Un nouveau critère pour l'équation de Catalan

Yann Bugeaud & Guillaume Hanrot

1. Introduction

La première majoration explicite de la taille des solutions de l'équation superelliptique

$$f(x) = y^m \quad \text{en entiers } x, y \in \mathbf{Z}, \tag{1}$$

où $m \geq 3$ est un entier et $f(X) \in \mathbf{Z}[X]$ est un polynôme irréductible de degré $n \geq 2$, a été obtenue par Baker [2] comme application de ses travaux sur les formes linéaires de logarithmes. Par la suite, plusieurs auteurs ont amélioré et généralisé son résultat ; pour de plus amples informations, le lecteur est invité à se reporter à [5], où figurent de nombreuses références bibliographiques ainsi que les meilleures estimations actuellement connues, énoncées dans un cadre très général. Cependant, même pour $m = 3$ et $n = 2$, les bornes obtenues pour $|x|$ et $|y|$ sont très élevées (disons de l'ordre, au moins, de $10^{10^{10}}$), car doublement exponentielles en m et n et exponentielles en la hauteur de f. Il existe toutefois une autre approche, purement élémentaire, dite méthode de Runge [30], qui, sous certaines hypothèses, certes restrictives, conduit à des estimations explicites très nettement meilleures. Elle a été récemment développée par Walsh [34] et Le [18] ; en outre, peu auparavant, André [1] avait obtenu des résultats légèrement plus généraux au moyen de la théorie des G–fonctions.

Dans le présent travail, nous développons une troisième technique qui, à l'instar de la méthode de Runge, est complètement élémentaire et conduit à de très bonnes estimations explicites, mais ne s'applique pas à (1) en toute généralité. Elle se trouve en filigrane dans les articles de Bilu [3] et Bilu & Hanrot [4] relatifs à la résolution explicite de (1), mais n'a jusqu'à présent donné lieu à aucun énoncé précis. Nous comblons cette lacune et montrons comment cette approche s'applique à l'équation de Catalan et nous permet d'obtenir, sans faire appel à de lourds calculs, des résultats récents de Mignotte et Roy, ainsi que de nouveaux énoncés.

2. L'équation de Catalan

Une célèbre conjecture affirme que l'équation diophantienne, appelée équation de Catalan,

$$x^m - y^n = 1 \quad \text{avec} \quad m, n \geq 2 \quad \text{et} \quad |x|, |y| > 1,$$

admet pour unique solution la solution évidente $3^2 - 2^3 = 1$. Pour étudier ce problème, il suffit de se restreindre aux exposants premiers et donc à l'équation

$$x^p - y^q = 1 \quad \text{avec} \quad p, q \geq 2 \text{ premiers} \quad \text{et} \quad |x|, |y| > 1. \tag{2}$$

Il découle des travaux de V. A. Lebesgue [15], Nagell [27] et Ko Chao [12] que si (2) possède une solution autre que la solution triviale, alors p et q sont supérieurs ou égaux à 5. Cassels [6] a démontré en 1960 le résultat fondamental suivant, à la base de tous les travaux ultérieurs concernant (2) : si (x, y, p, q) vérifie (2), alors p divise y et q divise x. En outre, Tijdeman [33], au moyen de la théorie des formes linéaires de logarithmes, a prouvé de manière effective la finitude du nombre de solutions de (2), puis Langevin [13], suivant la même approche, a calculé des bornes explicites, certes élevées, pour les exposants des solutions de (2). Autre outil vers la résolution complète de (2) : deux critères importants démontrés par Inkeri [10, 11], et reposant sur le résultat de Cassels, permettent d'affirmer que, sous certaines hypothèses, une paire de nombres premiers (p, q) ne peut être une *paire d'exposants* pour l'équation de Catalan (*i.e.*, aucun quadruplet

(x,y,p,q) avec $|x|>1$ et $|y|>1$ ne vérifie (2)). Son second critère a été raffiné par Mignotte [23], puis par Schwarz [31]. L'énoncé suivant correspond au Theorem 1 de [31], il englobe et précise les résultats de [10], [11] et [23]. On rappelle que si $\mathbf{K}$ est un corps CM (*i.e.*, une extension quadratique imaginaire d'un corps totalement réel), son nombre de classes $h(\mathbf{K})$ est égal au produit $h^+(\mathbf{K})\cdot h^-(\mathbf{K})$, où $h^+(\mathbf{K})$ est le nombre de classes du sous-corps réel maximal de $\mathbf{K}$ et $h^-(\mathbf{K})$ est appelé le nombre de classes relatif.

Théorème S. *Soient $p\neq q$ deux nombres premiers. Soit $\mathbf{K}^{(p)}$ le plus petit sous-corps imaginaire du corps cyclotomique $\mathbf{Q}(\zeta_p)$, où ζ_p est une racine p-ième de l'unité, et soit $h^-(\mathbf{K}^{(p)})$ le nombre de classes relatif de $\mathbf{K}^{(p)}$. Alors (p,q) n'est pas une paire d'exposants pour (2) si*

$$q \nmid h^-(\mathbf{K}^{(p)}) \qquad \text{et} \qquad p^{q-1}\not\equiv 1 \pmod{q^2}.$$

En obtenant une condition sur $h^-(\mathbf{K}^{(p)})$ et non plus sur le nombre de classes de $\mathbf{K}^{(p)}$, Schwarz [31] a effectué un progrès considérable. En effet, il est important de rappeler que $h^+(\mathbf{K}^{(p)})$ est très difficile à calculer et n'est pas connu pour plusieurs nombres premiers inférieurs à 200, alors que $h^-(\mathbf{K}^{(p)})$ est donné par une formule “élémentaire”, et peut donc être calculé, pourvu que p ne soit pas trop grand.

Au moyen de longs calculs sur ordinateur, Mignotte & Roy [25] ont montré que le plus petit exposant p d'une éventuelle solution non triviale de (2) vérifie $p>10^5$. Plus précisément, le Théorème S leur a permis d'éliminer toutes les paires d'exposants (p,q), avec $p<10^5$, à l'exception de $(p,q)\in\mathcal{E}:=\{(83,4867),(911,318917),(2903,18787)\}$, pour lesquelles un nouveau critère basé sur des congruences s'est révélé efficace [21]. En outre, un des outils prépondérants est une minoration fine de formes linéaires en deux logarithmes [14] qui permet de borner très précisément un exposant en fonction de l'autre. Pour de plus amples informations, le lecteur est invité à consulter [23, 24, 25], ainsi que [29], où se trouvent détaillés les énoncés et les démonstrations des résultats antérieurs à 1992.

Le résultat suivant présente un nouveau critère assurant qu'une paire de nombres premiers impairs (p,q) avec $p<q$ n'est pas une paire d'exposants pour (2). On désigne par h_p^- le nombre de classes relatif du corps cyclotomique $\mathbf{Q}(\zeta_p)$.

Théorème 1. *Soient $q>p$ deux nombres premiers impairs. S'il existe des entiers $x>0$ et $y>0$ tels que $|x^p-y^q|=1$, alors q divise h_p^-.*

Le Théorème 1 entraîne les résultats suivants, qui ne sont pas nouveaux, mais que nous parvenons à démontrer indépendamment de la théorie des formes linéaires de logarithmes.

Corollaire 1. *Soit p un nombre premier impair fixé. Les quadruplets (x,y,p,q) solutions de (2) sont en nombre fini.*

La démonstration du Corollaire 1 étant courte, nous la présentons maintenant. Il découle du Théorème 1 qu'il suffit de prouver que pour $p\geq 3$ et q des nombres premiers fixés, il n'existe qu'un nombre fini d'entiers x et y vérifiant $x^p-y^q=1$. Or un tel résultat a été démontré (de manière ineffective) par Siegel [32].

À notre connaissance, il s'agit de la première démonstration connue du Corollaire 1 ne faisant pas appel à la théorie des formes linéaires de logarithmes.

À l'aide de la table des valeurs des h_p^-, que l'on peut trouver dans le livre de Washington [35], le Théorème 1 nous permet, d'un simple coup d'œil, de démontrer que de nombreuses paires (p,q) de nombres premiers ne peuvent être des paires d'exposants pour l'équation de Catalan. On obtient en particulier le résultat suivant, qui sans être nouveau, n'était pas connu en 1992, comme le montrent deux notes de Mignotte [20, 22]. Il est important de souligner que les résultats obtenus dans [23, 24, 25] font appel à la théorie des formes linéaires de logarithmes et ont requis de nombreux mois de calcul sur ordinateur. Par opposition, le Théorème 1 est complètement élémentaire.

Corollaire 2. *L'équation (2) n'admet, outre $(3,2,2,3)$, aucune solution (x,y,p,q) avec $\min\{p,q\}\leq 41$.*

Contrairement au Théorème 1, le Théorème S ne s'applique pas à la paire d'exposants (p,q) si celle-ci est une double paire de Wieferich, c'est-à-dire si l'on a à la fois $p^{q-1}\equiv 1 \pmod{q^2}$ et $q^{p-1}\equiv 1 \pmod{p^2}$. En outre, Ernvall & Metsänkylä [7] (et, indépendamment, Mignotte & Roy) ont montré récemment que l'ensemble $\mathcal{E}$ est exactement l'ensemble des paires de Wieferich (p,q) avec $p \geq 7$, $q \geq 7$ et p et q inférieurs à 10^6. Grâce au Théorème 1, il suffit donc de vérifier que si $(p,q) \in \mathcal{E}$, le nombre de classes h_p^- n'est pas divisible par q, pour conclure que (p,q) n'est pas une paire d'exposants pour (2). Ceci remplace le critère de congruences de Mignotte [21], qui nous a signalé n'avoir jamais publié de démonstration complète concernant la paire $(2903, 18787)$, pour laquelle le critère présenté dans [21] échoue (il convient en fait de se placer dans un corps quadratique avant d'utiliser des congruences). Le calcul des trois nombres de classes relatifs correspondants a nécessité moins d'une minute par la méthode de Fung, Granville et Williams [8], et permet de constater que le Théorème 1 s'applique dans ces trois cas.

Ce qui précède pourrait laisser croire au lecteur que le Théorème 1 est plus efficace que le Théorème S. Tel n'est cependant pas le cas en pratique, car ce dernier fait intervenir le plus petit sous-corps CM contenu dans le corps cyclotomique $\mathbf{Q}(\zeta_p)$ (en particulier le corps quadratique $\mathbf{Q}(\sqrt{-p})$ si p est congru à 3 modulo 4), dont le nombre de classes relatif se calcule en règle générale beaucoup plus rapidement que h_p^-.

Les informations concernant le nombre de classes relatif des corps cyclotomiques sont rares ; elles permettent néanmoins de déduire du Théorème 1 un nouveau critère pour l'équation de Catalan, dont l'application ne nécessite pas le calcul d'un nombre de classes.

Théorème 2. *Soit p un nombre premier de la forme $p = 2\ell + 1$, avec ℓ premier impair. Si $q > p$ est un nombre premier dont l'ordre modulo 2ℓ est supérieur ou égal à $(\ell - 1)/2$, alors (p,q) n'est pas une paire d'exposants pour l'équation de Catalan.*

Contrairement aux résultats précédents, le Théorème 2 utilise les bornes inférieures pour l'équation de Catalan obtenues par Mignotte & Roy [25]. Ses hypothèses sont certes très contraignantes, mais son intérêt principal est que son application ne requiert qu'un minimum de calcul. En outre, les arguments utilisés dans sa démonstration permettent de traiter la paire $(p,q) = (83, 4867)$ sans faire appel au critère de congruences de Mignotte [21], ni au calcul explicite de h_{83}^-, ni, en fait, aux minorations de [25]. Il suffit en effet de constater que l'ordre de 4867 modulo 41 est égal à 40. Par conséquent, si 4867 divise h_{83}^-, il ressort de la démonstration du Théorème 2 que 4867^{40} le divise également, mais cela rentre en contradiction avec le Lemme 2.

Remarque.— L'énoncé du Théorème 1 n'est pas symétrique en p et q. Cependant, un examen rapide de la démonstration montre que l'hypothèse $q > p$ n'intervient que lors de l'étude du cas où l'un des ℓ_j est nul, et qu'une hypothèse plus faible, par exemple $q > p\,(1 + 1/\log p)/2$, suffit afin d'obtenir une contradiction avec le Lemme 1. Il en découle alors le résultat suivant.

Théorème 3. *Soient $p < q$ deux nombres premiers impairs vérifiant $p > q\,(1 + 1/\log q)/2$. S'il existe des entiers rationnels $x > 0$ et $y > 0$ tels que $|x^p - y^q| = 1$, alors q divise h_p^- et p divise h_q^-.*

De la même manière, on peut facilement obtenir, sous des hypothèses convenables, d'autres énoncés symétriques en p et q. Il est cependant intéressant de noter qu'il existe des paires (p,q) de nombres premiers vérifiant q divise h_p^- et p divise h_q^-, par exemple les paires $(433, 842353)$ et $(4129, 761633)$.

Remarque. — L'équation diophantienne

$$\frac{x^n - 1}{x - 1} = y^q, \quad \text{en entiers } x > 1,\ y > 1,\ n > 2,\ q \geq 2, \tag{3}$$

étudiée par Nagell [27, 28] puis par Ljunggren [19], a fait l'objet de plusieurs articles récents, de la part notamment de Bennett, Bugeaud, Mignotte, Roy, Saradha et Shorey. Dans un travail ultérieur, nous montrerons comment l'approche utilisée ici permet de majorer la taille des solutions de l'équation (3), et de la résoudre pour certaines valeurs du couple (n,q).

3. Conditions d'application de la méthode

Pour que la méthode élémentaire présentée dans ce travail puisse être appliquée à une équation $f(x) = ay^p$, où p est un nombre premier impair, deux conditions doivent être réunies :

(a) Si $\mathbf{K} = \mathbf{Q}(\alpha, \beta)$ est un corps de nombres contenant deux racines de f, on a $(p, [\mathbf{K} : \mathbf{Q}]) = 1$;

(b) Suivant la terminologie de Bilu [3] et de Bilu & Hanrot [4], il n'y a qu'un seul *corps admissible*, à savoir $\mathbf{K}$.

Ce dernier point mérite d'être discuté plus avant.

Dans un souci de simplification, on supposera f irréductible et unitaire, bien que ce ne soit pas nécessaire, la méthode s'appliquant par exemple *mutatis mutandis* à l'équation de Catalan $y^q = x^p - 1$ sous sa forme originale. On notera Δ_f le discriminant de f.

Nous donnons ci-dessous quatre conditions qui, ensemble, suffisent à assurer la non-existence de corps admissibles autres que $\mathbf{K}$.

(*i*) [racines de l'unité] $(p, t_{\mathbf{K}}) = 1$, où $t_{\mathbf{K}}$ est le nombre de racines de l'unité de $\mathbf{K}$; cette hypothèse assure que toute racine de l'unité est une puissance p-ème.

(*ii*) [unités] Le corps $\mathbf{K}$ est CM ; cette hypothèse assure que pour toute unité u, l'entier algébrique $u/\overline{u}$ est une racine de l'unité.

(*iii*) [premiers] Tout idéal premier $\mathfrak{p}$ de $\mathbf{K}^+$ divisant $a\Delta_f$ est inerte ou se ramifie dans l'extension $\mathbf{K}/\mathbf{K}^+$. Par conséquent, tout générateur τ de $\mathfrak{p}$ est tel que $\tau/\overline{\tau}$ est un entier algébrique dont tous les conjugués sont de module 1, donc est une racine de l'unité.

(*iv*) [groupe des classes] $(p, h^-(\mathbf{K})) = 1$, hypothèse qui permet de contrôler la contribution du groupe des classes d'idéaux, *cf.* la démonstration du Théorème 1.

Le lecteur remarquera que les deux hypothèses les plus restrictives, à savoir *(ii)* et *(iii)*, sont indépendantes de p, et que les hypothèses (a), *(i)* et *(iv)* sont réalisées pour tout p premier à l'exception d'un ensemble fini.

4. Résultats auxiliaires

Grâce au résultat de Cassels [6] relatif à l'équation de Catalan, Hyyrö [9] est parvenu à minorer, pour toute éventuelle solution non triviale de (2), les valeurs absolues de x et y. Le lemme suivant, combiné aux majorations que nous obtenons par la méthode de Bilu [3], nous permet de démontrer le Théorème 1.

Lemme 1. *Si $u \geq 5$ et $v \geq 5$ sont des nombres premiers tels qu'il existe des entiers $x > 0$ et $y > 0$ vérifiant $x^u - y^v = 1$, alors $x > 10^{11}$, $y > 10^{11}$ et*

$$x \geq \max\{u^{v-1}(v-1)^v + 1, v(2u+1)(2v^{u-1}+1)\},$$

$$y \geq \max\{v^{u-1}(u+1)^u - 1, u(v-1)(u^{v-1}(v-1)^v + 1)\}.$$

Démonstration. Il s'agit du Satz 2 et du Hilfssatz 2 de Hyyrö [9]. □

Le Théorème 1 affirme que si p est un nombre premier fixé et si $q > p$ est premier, le couple (p, q) ne peut être une paire d'exposants que si q divise le nombre de classes relatif h_p^- du corps cyclotomique engendré par une racine p-ième de l'unité. Les renseignements concernant ce nombre h_p^- sont rares ; on sait toutefois le majorer de manière satisfaisante, comme l'illustre le résultat suivant, sur lequel repose la démonstration du Théorème 2.

Lemme 2. *Pour tout nombre premier p, on a la majoration*

$$h_p^- \leq 2\,p\left(\frac{p}{4\,\pi^2}\right)^{(p-1)/4}(\log p)^5\, e^{15.49+4.66/\log p}.$$

Démonstration. Il s'agit d'un résultat de Lepistö [17], qui a également donné une minoration explicite de h_p^-, montrant ainsi que le Lemme 2 ne peut être substantiellement amélioré. □

5. Démonstrations

Démonstration du Théorème 1. Soient $q > p$ deux nombres premiers impairs et soient x et y deux entiers non nuls vérifiant $x^p - y^q = 1$. Nous supposons que q ne divise pas h_p^-. Notre objectif consiste à majorer très finement $|x|$, afin de rentrer en contradiction avec les minorations de Hyyrö énoncées au Lemme 1.

Au vu des résultats de V. A. Lebesgue [15], Nagell [27] et Ko Chao [12], on a $p \geq 5$. En outre, il résulte des travaux de Cassels [6] qu'il existe un entier v tel que

$$\frac{x^p - 1}{x - 1} = p\, v^q.$$

Notons ζ une racine primitive p-ième de l'unité, $\mathbf{K}$ le corps cyclotomique engendré par ζ et $\mathbf{K}^+$ le sous–corps totalement réel maximal inclus dans $\mathbf{K}$. On rappelle que dans le corps $\mathbf{K}$, l'idéal (p) est totalement ramifié et est égal à l'idéal $(1-\zeta)^{p-1}$. De plus, pour $2 \leq j \leq p-1$, le plus grand diviseur commun aux idéaux $(x-\zeta)$ et $(x-\zeta^j)$ divise $(1-\zeta)$, qui est un idéal premier. Soit maintenant $\mathfrak{p}$ un idéal premier tel que $\mathfrak{p}$ divise $(x-\zeta)$ avec un exposant premier à q. Il s'ensuit immédiatement que $\mathfrak{p}$ divise soit p, soit $x - \zeta^j$ pour une certaine valeur de j ; dans les deux cas, $\mathfrak{p}$ est alors égal à l'idéal premier $(1-\zeta)$. Il existe donc un entier ℓ compris entre 0 et $q-1$ et un idéal entier $\mathfrak{a}$ de $\mathbf{K}$ tel que $(x-\zeta) = (1-\zeta)^\ell \mathfrak{a}^q$. En comparant les normes des deux membres, on constate que ℓ est nécessairement égal à 1 et que donc

$$\left(\frac{x-\zeta}{1-\zeta}\right) = \mathfrak{a}^q. \tag{4}$$

Nous reprenons un argument de Schwarz [31] afin de déduire de (4), sous l'hypothèse $q \nmid h_p^-$, une égalité entre nombres algébriques. Notons $C_{\mathbf{K}}$ (*resp.* $C_{\mathbf{K}^+}$) le groupe des classes d'idéaux de $\mathbf{K}$ (*resp.* de $\mathbf{K}^+$), et Ψ l'application canonique $C_{\mathbf{K}^+} \to C_{\mathbf{K}}$. Comme Ψ est injective (*cf.* [35], Theorem 4.14), on a

$$\mathrm{Card}\, \frac{C_{\mathbf{K}}}{\Psi(C_{\mathbf{K}^+})} = h_p^-,$$

et, q et h_p^- étant premiers entre eux, on déduit de (4) que la classe de $\mathfrak{a}$ est l'image par Ψ de la classe d'un idéal de $\mathbf{K}^+$. Il existe ainsi $\alpha \in \mathbf{K}^*$ et $\mathfrak{b}$ un idéal de $\mathbf{K}^+$ tels que $\mathfrak{a} = (\alpha)\mathfrak{b}$. En outre, l'idéal $\mathfrak{b}^q$ étant principal, il existe $\beta \in \mathbf{K}^+$ et une unité $\eta_0 \in \mathbf{K}$ tels que

$$\frac{x-\zeta}{1-\zeta} = \eta_0\, \beta\, \alpha^q.$$

Or, pour toute unité ε d'un corps cyclotomique, $\varepsilon/\overline{\varepsilon}$ est une racine de l'unité, donc il existe η une racine de l'unité de $\mathbf{K}$ et $\theta \in \mathbf{K}$ tels que

$$\frac{x-\zeta}{x-\overline{\zeta}} = \eta\, \theta^q.$$

En outre, η est une puissance q-ième dans $\mathbf{K}$ car $q \neq p$. Ainsi $(x-\zeta)/(x-\overline{\zeta})$ est également la puissance q-ième d'un élément de $\mathbf{K}$, et, choisissant la détermination de la fonction $z \mapsto z^{1/q}$ définie par $-\pi/q < \arg z^{1/q} \leq \pi/q$, il existe ξ une racine primitive q-ième de l'unité et un entier ℓ_1 tels que

$$\xi^{\ell_1} \left(\frac{x-\zeta}{x-\overline{\zeta}}\right)^{1/q} \in \mathbf{K}.$$

Suivant la terminologie de Bilu & Hanrot [4] (voir aussi le travail antérieur de Bilu [3]), on se trouve dans le cas où l'unique *corps admissible* est le corps $\mathbf{K}$: on peut alors borner $|x|$ sans faire appel à la théorie de Baker et, par conséquent, obtenir des bornes bien meilleures que dans la situation générale. À cet effet, on considère (*cf.* [3, 4]) la quantité

$$\varphi(x) := (x-\overline{\zeta})\left(\xi^{\ell_1}\left(\frac{x-\zeta}{x-\overline{\zeta}}\right)^{1/q} - 1\right)^q,$$

qui est un entier algébrique appartenant à $\mathbf{K}$, car il existe un entier ℓ tel que

$$\varphi(x) = \left((x-\zeta)^{1/q} - \xi^{\ell}\,(x-\overline{\zeta})^{1/q}\right)^{q}.$$

En outre, comme $\prod_{0\le j\le q-1}\left((x-\zeta)^{1/q} - \xi^{j}\,(x-\overline{\zeta})^{1/q}\right)^{q} = (\overline{\zeta}-\zeta)^{q}$, il vient

$$\mathrm{N}_{\mathbf{K}/\mathbf{Q}}\varphi(x) \mid p^{q}. \tag{5}$$

Cependant, on a vu que $x-\overline{\zeta}$ diffère de $1-\zeta$ d'une puissance q-ième. Donc $\varphi(x)$ diffère également de $1-\zeta$ d'une puissance q-ième. Or l'idéal $(1-\zeta)$ est premier et sa norme vaut p. Ainsi, il existe un rationnel $\lambda > 0$ tel que $|\mathrm{N}_{\mathbf{K}/\mathbf{Q}}\varphi(x)| = p\,\lambda^{q}$, et il découle de (5) que

$$|\mathrm{N}_{\mathbf{K}/\mathbf{Q}}\varphi(x)| = p. \tag{6}$$

Il s'agit maintenant d'obtenir une autre estimation de $|\mathrm{N}_{\mathbf{K}/\mathbf{Q}}\varphi(x)|$. Pour cela, on procède exactement comme dans [4] et on considère les conjugués sur $\mathbf{K}$ de $\varphi(x)$, lesquels s'écrivent, pour $1 \le j \le p-1$,

$$\varphi_j(x) := (x-\overline{\zeta}^{j})\left(\xi^{\ell_j}\left(\frac{x-\zeta^{j}}{x-\overline{\zeta}^{j}}\right)^{1/q} - 1\right)^{q},$$

où les ℓ_j sont des entiers appartenant à $\{0,1,\ldots,q-1\}$, dépendant de la détermination de la fonction $z \mapsto z^{1/q}$ choisie. Malheureusement, nous ne savons pas contrôler précisément les ℓ_j.

- Premier cas : on suppose les ℓ_j tous non nuls.

Par le Lemme 1, on peut supposer $|x| \ge 10^{11}$, donc, pour tout $1 \le j \le p-1$, la quantité

$$\Lambda_j := \left|\xi^{\ell_j}\left(\frac{x-\zeta^{j}}{x-\overline{\zeta}^{j}}\right)^{1/q} - 1\right|$$

est minorée par $(1-10^{-10})\,|e^{2i\pi/q}-1|$ et, comme $q \ge 5$, on a $\Lambda_j \ge 5/q$. Ainsi, on obtient

$$|\mathrm{N}_{\mathbf{K}/\mathbf{Q}}\varphi(x)| \ge \left|\frac{x^{p}-1}{x-1}\right|\left(\frac{5}{q}\right)^{q(p-1)} \ge \frac{|x|^{p-1}}{2}\left(\frac{5}{q}\right)^{q(p-1)}.$$

Combiné à (6), cela mène à

$$|x| \le 4\left(\frac{q}{5}\right)^{q}. \tag{7}$$

- Second cas : l'un au moins des ℓ_j est nul.

Du fait de la conjugaison complexe, le nombre de ℓ_j non nuls est pair. On le note $2a$, avec $a > 0$. La quantité Λ_j définie ci-dessus est majorée par 3 lorsque ℓ_j est non nul, et par $3/(q|x|)$ sinon. Ainsi, compte tenu de (6), on obtient

$$p = |\mathrm{N}_{\mathbf{K}/\mathbf{Q}}\varphi(x)| \le \left|\frac{x^{p}-1}{x-1}\right| 3^{q(p-1)}\left(\frac{1}{q|x|}\right)^{2aq},$$

d'où, comme $q \ge p+2$, la majoration

$$|x| \le 3^{p}. \tag{8}$$

Ainsi, comme $q > p$, les estimations (7) et (8) entraînent

$$|x| \le 4\left(\frac{q}{5}\right)^{q} + 3^{q}. \tag{9}$$

Il nous reste à montrer que l'estimation (9) entre en contradiction avec le Lemme 1. Pour cela, on considère des nombres premiers $q > p \geq 5$ et des entiers strictement positifs x et y tels que $x^p - y^q = \pm 1$. On a alors $(\pm x)^p - (\pm y)^q = 1$ et, si q ne divise pas h_p^-, il découle de (9) la majoration $|x| \leq 4\,(q/5)^q + 3^q$ qui n'est pas compatible avec la conclusion du Lemme 1. □

Démonstration du Théorème 2. Avec les notations de Lehmer [16] et sous nos hypothèses, h_p^- est (*cf.* [16], formule (14)), à une puissance de $2p$ près, égal au produit de deux entiers $h_2(p)$ et $h_{2\ell}(p)$. Il découle des formules (9) et (10) de [8] que $h_2(p)$ ne possède aucun facteur premier strictement supérieur à p. Soit $q > p$ un nombre premier tel que (p, q) est une paire d'exposants pour Catalan. Le Théorème 1 entraîne que q divise h_p^- ; par conséquent, q divise $h_{2\ell}(p)$. Le Lemma 3 de Lehmer [16] affirme alors que q divise $h_{2\ell}(p)$ avec un exposant multiple de l'ordre de q modulo 2ℓ. Si cet ordre est supérieur ou égal à $(\ell - 1)/2$, il s'ensuit que h_p^- est au moins égal à $(p+2)^{(p-3)/4}$. Cette minoration contredit le Lemme 2 dès que p est supérieur à 10^5 et on sait (*cf.* [24]) que (2) n'a pas de solution non-triviale si le plus petit des exposants est inférieur à 10^5 : le Théorème 2 est donc démontré. □

6. Remerciements

Les auteurs tiennent à exprimer leur gratitude à Maurice Mignotte pour son soutien et ses conseils tout au long de la rédaction du présent article.

Références bibliographiques

[1] Y. André, *G–functions and Geometry*, Vieweg, Braunschweig 1989.

[2] A. Baker, Bounds for the solutions of the hyperelliptic equation, *Proc. Camb. Phil. Soc.* **65** (1969), 439–444.

[3] Y. Bilu, Solving superelliptic Diophantine equations by the method of Gelfond–Baker, preprint 94–09, Mathématiques Stochastiques, Univ. Bordeaux 2 (1994).

[4] Y. Bilu et G. Hanrot, Solving superelliptic Diophantine equations by Baker's method, *Compositio Math.* **112** (1998), 273–312.

[5] Y. Bugeaud, Bounds for the solutions of superelliptic equations, *Compositio Math.* **107** (1997), 187–219.

[6] J.W.S. Cassels, On the equation $a^x - b^y = 1$, II, *Proc. Cambridge Society* **56** (1960), 97–103.

[7] R. Ernvall et T. Metsänkylä, On the p-divisibility of Fermat quotients, *Math. Comp.* **66** (1997), 1353–1365.

[8] G. Fung, A. Granville et H. C. Williams, Computation of the First Factor of the Class Number of Cyclotomic Fields, *J. Number Theory* **42** (1992), 297–312.

[9] S. Hyyrö, Über das Catalansche Problem, *Ann. Univ. Turku* Ser. AI **79** (1964), 3–10.

[10] K. Inkeri, On Catalan's problem, *Acta Arith.* **9** (1964), 285–290.

[11] K. Inkeri, On Catalan's conjecture, *J. Number Th.* **34** (1990), 142–152.

[12] Ko Chao, On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$, *Sci. Sinica* **14** (1965), 457–460.

[13] M. Langevin, Quelques applications de nouveaux résultats de van der Poorten, *Sém. Delange-Pisot-Poitou* (1977/78), Paris, Exp. 4, 7 pages.

[14] M. Laurent, M. Mignotte et Y. Nesterenko, Formes linéaires en deux logarithmes et déterminants d'interpolation, *J. Number Th.* **55** (1995), 285–321.

[15] V. A. Lebesgue, Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$, *Nouv. Ann. Math.* **9** (1850), 178–181.

[16] D. H. Lehmer, Prime factors of cyclotomic class numbers, *Math. Comp.* **31** (1977), 599–607.

[17] T. Lepistö, On the growth of the first factor of the class number of the prime cyclotomic field, *Ann. Acad. Sci. Fenn. Ser. A1 Math.* **577** (1974), 21 pages.

[18] Maohua Le, A note on the integer solutions of hyperelliptic equations, *Colloq. Math.* **68** (1995), 171–177.

[19] W. Ljunggren. Noen Setninger om ubestemte likninger av formen $(x^n-1)/(x-1)=y^q$, *Norsk. Mat. Tidsskr.* **25** (1943), 17–20.

[20] M. Mignotte, Sur l'équation de Catalan, *C. R. Acad. Sci. Paris* **314** (1992), 165–168.

[21] M. Mignotte, Un critère élémentaire pour l'équation de Catalan, *C.R. Math. Rep. Acad. Sci. Canada* **15** (1993), 199–200.

[22] M. Mignotte, Sur l'équation de Catalan (II), *Theoretical Computer Science* **123** (1994), 145–149.

[23] M. Mignotte, A criterion on Catalan's equation, *J. Numb. Th.* **52** (1995), 280–283.

[24] M. Mignotte et Y. Roy, Catalan's equation has no new solution with either exponent less than 10651, *Experimental Mathematics* **4** (1995), 259–268.

[25] M. Mignotte et Y. Roy, Minorations pour l'équation de Catalan, *C. R. Acad. Sci. Paris* **324** (1997), 377–380.

[26] M. Mignotte et Y. Roy, Lower Bounds for Catalan's Equation, *The Ramanujan J.* **1** (1997), 351–356.

[27] T. Nagell, Des équations indéterminées $x^2+x+1=y^n$ et $x^2+x+1=3y^n$, *Nordsk. Mat. Forenings Skr. (1)* **2** (1920), 14 pages.

[28] T. Nagell. Note sur l'équation indéterminée $(x^n-1)/(x-1)=y^q$, *Norsk. Mat. Tidsskr.* **2** (1920), 75–78.

[29] P. Ribenboim. *Catalan's Conjecture.* Academic Press, Boston (1994).

[30] C. Runge, Ueber ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen, *J. reine angew. Math.* **100** (1887), 425–435.

[31] W. Schwarz, A note on Catalan's equation, *Acta Arith.* **72** (1995), 277–279.

[32] C. L. Siegel, Uber einige Anwendungen diophantischer Approximationen, *Abh. Preuss. Akad. Wiss. Phys.-math. Kl.*, **1** (1929), 70 pages.

[33] R. Tijdeman, On the equation of Catalan, *Acta Arith.* **29** (1976), 197–209.

[34] P. G. Walsh, A quantitative version of Runge's theorem on diophantine equations, *Acta Arith.* **62** (1992), 157–172.

[35] L.C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1982.

Yann Bugeaud
Université Louis Pasteur
U. F. R. de mathématiques
7, rue René Descartes
67084 STRASBOURG

e-mail : `bugeaud@math.u-strasbg.fr`

Guillaume Hanrot
Projet POLKA, INRIA Lorraine
Technopôle de Nancy-Brabois
615, rue du Jardin Botanique, B.P. 101
54600 VILLERS-LÈS-NANCY

e-mail : `Guillaume.Hanrot@loria.fr`