{1}{b}}$ pour n premier compris entre 17 et 337 et b entier compris entre 1 et $\lfloor c_n \rfloor - 1$. On a de plus indiqué, pour chaque valeur de n, les valeurs de b et de k pour lesquelles ce maximum est obtenu.

n	b	k	a_k
17	7	1 179	651 011
19	4	2 048	25 248
23	8	297	620 273
29	4	3 205	151 770
31	5	1 642	177 373
37	6	105	51 883
41	3	1 439	132 221
43	13	3 029	31 299
47	15	657	1 964 552
53	5	573	81 881
59	12	3 242	111 180
61	16	671	145 967
67	11	3 490	298 989
71	7	1 608	2 942 356
73	11	1 411	60 615
79	3	1 439	189 050
83	5	3 126	656 562
89	15	1 279	46 695
97	12	202	2 398 474
101	22	227	95 801
103	24	1 386	702 427

n	b	k	a_k
107	21	1 859	2 880 067
109	2	701	106 302
113	5	233	157 174
127	12	1 220	632 186
131	11	963	8 905 394
137	20	606	1 648 510
139	8	3 251	168 061
149	11	1 471	20 408
151	38	903	2 330 107
157	30	995	146 983
163	16	2 143	287 177
167	20	1 691	102 483
173	20	2 904	519 237
179	17	453	218 267
181	15	319	100 922
191	19	2 083	321 683
193	21	2 701	10 564 244
197	23	2 193	62 494
199	45	744	122 791
211	36	3 039	212 059
223	34	1 474	231 510

n	b	k	a_k
227	57	1 942	2 130 943
229	8	675	112 689
233	56	3 006	960 029
239	38	2 928	252 827
241	49	166	753 210
251	61	2 743	1 009 130
257	4	1 394	1 815 210
263	66	1 637	194 721
269	57	2 871	23 341
271	23	1 168	1 367 976
277	19	1 046	804 348
281	8	2 062	2 521 773
283	40	2 739	1 789 726
293	15	3 023	4 181 758
307	12	3 076	681 955
311	37	633	459 061
313	29	1 159	590 553
317	60	1 522	2 108 163
331	30	2 522	1 989 372
337	12	3 020	6 345 557

Bibliographie

[1] A. Baker – « Simultaneous rational approximations to certain algebraic numbers », *Proc. Camb. Phil. Soc.* **63** (1967), p. 693–702.

[2] — , *A concise introduction to the theory of numbers*, Cambridge University Press, 1984.

[3] H. Bateman et A. Erdélyi – *Higher Transcendental Functions*, vol. 1, McGraw-Hill, 1953.

[4] M. A. Bennett – « Explicit lower bounds for rational approximation to algebraic numbers », *Proc. London Math. Soc.* **75** (1997), p. 63–78.

[5] — , « Rational approximation to algebraic numbers of small height : the Diophantine equation $|ax^n - by^n| = 1$ », *J. Reine Angew. Math.* **525** (2001), p. 1–49.

[6] M. A. Bennett et B. M. M. de Weger – « On the diophantine equation $|ax^n - by^n| = 1$ », *Math. Comp.* **67** (1998), p. 413–438.

[7] G. V. Chudnovsky – « On the methode of Thue-Siegel », *Ann. Math. (II)* **117** (1983), p. 325–382.

[8] H. Darmon et L. Merel – « Winding quotients and some variants of Fermat's last Theorem », *J. Reine Angew. Math.* **490** (1997), p. 81–100.

[9] B. N. Delone – « Solution of the indeterminate equation $x^3q + y^3 = 1$ », *Izv. Akad. Nauk SSR (6)* **16** (1922), p. 253–272.

[10] Y. Domar – « On the diophantine equation $|Ax^n - By^n| = 1$, $n \geq 5$ », *Math. Scand.* **2** (1954), p. 29–32.

[11] D. Duverney – *Théorie des nombres*, 2nde éd., Dunod, 2007.

[12] J. H. Evertse – « On the equation $ax^n - by^n = c$ », *Comp. Math.* **47** (1982), p. 289–315.

[13] — , *Upper Bounds for the Numbers of Solutions of Diophantine Equations*, Mathematical Centre tracts, Mathematisch Centrum, 1983.

[14] G. H. Hardy et E. M. Wright – *An Introduction to the Theory of Numbers*, 6$^{\text{e}}$ éd., Oxford University Press, 1960.

[15] C. Hermite – « Sur la fonction exponentielle », *C. R. Math. Acad. Sci. Paris* **77** (1873), p. 18–24, 74–79, 226–233, 285–293.

[16] — , « Sur quelques approximations algébriques, extrait d'une lettre à M. Borchardt », Œuvre III, 1873, p. 146–149.

[17] — , « Sur la généralisation des fractions continues algébriques, Extrait d'une lettre à M. Pincherle », Œuvre IV, 1893, p. 357–377.

[18] M. Hindry – *Arithmétique*, Tableau noir, Calvage & Mounet, 2008.

[19] L. K. Hua – *Introduction to number theory*, Spinger-Verlag, 1982.

[20] H. Jager – « A multidimensional generalization of the Padé table I–VI », *Indagat. Math.* **26** (1964), p. 193–249.

[21] M. Laurent, M. Mignotte et Y. Nesterenko – « Formes linéaires en deux logarithmes et déterminants d'interpolation », *J. Number th.* **55** (1995), p. 285–321.

[22] H. Lenstra Jr – « Solving the Pell equation », *Notices Am. Math. Soc.* **49** (2002), p. 182–192.

[23] W. Ljunggren – « Einige Eigenschaften der Einheitenreeller quadratischer und rein biquatratischer Zahlkörper mit Anwendung auf die lösung einer klasse von bestimmter gleichungen vierten grades », *Det Norske Vidensk. Akad. Oslo Skrifter I* **12** (1936), p. 1–73.

[24] K. Mahler – « Ein Beweis des Thue-Siegelschen Satzes über die Approximation algebraischen Zahlen für binomische Gleichungen », *Math. Ann.* **105** (1931), p. 267–276.

[25] — , « Zur Approximation der Exponentialfunktion und des Logarithmus. Teil I. », *J. Reine Angew. Math.* **166** (1932), p. 118–150.

[26] M. Mignotte – « A note on the equation $ax^n - by^n = c$ », *Acta Arith.* **75** (1996), p. 287–295.

[27] R. A. Mollin – « Quadratic diophantine equations determined by continued fractions », *JP Jour. Algebra, Number Theory & Appl.* **1** (2001), p. 57–75.

[28] H. L. Montgomery et R. C. Vaughan – « The large sieve », *Mathematika* **20** (1973), p. 119–134.

[29] L. J. Mordell – *Diophantine Equations*, Academic Press, 1969.

[30] T. Nagell – « Solution complète de quelques équations cubiques à deux indéterminées », *J. de Math. (9)* **4** (1925), p. 209–270.

[31] I. Niven, H. S. Zuckerman et H. L. Montgomery – *An Introduction to the Theory of Numbers*, 5e éd., John Wiley & Sons, Inc., 1991.

[32] H. Padé – « Sur la représentation approchée d'une fonction par des fractions rationnelles », Thèse, 1892.

[33] — , « Mémoire sur les développements en fractions continues de la fonction exponentielle, pouvant servir d'introduction à la théorie des fractions continues algébriques », *Ann. Sci. Ec. Norm. Supér., 3e série,* **16** (1899), p. 395–426.

[34] — , « Sur l'expression générale de la fraction rationnelle approchée de $(1 + x)^m$ », *C. R. Math. Acad. Sci. Paris* **132** (1901), p. 754–756.

[35] O. Ramaré et R. Rumely – « Primes in arithmetic progressions », *Math. Comp.* **65** (1996), p. 397–425.

[36] J. B. Rosser et L. Schoenfeld – « Approximate formulas for some functions of primes numbers », *Ill. J. Math.* **6** (1962), p. 64–94.

[37] R. Rumely – « Numerical computations concerning the ERH », *Math. Comp.* **61** (1993), p. 415–440.

[38] C. L. Siegel – « Über einige Anwendungen diophantischer Approximationen », *Abh. Preuss. Akad. Wiss.* **1** (1929).

[39] — , « Die Gleichung $ax^n - by^n = c$ », *Math. Ann.* **114** (1937), p. 57–68.

[40] V. Tartakovskii – « Auflösung der Gleichung $x^4 - \rho y^4 = 1$ », *Izv. Akad. Nauk SSR (6)* **20** (1926), p. 301–324.

[41] A. Thue – « Bemerkungen Über gewisse Näherungsbrüche algebraischer Zahlen », *Kra. Vidensk. Selsk. Skrifter. I. Mat. Nat. Kl.* **3** (1908).

[42] — , « Über rationale Annäherungswerte der reellen Würzel der ganzen Funktion dritten Grades $x^3 - ax - b$ », *Kra. Vidensk. Selsk. Skrifter. I. Mat. Nat. Kl.* **6** (1908).