Sur l'équation diophantienne $\frac{x^n-1}{x-1}=y^q$, *III*

Yann Bugeaud, Guillaume Hanrot *&* Maurice Mignotte

1. Introduction

Vraisemblablement, l'équation diophantienne

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

possède uniquement les trois solutions

$$\frac{3^5-1}{3-1}=11^2, \ \frac{7^4-1}{7-1}=20^2 \text{ et } \frac{18^3-1}{18-1}=7^3, \tag{$\mathcal{S}$}$$

mais on ne sait cependant pas démontrer qu'elle n'en admet qu'un nombre fini. Les premiers résultats relatifs à (1) sont l'œuvre de Ljunggren [25] et de Nagell [32, 33], qui l'ont résolue complètement si, respectivement, $q=2$ et n est un multiple de 3 ou de 4, les seules solutions étant celles mentionnées ci-dessus. Pour de plus amples informations, et en particulier pour des énoncés assurant la finitude du nombre de solutions sous certaines hypothèses, le lecteur est invité à consulter les travaux de Shorey & Tijdeman [40, 41], ou encore le chapitre 4 du survol de Shorey [39].

Tout récemment, d'importants progrès concernant (3) ont été réalisés par Bennett, Bugeaud, Mignotte, Roy, Saradha et Shorey [3, 7, 10, 11, 12, 13, 35] et l'on sait maintenant, par exemple, que (1) ne possède aucune solution si x est un carré [3, 13, 35] ou si x est une puissance de 10 [10].

Dans le présent travail, nous étendons les résultats de Ljunggren et Nagell en résolvant (1) quand n est divisible par 5 ou par 7. Alors que leurs démonstrations sont élémentaires, dans le sens où elles ne font appel qu'à des arguments astucieux ou classiques en théorie algébrique des nombres, la nôtre combine diverses techniques diophantiennes, dont les minorations de formes linéaires de logarithmes. L'idée consiste à regarder (1) comme une équation superelliptique et à borner la taille de ses solutions (x,y) en fonction de n et de q. À cet effet, sous certaines conditions portant sur n et q, peu restrictives toutefois, il est possible d'appliquer une méthode dont l'origine remonte à des travaux de Bilu [4] et Bilu & Hanrot [5], et qui a déjà été utilisée avec succès dans le cadre de l'équation de Catalan par Bugeaud & Hanrot [9]. Les estimations qui en découlent sont alors suffisamment fines pour que, en criblant modulo des nombres premiers bien choisis, on parvienne, en un temps raisonnable, à résoudre complètement (1) pour des petites valeurs de n et q. Comme la théorie des formes linéaires de logarithmes nous permet de contrôler q en fonction de n, on peut ainsi, par exemple, résoudre complètement (1) avec $n = 5$. Dans le cas $n \geq 7$, il est nécessaire d'avoir recours à des idées maintenant classiques de réduction des bornes, basées sur des méthodes d'approximation diophantienne effective de type fractions continues ou algorithme LLL.

Il convient d'insister sur le fait que rares sont les exemples de résolution complète d'équations diophantiennes exponentielles $f(x) = y^q$ en inconnues x, y, $q \geq 2$, où f est un polynôme à coefficients entiers de degré ≥ 3. Les techniques classiques assurent, si par exemple f possède trois racines distinctes, que le nombre de solutions est fini, mais les bornes explicites que l'on obtient sont très élevées. Ici, nous tirons parti de la forme particulière de f, qui est un polynôme cyclotomique, afin d'aborder ce problème sous un angle différent.

Ce travail est organisé de la façon suivante. Nous présentons nos résultats dans la partie qui suit, où nous établissons également un parallèle entre (1) et l'équation de Catalan. La troisième partie est consacrée à un lemme auxiliaire relatif à (1) et, dans la quatrième, nous montrons comment les formes linéaires en deux logarithmes s'appliquent à (1) pour majorer q en fonction de n, quand n est un nombre premier. L'avant-dernière partie est consacrée à l'obtention d'une borne élémentaire pour l'entier x, sous certaines hypothèses sur n et q. Enfin, la dernière partie explique comment exploiter cette borne pour résoudre l'équation dans les cas où la borne est trop grande pour mettre en œuvre une énumération exhaustive des valeurs de x (ou de y) restant possibles. Un appendice regroupant des données numériques conclut le présent travail.

2. Résultats

Le résultat principal de ce travail est le suivant.

Théorème 1. *Le quadruplet $(3, 11, 5, 2)$ est la seule solution (x, y, n, q) de l'équation (1) avec n multiple de 5, 7, 11 ou 13.*

Dans toute la suite, les lettres p et q désignent des nombres premiers impairs : on ne se préoccupe pas de (1) avec $q = 2$ puisqu'elle a été résolue par Nagell et Ljunggren.

Avant d'énoncer nos autres résultats, nous montrons comment sont étroitement liées l'équation (1) et l'équation de Catalan, et nous donnons les grandes lignes de la démonstration du Théorème 1.

Soient p et q des nombres premiers impairs. Pour que (1) n'ait pas de solution (x, y, n, q) avec n multiple de p, il suffit, d'après le Lemme 1 ci-dessous, que p soit congru à 1 modulo q ou, sinon, de prouver que les équations

$$\frac{x^p - 1}{x - 1} = y^q \tag{2}$$

et

$$\frac{x^p - 1}{x - 1} = p\, y^q \tag{3}$$

n'ont que des solutions triviales. Cette dernière équation apparaît également dans l'étude de l'équation de Catalan

$$x^p - y^q = 1. \tag{4}$$

De façon plus précise, pour l'équation de Catalan, on écrit

$$(x-1)\frac{x^p - 1}{x-1} = y^q$$

et on sait depuis Cassels [18] que p divise $x-1$, ce qui donne en particulier une relation de la forme

$$\frac{x^p - 1}{x-1} = p\, y_1^q,$$

où y_1 est un diviseur de y : nous retrouvons ainsi l'équation (3).

En 1976, R. Tijdeman [42] a montré que l'équation (4) ne possède qu'un nombre fini de solutions non triviales (p,q,x,y). Il a obtenu ce résultat en minorant deux formes linéaires de logarithmes de nombres rationnels, l'une en deux logarithmes et l'autre en trois logarithmes. Dans le cas $p \not\equiv 1 \pmod 8$, Mignotte et Roy ont amélioré (voir [27] et [31]) les estimations obtenues par la méthode de Tijdeman en considérant des formes linéaires en deux logarithmes de nombres algébriques et en les minorant par les résultats très précis de [21]. Un des buts du présent travail est de montrer que cette méthode s'applique aux équations (2) et (3) et conduit, même lorsque p est congru à 1 modulo 8, à d'excellentes majorations pour q, inaccessibles par les méthodes classiques, lesquelles reposent sur des minorations de formes linéaires en au moins trois logarithmes. Les détails sont donnés dans la partie 4, mais notons d'ores et déjà que les formes linéaires de logarithmes que nous considérons sont obtenues à partir de la démonstration de différents critères sur l'équation de Catalan (voir [19], [20], [28] et aussi un travail de T. Nagell [33]).

Nous avons ainsi réduit notre problème à la résolution des équations (2) et (3) pour des "petites" valeurs de q. Si q est différent de p et ne divise pas le nombre de classes relatif du p-ème corps cyclotomique (condition vérifiée pour tout $p \leq 19$), la méthode décrite dans [9] et inspirée de travaux de Bilu et de Bilu & Hanrot s'applique aux équations (2) et (3), et permet d'obtenir de très bonnes majorations pour x et y. Les bornes précises sont explicitées dans la partie 5, ainsi que le crible qui permet de conclure. Dans le cas $q = p$, que nous appelons *cas diagonal*, la situation s'avère plus délicate et nous n'avons pas d'autre choix que de résoudre (2) et (3) à l'aide des algorithmes décrits dans [5], qui sont malheureusement trop lourds à mettre en œuvre dès que $p = q \geq 11$. Comme le montre l'énoncé ci–dessous, le cas diagonal est le seul que l'on ne sache pas résoudre quand p et q sont tous les deux petits.

Théorème 2. *Si (x,y,n,q) est une solution de (1) n'appartenant pas à $\mathcal{S}$ et si p est un diviseur premier impair de n, alors ou bien $p \geq 29$ ou bien $(p,q) \in \{\,(17,17),\ (19,19),\ (23,23)\}$.*

Remarque : Il est envisageable, au prix de calculs assez lourds, d'améliorer la borne 29 du Théorème 2 ; il faut toutefois toujours exclure le cas (p,p) pour $p \geq 17$, qu'il n'est pas réaliste d'espérer traiter par les méthodes présentées.

On ne sait pas démontrer que (1) n'a qu'un nombre fini de solutions (x, y, n, q) avec $q = 3$, cependant de telles solutions, si elles existent, vérifient

- $n \equiv 5 \pmod 6$ (résultat dû à Ljunggren [25]),
- n est une puissance de nombre premier (Corollary 1.2 (d) de Bennett [3]).

La méthode développée dans ce travail nous permet d'affiner ces résultats.

Théorème 3. *Si les entiers $n \geq 4$, $x > 1$ et $y > 1$ vérifient*

$$\frac{x^n - 1}{x - 1} = y^3,$$

alors il existe un nombre premier p congru à 5 modulo 6, et $a \geq 1$ tels que $n = p^a$. De plus, $p \geq 101$.

Remarque : En utilisant le Théorème 6 et le Lemme 1 ci-dessous, il est possible de montrer que si l'on suppose en outre dans le Théorème 3 que $h^-(\mathbf{Q}(\zeta_p))$ (le nombre de classes relatif du p-ème corps cyclotomique) n'est pas un multiple de 3, alors $n = p$ ou p^2. On constate qu'environ 56 % des nombres premiers p compris entre 100 et 5000 satisfont cette hypothèse portant sur $h^-(\mathbf{Q}(\zeta_p))$.

Le dernier énoncé complète les Théorèmes 1, 2 et 3 et présente d'autres paires (p, q) que nous sommes parvenus à traiter.

Théorème 4. *Si (x, y, n, q) est une solution de (1) n'appartenant pas à $\mathcal{S}$ et si p est un diviseur premier impair de n, alors $(p, q) \notin \{(29, 5), (29, 19), (29, 23), (31, 23), (37, 5), (37, 7), (37, 11), (67, 5)\}$.*

Remarque : Notre méthode nous permet en outre de retrouver l'un des résultats de Nagell et Ljunggren mentionné dans l'introduction, à savoir de résoudre (1) lorsque n est un multiple de 3.

3. Résultat auxiliaire

L'étude de l'équation (3) se trouve grandement facilitée par le résultat de factorisation suivant, complémentaire du Lemma 7 de Shorey [38].

Lemme 1. *Soit $n > 3$ un entier non divisible par 4 et soit q un nombre premier impair. Ecrivons n sous la forme $n = 2^c\, p^k\, d$ avec $k \geq 1$, $c \in \{0, 1\}$ et p premier impair ne divisant pas d. Si l'équation*

$$\frac{x^n - 1}{x - 1} = y^q$$

admet une solution vérifiant $x > 1$, alors $p \not\equiv 1 \pmod q$ et l'une des équations

$$\frac{x^p - 1}{x - 1} = y^q, \qquad \frac{x^p - 1}{x - 1} = p\, y^q$$

admet une solution vérifiant $x > 1$.

Démonstration : Sous l'hypothèse du lemme, la démonstration du résultat (A8.2) de Ribenboim [34] montre que l'équation $(x^{p^k} - 1)/(x-1) = y^q$ admet alors une solution avec $x > 1$. Or nous savons (il s'agit du Corollary 1.2 (a) de Bennett [3], démontré indépendamment et au moyen de techniques différentes par Mignotte [29]) que l'équation (1) n'admet aucune solution (X, Y, N, Q) vérifiant $N \equiv 1 \pmod{Q}$ et $Q \geq 3$. On en déduit que q ne divise pas $p^k - 1$, et donc, comme $k \geq 1$, que q ne divise pas $p - 1$. La dernière assertion du lemme est contenue dans l'énoncé (A8.2) de Ribenboim [34]. □

4. Majoration de q en fonction de p

Soient a un entier non nul et f un polynôme à coefficients entiers et à racines simples, de degré $n \geq 2$. Tijdeman [42] (*cf.* également le chapitre 10 de [41]) a démontré que l'équation diophantienne

$$f(x) = a\, y^m \quad \text{en entiers } m \geq 0, x, y \notin \pm 1, 0$$

entraîne que m est majoré par une constante effective ne dépendant que de f et de a. Une version explicite de ce résultat se trouve dans une note de Bugeaud [8], qui prouve, dans le cas particulier où f est unitaire de hauteur (ici, la hauteur d'un polynôme à coefficients entiers est le maximum des valeurs absolues de ceux-ci) égale à H et de discriminant égal à D, que l'on a

$$m < \max\left\{n \log(2H+3),\ 2^{15(n+6)}\, n^{7n}\, |D|^{3/2}\, (\log |D|)^{3n}\, \log^3 |3a|\right\}.$$

La démonstration repose entre autres sur des minorations de formes linéaires en $r + 3$ logarithmes, où r désigne ici le rang du groupe des unités d'un corps de nombres engendré par une racine de f. C'est en raison de l'absence d'estimations très fines pour les formes linéaires en $m \geq 3$ logarithmes que l'on obtient par cette approche des constantes numériques élevées, beaucoup trop grandes pour pouvoir traiter le problème qui nous intéresse. Cependant, dans le cas très particulier des équations (1) et (2), il s'avère en fait possible de ne faire appel qu'à des formes linéaires en deux logarithmes. Ainsi, grâce aux estimations très précises de [21], on obtient le résultat suivant.

Théorème 5. *Soit p un nombre premier impair. Alors les équations (2) et (3) ne peuvent avoir de solutions non triviales que pour*

$$q \leq 9000\, p^2 \log^4 p.$$

En outre, si p n'est pas congru à 1 modulo 8, on dispose de la majoration plus fine

$$q \leq 64000\, p \log^2 p.$$

Enfin, pour $p = 5, 7, 11, 13, 17, 19, 23$*, nous obtenons respectivement les bornes* 5521, 25404, 41784, 213949, 197658, 72123, 87523.

Remarque : Les deux premières majorations de q sont obtenues en appliquant, respectivement, le Corollaire 1 et le Théorème 3 de [21]. Pour les petites valeurs de p, nous avons cependant besoin d'estimations plus fines. À cet effet, nous avons utilisé le Théorème 1 de [21], avec un choix ad hoc des paramètres, et en tenant compte de la minoration $y \geq 2p+1$, qui découle des travaux sur les diviseurs primitifs (voir par exemple [34], page 17). En pratique, nous avons obtenu de meilleures bornes sous diverses hypothèses sur y, et vérifié celles-ci en énumérant les y correspondants dans les intervalles requis. On consultera l'appendice pour une table des bornes utilisées.

Nous présentons maintenant la démonstration de la première assertion du Théorème 5.

a. Préliminaires algébriques.

Soit (x, y, p, q) une solution de (2) ou de (3). Notons $\zeta_p = e^{2i\pi/p}$ et $\mathbf{L}$ le corps cyclotomique $\mathbf{Q}(\zeta_p)$.

Ecrivons $p-1 = d\,f$, avec f et d des entiers que l'on choisira ultérieurement. Désignons par g une racine primitive modulo p. Alors le groupe de Galois $\mathrm{Gal}(\mathbf{L}/\mathbf{Q})$ est cyclique, engendré par la transformation $\sigma : \zeta_p \mapsto \zeta_p^g$. Si $\tau = \sigma^d$ alors $\tau(\zeta_p) = \zeta_p^m$ où $m = g^d \bmod p$. Désignons par $\mathbf{K}$ le sous-corps de $\mathbf{L}$ qui est invariant sous l'action de τ. Alors $\mathbf{K}$ est un corps de degré d et $\mathbf{K} = \mathbf{Q}(\xi)$ où $\xi = \zeta_p + \zeta_p^m + \cdots + \zeta_p^{m^{f-1}}$; en outre $\mathrm{Gal}(\mathbf{K}/\mathbf{Q}) = \{1, \sigma, \ldots, \sigma^{d-1}\}$. On désigne par $h_{\mathbf{K}}$ le nombre de classes de $\mathbf{K}$. Dans le cas où f est impair, le corps $\mathbf{K}$ est de type CM et $\rho := \sigma^{d/2}$ est la conjugaison complexe ; en outre, $h_{\mathbf{K}}$ 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 un entier, appelé le nombre de classes relatif.

Posons

$$A(X) = \prod_{j=0}^{f-1} (X - \zeta_p^{m^j}) = N_{\mathbf{L}/\mathbf{K}}(X - \zeta_p),$$

$$\beta = \begin{cases} 1, & \text{dans le cas de l'équation (2),} \\ A(1) = \prod_{j=0}^{f-1}(1 - \zeta_p^{m^j}), & \text{dans le cas de l'équation (3),} \end{cases}$$

et

$$\hat{p} = \begin{cases} 1, & \text{dans le cas (2),} \\ p, & \text{dans le cas (3).} \end{cases}$$

Nous obtenons alors $\prod_{i=0}^{d-1} \sigma^i(\beta) = \hat{p}$ dans les deux cas.

Dans le corps $\mathbf{K}$, nous avons la factorisation

$$y^q = \delta_1 \cdots \delta_d, \qquad \delta_i = \sigma^{i-1}\big(A(x)/\beta\big), \quad i = 1, \ldots, d,$$

où les δ_i sont des entiers de $\mathbf{K}$ premiers entre eux deux à deux (voir [20]). Si $q \nmid h_{\mathbf{K}}$ il existe un entier algébrique α et une unité η de $\mathbf{K}$ tels que

$$A(x) = \eta \beta \alpha^q.$$

Un argument dû à Schwarz [36] montre que si $\mathbf{K}$ est un corps de type CM, alors l'hypothèse $q \not| h_{\mathbf{K}}^-$ suffit pour obtenir une factorisation analogue à la précédente.

On suppose d'abord $f > 1$ et impair. Comme les seules racines de l'unité appartenant à $\mathbf{K}$ sont ± 1 et que $\mathbf{K}$ est un corps de type CM, ceci implique que $\bar{\eta} = \pm\eta$. Remarquons aussi que (dans tous les cas)

$$A^\rho(X) = \prod_{j=0}^{f-1}(X - \zeta_p^{-m^j}) = \prod_{j=0}^{f-1}(\zeta_p^{m^j}X - 1) = -X^f \prod_{j=0}^{f-1}(X^{-1} - \zeta_p^{m^j}) = -X^f A(1/X),$$

la seconde égalité résultant de la congruence $1 + m + \cdots + m^{f-1} \equiv 0 \pmod p$, elle-même conséquence des relations $m^f \equiv g^{df} \equiv 1 \pmod p$.

En particulier, on a ici $A^\rho(X) = \bar{A}(X)$ et $\bar{\beta} = \bar{A}(1) = -A(1) = -\beta$ dans le cas (3). Donc $\bar{A}(x) = \pm\beta\eta\bar{\alpha}^q$. De plus la preuve de [28] montre que $\bar{A}(x) \neq A(x)$. D'où les relations

$$\frac{\bar{A}(x)}{A(x)} = \pm\left(\frac{\bar{\alpha}}{\alpha}\right)^q = \prod_{j=0}^{f-1}\left(\frac{x - \zeta_p^{m^j}}{x - \zeta_p^{-m^j}}\right) = \prod_{j=0}^{f-1}\left(\frac{1 - \zeta_p^{m^j}/x}{1 - \zeta_p^{-m^j}/x}\right) \neq 1. \qquad (11)$$

Si l'on choisit $f = 1$, on a $\mathbf{K} = \mathbf{L}$ et $\bar{\eta} = \xi\eta$, où ξ est une racine de l'unité, donc $\xi = \pm\zeta_p^j$ et, quitte à remplacer α par $\pm\zeta_p^k\alpha$ avec k convenable, on aboutit encore à la relation (11).

Le dernier cas qui nous servira est celui où $\mathbf{K} = \mathbf{Q}(\sqrt{p})$ (dans ce cas $p \equiv 1$ modulo 4 et f est pair), pour lequel on a $A(x) = \eta\beta\alpha^q$ et $A^\rho(x) = \rho(\eta\beta)\big(\rho(\alpha)\big)^q$, d'où

$$\frac{A^\rho(x)}{A(x)} = \eta'\left(\frac{\rho(\alpha)}{\alpha}\right)^q,$$

où η' est une unité de $\mathbf{K}$. Si ε (> 1) est l'unité fondamentale de $\mathbf{K}$, on en déduit

$$\frac{A^\rho(x)}{A(x)} = \varepsilon^j\gamma^q \qquad (12)$$

avec $\gamma \in \mathbf{K}$ et j entier, $|j| \leq q/2$.

b. Les formes linéaires en deux logarithmes.

Clairement,

$$\frac{A^\rho(x)}{A(x)} = 1 + O\left(\frac{1}{x}\right).$$

De manière précise, on a $|x| > 2$, ce qui implique $|\log(1 + z/x)| < \frac{2}{|x|}$ pour tout nombre complexe z de module 1 (où log désigne la détermination principale du logarithme) et donc

$$\Lambda := \left|\log\frac{A^\rho(x)}{A(x)}\right| \leq \sum_{j=0}^{f-1}\left|\log\frac{1 - \zeta_p^{m^j}/x}{1 - \zeta^{-m^j}/x}\right| < \frac{4f}{|x|}. \qquad (13)$$

Supposons que le corps $\mathbf{K}$ ne soit pas réel. Il existe alors un entier rationnel k, avec $|k| \leq q$, tel que

$$\Lambda = |q \log(\bar{\alpha}/\alpha) - ki\pi| \neq 0.$$

Comme le nombre algébrique $\bar{\alpha}/\alpha$ est racine du polynôme à coefficients entiers

$$\prod_{i=0}^{d-1} \sigma^j(\bar{\alpha} - \alpha X) = N_{\mathbf{K}/\mathbf{Q}}(\alpha) X^d + \cdots,$$

et que tous ses conjugués sont de module 1, on a

$$\mathrm{h}(\bar{\alpha}/\alpha) = \frac{1}{d} \log |N_{\mathbf{K}/\mathbf{Q}}(\alpha)| = \frac{\log |y|}{d}, \tag{14}$$

puisque $N_{\mathbf{K}/\mathbf{Q}} A(x) = \pm N_{\mathbf{K}/\mathbf{Q}}(\beta) \cdot N_{\mathbf{K}/\mathbf{Q}}(\alpha^q) = \pm \hat{p} y^q$, où h désigne la hauteur logarithmique absolue (définie par exemple dans [21]).

Nous supposons désormais de plus que p n'est pas congru à 1 modulo 8 et que $p-1 = 4f$ ou $2f$, avec f impair. Le corps $\mathbf{K}$ est alors le plus petit sous-corps CM de $\mathbf{L}$ et l'on déduit de (13) l'estimation

$$\Lambda < \frac{2p}{|x|}. \tag{15}$$

En appliquant le Théorème 3 de [21], on a la minoration

$$\log |\Lambda| \geq -8.87 a H^2,$$

où $D = [\mathbf{K} : \mathbf{Q}]/2 = d/2 \leq 2$ et

$$a \geq \max\Big\{20,\ 10.98 |\log(\bar{\alpha}/\alpha)| + D\mathrm{h}(\bar{\alpha}/\alpha)\Big\},$$
$$H = \max\Big\{17,\ \frac{\sqrt{D}}{10},\ D \log\left(\frac{|k|}{2a} + \frac{q}{68.9}\right) + 2.35D + 5.03\Big\}.$$

Un calcul élémentaire s'appuyant sur (14) et sur la minoration $y \geq 11$ montre ensuite que l'on peut choisir

$$a = 12 \log |y| + 16 \quad \text{et} \quad H = \max\Big\{2 \log\left(q\left(\frac{1}{2a} + \frac{1}{68.9}\right)\right) + 9.73, 17\Big\}^2$$

obtenant ainsi, par (15)

$$\log |x| \leq \log 2p + 8.87(12 \log |y| + 16) \max\Big\{2 \log\left(q\left(\frac{1}{2a} + \frac{1}{68.9}\right)\right) + 9.73, 17\Big\}^2.$$

La relation $(x^p - 1)/(x - 1) = \hat{p} y^q$ entraîne $|x^p| > |y|^q$, et, comme $|y| \geq 11$ et $p \geq 5$, il vient

$$q \leq 0.42\, p \log 2p + 237\, p \Big\{\log\left(\frac{q}{27}\right) + 9.73\Big\}^2,$$

d'où
$$q \leq 64000\, p \log^2 p. \tag{16}$$

Supposons maintenant que le corps $\mathbf{K}$ est quadratique réel et donc que $p-1 = 2f$ avec f pair. D'après (12), nous devons alors considérer la forme linéaire en deux logarithmes de nombres algébriques réels
$$\Lambda' = |j \log \varepsilon + q \log \gamma|.$$
Une partie des calculs précédents s'applique encore, en particulier la majoration (15) reste valable pour Λ'. On sait (voir par exemple [17], page 199) que l'on a
$$\log \varepsilon \leq \sqrt{p} \log(4p)$$
et le même calcul que (14) montre que
$$\begin{aligned} q\mathrm{h}(\gamma) &\leq \mathrm{h}\left(\frac{A^p(x)}{A(x)}\right) + |j|\mathrm{h}(\varepsilon) \\ &\leq \frac{\log p}{2} + \frac{q \log y}{2} + \frac{q}{2}(\sqrt{p}\log(4p)). \end{aligned}$$
Comme $q \geq 3$, afin de minorer Λ', on peut alors appliquer le Corollaire 1 de [21] avec
$$\log A_1 = \frac{\sqrt{p}\log(4p)}{2}, \qquad \log A_2 = \frac{1}{2}\big(\log|y| + \sqrt{p}\log(6p)\big)$$
et
$$b' = \frac{q}{2}\left(\frac{1}{\log A_1} + \frac{1}{2\log A_2}\right),$$
et, compte-tenu de (15), cela donne
$$\log|x| \leq \log(2p) + 123.6\,(\sqrt{p}\log 4p)\,(\log|y| + \sqrt{p}\log 6p)\, \max\{\log b', 10.5\}^2.$$
Comme $|x|^p > |y|^q$ avec $|y| \geq 2p+1$ et $p \geq 5$, on en déduit aussitôt
$$q \leq 67.8\, p^2\,(\log 4p)\,(\log 6p)\, \log^2(q/5),$$
d'où
$$q \leq 9000\, p^2 \log^4 p. \tag{17}$$

Les majorations (16) et (17) reposent respectivement sur l'hypothèse $(q, h_{\mathbf{K}}^-) = 1$, quand $\mathbf{K}$ est de type CM, et sur l'hypothèse q ne divise pas $h_{\mathbf{K}}$ sinon, c'est-à-dire lorsque $\mathbf{K}$ est un corps quadratique réel. Compte-tenu des majorations des nombres de classes, nous avons, dans le premier cas considéré, $h_{\mathbf{K}}^- \leq p^2 \log p$ (cela se déduit des majorations de Louboutin [26]) et, dans le second, $h_{\mathbf{K}} \leq \sqrt{p}\log 4p$ (voir [17], page 199). Par conséquent, les bornes (16) et (17) sont valables sans aucune condition de divisibilité portant sur le nombre de classes.

Remarque : Notons qu'en suivant la méthode qui a mené à (16) il est possible de majorer q lorsque p est congru à 1 modulo 8. Cependant, la borne obtenue est alors, *en général*, moins précise que (17), car on ne contrôle plus le degré de $\mathbf{K}$: il peut être de l'ordre de p, ce qui conduit à une majoration de q de l'ordre de p^5.

5. Majoration de x et de y

Ce paragraphe est consacré à la majoration de la taille des solutions (x, y) des équations (2) et (3). Comme indiqué dans la partie 2, pour démontrer les Théorèmes 1 à 4, on peut supposer que p n'est pas congru à 1 modulo q. Sous une hypothèse supplémentaire portant sur $h^-(\mathbf{Q}(\zeta_p))$, le nombre de classes relatif du p-ème corps cyclotomique, le résultat suivant présente d'excellentes estimations, qui s'avèrent déterminantes pour la suite de nos travaux.

Théorème 6. *Soient p et q deux nombres premiers distincts tels que $p \not\equiv 1 \bmod q$ et $q \not| h^-(\mathbf{Q}(\zeta_p))$. On définit*

$$\alpha(\ell) = \left(2\sin\frac{\pi}{q}\right)^{q(p-1-2\ell)} \left(\left(\frac{2}{q}\right)^{\ell} \prod_{j=1}^{\ell} \sin\frac{2j\pi}{p}\right)^{2q},$$

$$\beta(\ell) = \left(2\cos\frac{\pi}{2q}\right)^{q(p-1-2\ell)} \left(\left(\frac{2}{q}\right)^{\ell} \prod_{j=1}^{\ell} \cos\frac{j\pi}{p}\right)^{2q}$$

et enfin

$$M(\ell) = \begin{cases} p^q/\alpha^{\ell}, & \text{si } p-1 > 2q\ell, \\ \beta(\ell), & \text{si } p-1 < 2q\ell. \end{cases}$$

Alors si $(x^p - 1)/(x-1) = y^q$ ou py^q, et si C est un réel arbitraire, on a

$$|x| \leq \max\left(8q^2, \frac{8(p-1)q^3\log 2}{C}, \max_{0\leq\ell\leq(p-1)/2} \left(e^C M(\ell)\right)^{\frac{1}{|p-1-2q\ell|}}\right).$$

La méthode de preuve suit les travaux de Bilu [4], puis de Bilu & Hanrot [5], encore que cette "méthode" n'ait été isolée en tant que telle que dans le travail de Bugeaud & Hanrot [9].

Démonstration : On garde les notations et les hypothèses du paragraphe précédent, dans le cas où $\ell = 1$, c'est-à-dire que $A(x) = x - \zeta_p$. D'après la remarque qui suit la relation (11), on voit que $\overline{A}(x)/A(x)$ est une puissance q-ème dans $\mathbf{L} = \mathbf{Q}(\zeta_p)$. Par suite, il existe un $k \in \mathbf{Z}/q\mathbf{Z}$ tel que $\zeta_q^k(\overline{A}(x)/A(x))^{1/q} \in \mathbf{L}$, où ζ_q est une racine primitive q-ème de l'unité fixée.

On forme maintenant l'entier algébrique de $\mathbf{L}$

$$\varphi(x) := A(x)\left(\zeta_q^k\left(\frac{\overline{A}(x)}{A(x)}\right)^{1/q} - 1\right)^q.$$

Les conjugués $\varphi^\tau(x)$ sont de la forme

$$A(x)\left(\zeta_q^{k_\tau}\left(\frac{\overline{A}(x)}{A(x)}\right)^{1/q} - 1\right)^q,$$

où $k_\tau \in \mathbf{Z}/q\mathbf{Z}$, avec $k_\tau + k_{\rho\tau} = 0$.

Par ailleurs, $\varphi(x)$ est un entier algébrique qui divise

$$A(x)^q \prod_{k=1}^{q}\left(\zeta_q^l(\overline{A}(x)/A(x))^{1/q} - 1\right)^q = (\overline{A}(x) - A(x))^q = (\zeta_p - \overline{\zeta}_p)^q,$$

et donc $N_{\mathbf{L}/\mathbf{Q}}(\varphi(x))$ est un entier qui divise p^q.

Mais $N_{\mathbf{L}/\mathbf{Q}}(\varphi(x))$ est égal, à une puissance q-ème près, à $N_{\mathbf{L}/\mathbf{Q}}(x - \zeta_p) = \hat{p}y^q$. Quand $\hat{p} = p$, cela permet de conclure que $N_{\mathbf{L}/\mathbf{Q}}(\varphi(x)) = p$, et quand $\hat{p} = 1$, que $N_{\mathbf{L}/\mathbf{Q}}(\varphi(x)) \in \{1, p^q\}$. En particulier, on a l'encadrement

$$1 \leq |N_{\mathbf{L}/\mathbf{Q}}(\varphi(x))| \leq p^q. \tag{18}$$

La seconde partie de la preuve consiste à étudier la norme de $\varphi(x)$ d'un point de vue analytique quand $|x| \to \infty$.

Lemme 4. *Posons $\psi_\tau = (\zeta_q^{k_\tau} - 1)^q, \sigma_\tau = 1$ si $k_\tau \neq 0$, et $\psi_\tau = (\zeta_p^\tau - \overline{\zeta}_p^\tau)^q/q^q$, $\sigma_\tau = 1 - q$ sinon. Alors si $|x| \geq 8q^2$,*

$$\left|\log\frac{\varphi^\tau(x)}{\psi_\tau x^{\sigma_\tau}}\right| \leq \frac{8q^3\log 2}{|x|}.$$

Démonstration : Si z est un nombre complexe de module inférieur à $1/2$, on a $|(1+z)^{1/q} - 1| \leq 2(1 - 2^{-1/q})|z| \leq 2|z|$, comme on le voit en développant le membre de gauche en série entière ; de la même façon, $|\mathrm{Log}\,(1+z)| \leq 2|z|\log 2$.

Par ailleurs, si a et b sont deux nombres complexes dont les parties réelles sont strictement positives, $(ab)^{1/q} = a^{1/q}b^{1/q}$; par suite, pour $|x| \geq 1$, on a $\varphi^\tau(x) = x(\zeta_q^{k_\tau}(1 - \overline{\zeta}_p^\tau x^{-1})^{1/q} - (1 - \zeta_p^\tau x^{-1})^{1/q})^q$.

Mais

$$\left|\frac{\zeta_q^{k_\tau}(1 - \overline{\zeta}_p^\tau x^{-1})^{1/q} - (1 - \zeta_p^\tau x^{-1})^{1/q}}{\zeta_q^{k_\tau} - 1} - 1\right| \leq \frac{4}{|\zeta_q^{k_\tau} - 1||x|} \leq \frac{q}{|x|}.$$

Si $|x| \geq 2q$, on peut appliquer l'identité sur le logarithme, et en multipliant les deux membres de l'inégalité par q, il vient

$$\left|\mathrm{Log}\,\frac{\varphi^\tau(x)}{(\zeta_q^{k_\tau}-1)^q x}\right| \le \frac{2q^2\log 2}{|x|}.$$

Le cas $k_\tau = 0$ se traite de façon analogue, en poussant le développement de $(1+z)^{1/q}$ à l'ordre 2, ce qui conclut la preuve du lemme. □

Notons 2ℓ le nombre de τ tels que $k_\tau = 0$. La relation $k_\tau + k_{\rho\tau} = 0$ montre en effet que ce nombre est pair. La somme $\sum_\tau \sigma_\tau$ vaut alors $2(1-q)\ell + (p-1-2\ell) = p-1-2q\ell$. On a alors, pour $|x| \ge 8q^2$,

$$\left|\log \frac{N_{\mathbf{L}/\mathbf{Q}}\varphi(x)}{x^{p-1-2q\ell}\prod_\tau \psi_\tau}\right| \le \frac{8(p-1)q^3\log 2}{|x|}.$$

Soit alors C un réel plus grand que $8(p-1)q^3\log 2/|x|$. Il vient

$$e^{-C}\left|\frac{N_{\mathbf{L}/\mathbf{Q}}\varphi(x)}{\prod_\tau \psi_\tau}\right| \le |x|^{p-1-2q\ell} \le e^{C}\left|\frac{N_{\mathbf{L}/\mathbf{Q}}\varphi(x)}{\prod_\tau \psi_\tau}\right|. \tag{19}$$

Comme $|\psi_\tau| = |2\sin(k_\tau\pi/q)|^q$ si $k_\tau \ne 0$, et $|\psi_\tau| = (2\sin(2l_\tau\pi/p))^q/q^q$ sinon, où l_τ est l'entier défini par $\zeta_p^{l_\tau} = \zeta_p^\tau$, et que dans ce dernier cas une valeur donnée de l_τ ne peut être prise que pour deux τ complexes conjugués, il vient

$$\alpha(\ell) \le \left|\prod_\tau \psi_\tau\right| \le \beta(\ell). \tag{20}$$

Le résultat est alors une conséquence de (18), (19) et (20). □

En particulier, si q est grand devant p, on trouve une borne pour $|x|$, atteinte pour $\ell = 0$, de l'ordre de $(q/(2\pi))^q p^{q/(p-1)}$. Noter que les valeurs des bornes utilisées ultérieurement sont celles obtenues pour $C = 3$.

Remarque : Plutôt que d'énumérer toutes les valeurs de x en-deçà de cette borne, il est préférable d'éliminer la majorité des valeurs par des arguments de congruence, en cherchant, pour chaque premier $s = 1 \bmod p$, à quelles classes de congruence peut appartenir x. Comme, heuristiquement, seule une proportion $1/p$ des x survit au crible pour chaque s, cette procédure est très efficace et permet – moyennant quelques optimisations, notamment concernant la gestion de la mémoire – d'atteindre des bornes de l'ordre de 10^{15} en quelques minutes. Il est utile de noter toutefois que pour $q > p-1$, la borne obtenue pour $|y|$ est de meilleure qualité et doit donc être préférée, même si le crible associé est un peu moins efficace (on peut espérer atteindre des bornes de l'ordre de 10^{12}).

Remarque : Il convient de dire un mot du cas où q divise $h^-(\mathbf{Q}(\zeta_p))$, par exemple le cas $(p,q) = (23,3)$. Il est malgré tout possible d'appliquer le théorème précédent dès lors que l'on sait montrer que $A(x)/\overline{A}(x)$ est bien une puissance q-ème. Dans le cas contraire, il existe un idéal $\mathfrak{I}$ dont l'ordre de la classe dans $\mathrm{Cl}(\mathbf{Q}(\zeta_p))$ est q, et, si l'on pose $(\xi) = \mathfrak{I}^q$, on a $A(x)/\overline{A}(x) = \alpha^q \xi/\overline{\xi}$. Noter que si ξ est défini à une unité près, $\xi/\overline{\xi}$ est lui défini à une puissance q-ème près (racine de l'unité). Soit s un premier congru à 1 modulo pq. On sait que $\mathbf{Z}[\zeta_p]/(s) = \mathbf{F}_s^{p-1}$, l'identification se faisant en substituant à ζ_p les $p-1$ racines primitives p-èmes de l'unité de $\mathbf{F}_s$.

On peut alors, si l'on connaît des générateurs de la q-partie du groupe des classes, tester pour chaque $\xi \neq 1$ si $A(x)\overline{\xi}/(\xi\overline{A}(x))$ est une puissance q-ème modulo s pour un certain x mod s. Dans le cas contraire, on sait que $A(x)/\overline{A}(x)$ est une puissance q-ème et le Théorème 6 s'applique. Nous présentons dans la partie c. de l'appendice les éléments ξ correspondant aux couples $(23, 3)$, $(59, 3)$ et $(83, 3)$ et expliquons brièvement la façon dont ils ont été obtenus.

On établit dès maintenant une proposition concernant les k_τ qui nous sera utile ultérieurement dans le traitement du cas diagonal.

Lemme 5. *On se place dans le cas où $p = q$, et l'on suppose que $A(x)/\overline{A}(x)$ n'est pas une puissance p-ème. Alors*

(a) Si $\{\tau_0, \ldots, \tau_{p-1}\}$ sont les prolongements à $\mathbf{Q}(\zeta_{p^2})$ d'un même automorphisme de $\mathbf{Q}(\zeta_p)$, alors $\{k_{\tau_0}, \ldots, k_{\tau_{p-1}}\} = \{0, \ldots, p-1\}$.

(b) On écrit $(x - \zeta_p)/(x - \overline{\zeta}_p) = \zeta_p^\iota \lambda^p$; sil'on définit ι_τ par $\tau(\zeta_{p^2}^\iota) = \zeta_p^{\iota_\tau}(\tau(\zeta_p^\iota))^{1/p}$, on a, si , pour τ et τ' deux plongements de $\mathbf{Q}(\zeta_{p^2})$ dans $\mathbf{C}$ coïncidant sur $\mathbf{Q}(\zeta_p)$, $k_\tau - k_{\tau'} \equiv \iota_\tau - \iota_{\tau'} \bmod p$.

Démonstration : Pour la première partie, il suffit de remarquer que si $k_{\tau_1} = k_{\tau_2}$ et que τ_1 et τ_2 coïncident sur $\mathbf{Q}(\zeta_p)$, alors en vertu de la définition des k_τ,

$$\tau_1 \left(\left(\frac{x - \zeta_p}{x - \overline{\zeta}_p} \right)^{1/p} \right) = \tau_2 \left(\left(\frac{x - \zeta_p}{x - \overline{\zeta}_p} \right)^{1/p} \right),$$

et donc $\tau_1 = \tau_2$. Pour la seconde partie, on renvoie à l'appendice B de [5]. □

6. Réduction

Au préalable, il est bon de récapituler les résultats déjà obtenus, afin de bien préciser le travail qu'il nous reste à effectuer pour démontrer nos résultats. Soit donc $p \geq 5$ un nombre premier et cherchons à montrer que (1) ne possède aucune solution (x, y, n, q) avec n un multiple de p et q un nombre premier impair. On sait que cela est vrai si p est congru à 1 modulo q. Pour les autres valeurs de q, il convient de prouver que les équations (2) et (3) n'admettent aucune solution. On utilise alors le Théorème 5 afin de majorer q, de sorte qu'il nous reste seulement un *petit* nombre d'équations à traiter. Si le couple (p, q) est tel que q ne divise pas $h^-(\mathbf{Q}(\zeta_p))$, et c'est le cas en particulier pour $p \leq 19$, alors le Théorème 6 nous offre de très bonnes majorations pour la taille des solutions des équations (2) et (3) : il suffit alors d'énumérer les différentes valeurs possibles de x et de y, puis de constater qu'aucune ne convient. Toutefois, même les majorations que nous obtenons se révèlent très vite insuffisantes pour permettre une énumération complète. Il faut alors avoir recours à des idées de réduction. La mise en œuvre de ces idées constitue l'essentiel de cette partie 6. Nous en rappelons d'abord très brièvement les principes.

On cherche à minorer précisément une quantité du type $|b_1\alpha_1 + \ldots + b_n\alpha_n + \lambda|$, sous l'hypothèse $|b_i| \leq B$. Quand $n = 2$, cela peut être fait à l'aide du développement en fractions continues de α_1/α_2, comme le firent originellement Baker et Davenport [1]. Quand $n \geq 3$, on peut utiliser une généralisation du lemme de Baker-Davenport due à Ellison [16] ; toutefois on a généralement recours à l'algorithme de réduction de réseaux LLL, dû à Lenstra, Lenstra, et Lovàsz [23]. Pour une présentation des principes et de la mise en œuvre de cette méthode, on pourra consulter par exemple la thèse de de Weger [45]. On se contente de rappeler le lemme suivant :

Lemme 6. *Soit m un entier compris entre 1 et n. Soient $(\alpha_{ij})_{1\leq i\leq n, 1\leq j\leq n}$ et $\lambda_1, \ldots, \lambda_m$ des nombres réels, $b_1, \ldots, b_n, C$ des entiers et soit $B = \max_i |b_i|$. Soit Λ le réseau engendré par les colonnes de la matrice*

$$A = \begin{pmatrix} 1 & 0 & \ldots & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & \ldots & 0 \\ \lfloor C\alpha_{1,1} \rceil & \lfloor C\alpha_{2,1} \rceil & \ldots & \lfloor C\alpha_{n-m,1} \rceil & \ldots & \lfloor C\alpha_{n,1} \rceil \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \lfloor C\alpha_{1,m} \rceil & \lfloor C\alpha_{2,m} \rceil & \ldots & \lfloor C\alpha_{n-m,m} \rceil & \ldots & \lfloor C\alpha_{n,m} \rceil \end{pmatrix},$$

$\boldsymbol{x}$ le point de coordonnées ${}^t(0, 0, \ldots, -\lfloor C\lambda_1 \rceil, \ldots, -\lfloor C\lambda_m \rceil)$ et $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ une base LLL-réduite de Λ.

1. On a

$$\max_j \left| \sum_{i=1}^{n} b_i \alpha_{i,j} \right| \geq \frac{1}{C} \left(\sqrt{\frac{2^{1-n}\|\boldsymbol{v}_1\|^2 - (n-m)B^2}{m}} - nB/2 \right).$$

2. Soit (s_i) les coordonnées de x dans la base $(\boldsymbol{v}_1, \ldots, \boldsymbol{v}_n)$ et soit $i^* = \min\{i : s_i \notin \mathbf{Z}\}$. Alors

$$\max_j \left| \sum_{i=1}^{n} b_i \alpha_{i,j} + \lambda_j \right| \geq \frac{1}{C} \left(\sqrt{\frac{2^{1-n} d(s_{i^*}, \mathbf{Z})\|\boldsymbol{v}_1\|^2 - (n-m)B^2}{m}} - (nB+1)/2 \right).$$

a. Une forme linéaire de logarithmes.

L'objet de ce paragraphe est principalement de rappeler la construction de la forme linéaire de logarithmes décrite dans [5], afin de permettre au lecteur de lire ce travail indépendamment de [5]. C'est en effet à cette forme linéaire de logarithmes que nous appliquerons le Lemme 6.

Soient x, y des entiers tels que $y^q = (x^p-1)/(x-1)$ ou $py^q = (x^p-1)/(x-1)$ et soit $\mathbf{K}$ un corps contenant $\mathbf{Q}\left(\zeta_q^{k(x)}\left(\frac{x-\zeta_p}{x-\bar{\zeta}_p}\right)^{1/q}\right)$. D'après le paragraphe 4a de [5], on a $\mathbf{K} = \mathbf{Q}(\zeta_p)$ si $p \neq q$, $\mathbf{K} \in \{\mathbf{Q}(\zeta_p), \mathbf{Q}(\zeta_{p^2})\}$ sinon.

On considère de nouveau l'entier algébrique $\varphi(x)$ de $\mathbf{K}$, dont on sait (voir le paragraphe 5) que

$$\varphi(x) = \theta\eta,$$

où $\theta \in \{1, 1-\zeta_p, p\}$ et où η est une unité, dans le cas ordinaire $p \neq q$. Un argument analogue donne le même résultat dans le cas diagonal $p = q$.

Soient $\eta_1, \ldots, \eta_r$ les éléments d'un système fondamental d'unités du corps $\mathbf{K}$, et ξ engendrant la partie de torsion du groupe des unités. On définit alors les entiers $(b_i)_{1\leq i\leq r}$ par $\eta = \xi^t\eta_1^{b_1}\ldots\eta_r^{b_r}$. Dans toute la suite, Log désignera la détermination principale du logarithme, i.e., telle que $-\pi \leq \operatorname{Im}\operatorname{Log}(x) < \pi$.

Supposons également donnés τ_1 et τ_2 sont deux éléments distincts de $\operatorname{Gal}(\mathbf{K}/\mathbf{Q})$ tels que k_{τ_1} et k_{τ_2} sont tous deux non nuls, et définissons $\Phi_{\tau_1,\tau_2} := \varphi^{\tau_1}\psi_{\tau_2}/\varphi^{\tau_2}\psi_{\tau_1}$.

Le lemme suivant est alors une conséquence facile du Lemme 4.

Lemme 7. *Posons* $\Lambda := \operatorname{Log}\Phi_{\tau_1,\tau_2}$. *Il existe un réel c et un entier b_{r+1}, avec* $|b_{r+1}| \leq |b_1| + \ldots + |b_r| + 1 + O(|x|^{-1})$, *tels que :*

$$\Lambda = \sum_{j=1}^{r} b_j \operatorname{Log}\frac{\eta_j^{\tau_1}}{\eta_j^{\tau_2}} + \operatorname{Log}\frac{\psi_{\tau_2}\theta^{\tau_1}}{\psi_{\tau_1}\theta^{\tau_2}} + i\pi b_{r+1} = O(|x|^{-1}) = O(\exp(-c\max_i |b_i|)). \tag{21}$$

Remarque : L'hypothèse k_{τ_1} *et* k_{τ_2} *sont tous deux non nuls* n'est pas gênante. En effet, dans le cas diagonal, qu'un tel choix est possible résulte du lemme 5 ; dans le cas ordinaire, si l'on suppose que l'un au moins des k_τ est nul – i.e., $\ell \geq 1$, la borne du théorème 6 se trouve très nettement améliorée dans le cas où q est grand devant p. À titre d'illustration, la borne pour $|y|$ quand $(p,q) = (5, 6991)$ passe de $7.7\cdot 10^{12}$ à 1.

Si l'on pose alors

$$\alpha_{i,j} = \log|\eta_i^{\tau_j}/\eta_i^{\tau_1}|$$

et

$$\lambda_j = q\log|\sin(k_{\tau_1}\pi/q)/\sin(k_{\tau_j}\pi/q)| + \log|\theta^{\tau_j}/\theta^{\tau_1}|,$$

nous avons alors une identité du type

$$\left|\sum_{1\leq i\leq r} b_i\alpha_{ij} + \lambda_j\right| = O(\exp(-c\max_i |b_i|),$$

le Lemme 7 permet en particulier d'obtenir une borne supérieure pour les $|b_i|$ à partir de la borne du Théorème 6. Nous sommes donc en position d'appliquer le Lemme 6, qui nous donnera une borne inférieure pour $\max_j |\sum_{1\leq i\leq r} b_i\alpha_{i,j}+\lambda_j|$, que l'on peut exploiter, soit pour améliorer la borne sur $\max_i |b_i|$, soit pour obtenir une borne finale sur $|x|$ (en utilisant (21)).

Dans le cas diagonal, pour pouvoir utiliser le même procédé, il nous faut une telle borne de départ sur $\max_i |b_i|$, qui découle classiquement de la combinaison de (21) et d'une borne inférieure pour les formes linéaires en logarithmes telle celle due à Baker et Wüstholz [2] ; il faut toutefois pouvoir garantir que $\Phi_{\tau_1,\tau_2}(x)\neq 1$, ce qui fait l'objet du lemme suivant.

Lemme 8. *Pour tout entier x non nul, $\Phi_{\tau_1,\tau_2}(x)\neq 1$.*

Démonstration : Comme cela ne sera utilisé que dans le cas diagonal, on peut supposer que τ_1 et τ_2 sont choisis de telle sorte que $k_{\tau_1}\neq 0, k_{\tau_2}\neq 0$ et que τ_1 et τ_2 coïncident sur $\mathbf{Q}(\zeta_p)$. Par suite, l'équation $\Phi_{\tau_1,\tau_2}(x)=1$ se récrit, pour $|x|>1$:

$$\zeta_p^{k_{\tau_1}}\left(1-\frac{\zeta_p^{\tau_1}}{x}\right)^{1/p}-\left(1-\frac{\overline{\zeta_p}^{\tau_1}}{x}\right)^{1/p}=\zeta_p^t\left(\zeta_p^{k_{\tau_2}}\left(1-\frac{\zeta_p^{\tau_1}}{x}\right)^{1/p}-\left(1-\frac{\overline{\zeta_p}^{\tau_1}}{x}\right)^{1/p}\right),$$

pour un certain entier t défini modulo p par l'identité ci-dessus.

Un calcul simple conduit alors à $k_{\tau_1}=k_{\tau_2}$, soit encore $\tau_1=\tau_2$, impossible. □

b. Aspects pratiques de la réduction, cas ordinaire.

Dans ce paragraphe, on se placera dans le cas où q est grand devant p ; en vertu de la remarque qui suit le lemme 7, on peut alors supposer à peu de frais que $k_\tau\neq 0$ pour tout τ. En particulier, tous les σ_τ sont égaux à 1.

Il est *a priori* nécessaire d'effectuer le test de réduction pour tous les $m+1$-uplets $(k_{\tau_i})_{i\leq m}$ avec $1\leq k_{\tau_1},k_{\tau_2},\ldots,k_{\tau_{m+1}}\leq q-1$, car les restrictions établies au lemme 5 ne sont valides que dans le cas diagonal. Toutefois, ceci conduirait à un temps de réduction pour un couple (p,q) de l'ordre de $O(q^{m+1})$, et donc, dans le cas $m=1$ le plus fréquent, de l'ordre de $O(q^3_{\max})$ pour une valeur de p donnée, ce qui requerrait déjà un effort important de calcul pour $p=7$.

Il est toutefois possible de diminuer la complexité de ce calcul pour gagner (presque) un facteur q, en utilisant une stratégie de type “diviser pour régner”, comme suit.

Pour appliquer le lemme de réduction, on est amené à minimiser, dans le cas $i^*=1$ que l'on rencontre en pratique, la quantité

$$\left\|\sum_{j=1}^m \kappa_{jr}\left\lfloor C\left(\log\left|\frac{\sin(k_{\tau_1}\pi/q)}{\sin(k_{\tau_{j+1}}\pi/q)}\right|+\log\left|\frac{\sin(l_{\tau_{j+1}}\pi/p)}{\sin(l_{\tau_1}\pi/p)}\right|^*\right)\right\rceil\right\|, \tag{22}$$

où le terme étoilé peut être nul selon la valeur de θ dans $\{1, 1-\zeta_p, p\}$), et où (κ_{ij}) est l'inverse de la matrice des coordonnées dans la base canonique des vecteurs d'une base LLL-réduite du réseau Λ (les κ_{jr} sont donc des nombres rationnels, en pratique petits devant 1).

Il faut alors distinguer deux cas. Quand $m > 1$, on minore cette quantité par

$$\left\| \sum_{j=1}^{\lceil (m-1)/2 \rceil} \kappa_{jr} \left\lfloor C \log \left| \frac{\sin k_{\tau_{j+1}} \pi/q}{\sin k_{\tau_1} \pi/q} \right| \right\rceil + \sum_{j=\lceil (m-1)/2 \rceil+1}^{m} \kappa_{jr} \left\lfloor C \log \left| \frac{\sin k_{\tau_{j+1}} \pi/q}{\sin k_{\tau_1} \pi/q} \right| \right\rceil \right.$$
$$\left. + \sum_{j=1}^{m} \kappa_{jr} \left(\left\lfloor C \log \left| \frac{\sin(l_{\tau_{j+1}} \pi/p)}{\sin(l_{\tau_1} \pi/p)} \right| \right\rceil \right)^* \right\| - \sum_{j=1}^{m} |\kappa_{jr}|.$$

Cette dernière quantité présente l'avantage de se calculer plus efficacement : il suffit de calculer séparément toutes les valeurs possibles des deux premiers termes (respectivement $q^{\lceil (m-1)/2 \rceil+1}$ et $q^{\lfloor (m+1)/2 \rfloor+1}$, à une constante près si l'on tient compte des symétries), de trier les deux listes obtenues, et de parcourir les listes pour trouver les couples dont la différence est la plus voisine de 0 ou du terme étoilé ; en procédant de cette façon on obtient le minorant souhaité en $O(q^{\lfloor (m+1)/2 \rfloor+1} \log q)$ opérations.

Dans le cas où le minimum de ces différences est plus grand que $\sum_{j=1}^{r} |\kappa_{jr}|$ (toujours en pratique quand $m \leq 4$, quitte à augmenter C), on obtient un minorant pour le terme $d(s_{i^*}, \mathbf{Z})$, et l'on peut donc appliquer le lemme de réduction.

Si $m = 1$, on minore l'expression (22) par

$$\left\| \kappa_{1r} \left\lfloor C \log \sin \frac{k_{\tau_2} \pi}{q} \right\rceil - \kappa_{1r} \left\lfloor C \log \sin \frac{k_{\tau_1} \pi}{q} \right\rceil + \kappa_{1r} \left(\left\lfloor C \log \left| \frac{\sin(l_{\tau_2} \pi/p)}{\sin(l_{\tau_1} \pi/p)} \right| \right\rceil \right)^* \right\| - |\kappa_{1r}|,$$

et l'on procède de la même façon que précédemment avec les deux premiers termes, ce qui conduit à une complexité de calcul en $O(q \log q)$.

Le cas $k_{\tau_1} = k_{\tau_2} = \ldots = k_{\tau_m}$ qui se traite en principe via le premier point du lemme de réduction, peut être omis. On constate aisément que les bornes qu'il donne sont toujours meilleures que les bornes obtenues par application du second point.

c. Aspects pratiques de la réduction, cas diagonal.

Dans le cas diagonal, la méthode du paragraphe b n'est plus satisfaisante, en raison de la dimension trop importante du réseau sous-jacent ; on applique la méthode de Bilu et Hanrot (décrite en détail dans [5]), qui permet, au prix de l'énumération des $p(p-1)$-uplets k_τ, de se ramener à un réseau de dimension 2. On ne reprendra pas ici l'exposé détaillé, mais on indique juste quelles sont les difficultés qui obligent à se restreindre aux deux cas $p = q = 5$ et $p = q = 7$. Noter qu'on pourra aussi consulter avec profit [6, paragraphe 8.2.2], qui traite d'une situation cyclotomique analogue quoique différente.

Énumération des k_τ. — Le nombre total de $p(p-1)$-uplets (k_τ) est *a priori* gigantesque, mais les deux assertions du Lemme 5 permettent de le réduire considérablement. En plus de ces deux restrictions, le fait que le corps de base $\mathbf{Q}(\zeta_p)$ contienne déjà les racines p-èmes de l'unité permet de *choisir* l'un des k_τ (que l'on fixe arbitrairement à 0) pour la construction de $\varphi(x)$. Toutes ces remarques, auxquelles s'ajoute l'utilisation de la conjugaison complexe, permettent de voir qu'il n'y a que $(p-1)p^{(p-3)/2}$ possibilités pour le $p(p-1)$-uplet k_τ. On peut par ailleurs noter que changer k_τ en son opposé modulo p n'a pas d'incidence sur le processus de réduction, ce qui permet encore de diviser par 2 le nombre de $p(p-1)$-uplets à examiner, soit respectivement pour 5, 7, 11, 13 : 10, 147, 73205, 2227758. Pour $p \geq 17$, le nombre de cas à considérer implique un temps de calcul qui nous a paru déraisonnable.

Unités non fondamentales. — Enfin, dans le cas $q = 11$ ou 13, une difficulté complémentaire se greffe ; on ne connaît plus de système fondamental d'unités, juste un système de rang maximal (les unités cyclotomiques). Il est possible, dans la mesure où l'on maîtrise l'indice d'un tel système, d'utiliser la variation technique décrite dans [18]. On peut obtenir de cette façon les bornes $|x| \leq$ (pour $p = 11$) ou $|x| \leq$ (pour $p = 13$).

Énumération des petites valeurs de x. — Afin de pouvoir traiter les bornes obtenues pour x dans le cas $p = q \in \{11, 13\}$, il nous faut disposer d'une méthode de crible efficace. Nous utilisons à cette fin la remarque qui précède le Lemme 5. Observons que dans ce cas, il existe un k_x tel que $A(x)/\overline{A}(x) = \zeta_p^{k_x}\alpha^p$. On peut alors, pour chaque valeur possible de k_x, cribler en utilisant cette identité. On élimine alors très vite tous les k_x possibles sauf deux, qui correspondent aux deux solutions triviales $x = 0$ et $x = 1$; cela permet déjà de diviser par $p/2$ le nombre de p-uplets à utiliser.

En outre, pour beaucoup de petits premiers $s_i = 1 \bmod p$, seule une classe $x \bmod s_i$ est possible pour chaque k_x (les classes 0 et 1). On obtient donc simplement que toute solution est soit congrue à 0 mod $\prod_i s$ ou 1 mod $\prod_i s_i$; par suite, toute solution non triviale vérifie $|x| \geq \prod_i s_i - 1$.

Notons qu'il est impossible d'appliquer cette méthode au cas $p \neq q$; on ne peut dans ce cas pas séparer les solutions $x = 0$ et $x = 1$; par suite il faut considérer au moins 2^I classes, où I est le nombre de s_i, ce qui devient très rapidement irréalisable.

Appendice. Tables numériques

a. Bornes pour q selon les valeurs de y.

$y \backslash p$	5	7	11	13	17	19	23
$\geq 2p+1$	5521	25391	41777	213949	197651	72109	87523
$\geq 10^6$	2053	7417	13933	76099	96973	28859	36821
$\geq 10^9$	1609	5147	9769	52489	75437	20029	25537

Pour obtenir ces majorations nous avons appliqué le Théorème 1 de [21] et non l'un de ses corollaires. Par exemple, pour $p = 5$ et sous l'hypothèse $y \geq 11$, nous avons choisi les paramètres $L = 20$, $K = 92$, $S = 40$, $R = 56$ et $\rho = 6.0263665$ afin d'en déduire la borne 5521 pour q.

b. Bornes pour x et y pour quelques valeurs de (p, q).

p	q	$\lvert x\rvert \leq$	$\lvert y\rvert \leq$
5	1609	$3.63 \cdot 10^{2571}$	$4.20 \cdot 10^{9}$
7	5147	$1.31 \cdot 10^{15720}$	$2.12 \cdot 10^{18}$
11	9769	$6.00 \cdot 10^{32196}$	$9.10 \cdot 10^{32}$
13	52489	$3.13 \cdot 10^{210728}$	$1.51 \cdot 10^{48}$
17	75437	$2.43 \cdot 10^{313539}$	$3.17 \cdot 10^{66}$
19	20029	$1.25 \cdot 10^{71594}$	$2.20 \cdot 10^{64}$
23	36821	$3.39 \cdot 10^{141017}$	$1.81 \cdot 10^{84}$
29	5	$1.60 \cdot 10^{9}$	$3.49 \cdot 10^{51}$
29	19	$1.17 \cdot 10^{11}$	$2.03 \cdot 10^{16}$
29	23	$1.59 \cdot 10^{14}$	$1.94 \cdot 10^{17}$
31	23	$1.39 \cdot 10^{14}$	$2.79 \cdot 10^{18}$
37	5	$4.73 \cdot 10^{5}$	$7.20 \cdot 10^{40}$
37	7	$1.61 \cdot 10^{7}$	$1.15 \cdot 10^{37}$
37	11	$1.89 \cdot 10^{10}$	$4.23 \cdot 10^{33}$
67	5	$1.04 \cdot 10^{11}$	$2.36 \cdot 10^{145}$

c. La 3-partie du groupe des classes de $\mathbf{Q}(\zeta_p)$ pour $p \in \{23, 59, 83\}$.

On donne dans cette partie des $x \in \mathbf{Q}(\zeta_p)$ tels que $(x) = \mathfrak{I}^3$ soit le cube d'un idéal $\mathfrak{I}$ non principal, et on indique succinctement comment les obtenir (il faut noter que 9 ne divise pas $h^-(\mathbf{Q}(\zeta_p))$ et que $h^+(\mathbf{Q}(\zeta_p)) = 1$ dans les trois cas considérés).

Dans les trois cas étudiés, on a $(3) = \mathfrak{p}_3\overline{\mathfrak{p}}_3$ dans $\mathbf{Q}(\zeta_p)$. La réduction LLL d'un idéal $\mathfrak{I}$ (voir [15, partie 6.5.1]) nous fournit un élément α tel que l'idéal $\mathfrak{I}/\alpha$ soit en un certain sens minimal dans la classe de $\mathfrak{I}$ (pour être précis, il serait juste de parler de réduction dans la direction $(1, \ldots, 1)$). Dans notre cas, la réduction de l'idéal $\mathfrak{p}_3$ laisse supposer (sans offrir de certitude) que $\mathfrak{p}_3$ peut ne pas être principal, alors que, appliquée à $\mathfrak{p}_3^3$, elle montre que ce dernier est principal, et fournit des valeurs numériques approchées de l'image d'un générateur par les différents plongements de $\mathbf{Q}(\zeta_p)$ dans $\mathbf{C}$; ceci permet de déterminer ce générateur ξ de façon exacte (on vérifie la validité du résultat en factorisant l'idéal (ξ)). La table suivante présente les différentes valeurs de ξ.

p	$h^-(\mathbf{Q}(\zeta_p))$	ξ
23	3	$2(\zeta_{23}^{18}+\zeta_{23}^{16}+\zeta_{23}^{13}+\zeta_{23}^{12}+\zeta_{23}^{9}+\zeta_{23}^{8}+\zeta_{23}^{6}+\zeta_{23}^{4}+$ $\zeta_{23}^{3}+\zeta_{23}^{2}+\zeta_{23})+3$
59	$3\cdot 59\cdot 233$	$\zeta_{59}^{54}+\zeta_{59}^{53}+\zeta_{59}^{48}+\zeta_{59}^{44}+\zeta_{59}^{43}+\zeta_{59}^{41}+\zeta_{59}^{40}+\zeta_{59}^{38}+\zeta_{59}^{36}+\zeta_{59}^{32}$ $+\zeta_{59}^{30}+\zeta_{59}^{29}+\zeta_{59}^{27}+\zeta_{59}^{26}+\zeta_{59}^{25}+\zeta_{59}^{23}+\zeta_{59}^{21}+\zeta_{59}^{18}+\zeta_{59}^{15}+\zeta_{59}^{14}$ $+\zeta_{59}^{13}+\zeta_{59}^{11}+\zeta_{59}^{10}+\zeta_{59}^{9}+\zeta_{59}^{8}+\zeta_{59}^{5}+\zeta_{59}^{4}+\zeta_{59}^{3}+\zeta_{59}^{2}+\zeta_{59}$
83	$3\cdot 279405653$	$\zeta_{83}^{81}+\zeta_{83}^{80}+\zeta_{83}^{76}+\zeta_{83}^{73}+\zeta_{83}^{72}+\zeta_{83}^{70}+\zeta_{83}^{69}+\zeta_{83}^{68}+$ $\zeta_{83}^{65}+\zeta_{83}^{63}+\zeta_{83}^{62}+\zeta_{83}^{61}+\zeta_{83}^{60}+\zeta_{83}^{59}+\zeta_{83}^{58}+\zeta_{83}^{57}+\zeta_{83}^{55}+\zeta_{83}^{53}$ $+\zeta_{83}^{49}+\zeta_{83}^{48}+\zeta_{83}^{44}+\zeta_{83}^{43}+\zeta_{83}^{42}+\zeta_{83}^{41}+\zeta_{83}^{39}+\zeta_{83}^{36}+\zeta_{83}^{35}$ $+\zeta_{83}^{33}+3\zeta_{83}^{32}+\zeta_{83}^{30}+\zeta_{83}^{27}+\zeta_{83}^{26}+\zeta_{83}^{24}+\zeta_{83}^{19}+\zeta_{83}^{18}+\zeta_{83}^{17}$ $+\zeta_{83}^{14}+\zeta_{83}^{13}+\zeta_{83}^{12}+\zeta_{83}^{10}+\zeta_{83}^{8}+1$

On peut alors appliquer la remarque qui précède le lemme 5 à cet élément et à son carré ; cela permet d'appliquer le Théorème 6 aux cas $(23,3)$, $(59,3)$, $(83,3)$, sous réserve, dans chacun des cas, que l'idéal $\mathfrak{p}_3$ correspondant ne soit pas principal.

Reste donc à prouver que $\mathfrak{p}_3$ n'est pas principal. Cela découle *de facto* du succès de la méthode de la remarque. En effet, supposons que $\mathfrak{p}_3$ soit engendré par un élément μ. Alors il existe une unité u de $\mathbf{Q}(\zeta_p)$ telle que $u\mu^3=\xi$, et $\xi/\overline{\xi}$ est par suite un cube. Il en résulte que l'équation $(x-\zeta)/(x-\overline{\zeta})=\lambda^3\xi/\overline{\xi}$ sur laquelle est basée la remarque se réduit à $(x-\zeta)/(x-\overline{\zeta})=\lambda^3$, laquelle a la solution $x=0$. Par suite, si $\mathfrak{p}_3$ est principal, la méthode exposée dans la remarque échoue nécessairement. Le simple fait qu'elle réussisse prouve simultanément que $\mathfrak{p}_3$ n'est pas principal.

Références bibliographiques

[1] A. Baker, H. Davenport, The equations $3x^2-2=y^2$ and $8x^2-7=z^2$, *Quart. J. Math. Oxford (2)* **20** (1969), 129–137.

[2] A. Baker, G. Wüstholz, Logarithmic forms and group varieties, *J. Reine Angew. Math.* **442** (1993), 19–62.

[3] M. Bennett, Rational approximation to algebraic number of small height : The diophantine equation $\mid ax^n-by^n\mid=1$, *J. Reine Angew. Math.* À paraître.

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

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

[6] Y. Bilu, G. Hanrot, P. M. Voutier, avec un appendice de M. Mignotte, Existence of primitive divisors of Lucas and Lehmer sequences. Soumis.

[7] Y. Bugeaud, Linear forms in p-adic logarithms and the Diophantine equation $(x^n-1)/(x-1)=y^q$, *Math. Proc. Cambridge Philos. Soc.* À paraître.

[8] Y. Bugeaud, Sur la distance entre deux puissances pures, *C. R. Acad. Sci. Paris Série I* **322** (1996), 1119–1121.

[9] Y. Bugeaud et G. Hanrot, Un nouveau critère pour l'équation de Catalan. Soumis.

[10] Y. Bugeaud et M. Mignotte, On integers with identical digits, *Mathematika.* À paraître.

[11] Y. Bugeaud et M. Mignotte, Sur l'équation diophantienne $(x^n-1)/(x-1)=y^q$, *II*, *C. R. Acad. Sci. Paris Série I* **328** (1999), 741–744.

[12] Y. Bugeaud, M. Mignotte et Y. Roy, On the diophantine equation $(x^n-1)/(x-1)=y^q$, *Pacific J. Math.* À paraître.

[13] Y. Bugeaud, M. Mignotte, Y. Roy et T. N. Shorey, The diophantine equation $(x^n-1)/(x-1)=y^q$ has no solution with x square, *Math. Proc. Cambridge Philos. Soc.* À paraître.

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

[15] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Math., Vol. 138, Springer-Verlag, New York, 1993.

[16] W.J. Ellison, Recipes for solving diophantine problems by Baker's method, Sem. Théorie Nombres 1970-1971, Univ. Bordeaux, No.11, 10 p.

[17] A. Faisant, *L'équation diophantienne du second degré*, Herrmann, Paris, 1991.

[18] G. Hanrot, Solving Thue equations without the full unit group, *Math. Comp.* À paraître.

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

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

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

[22] Maohua Le, A note on the diophantine equation $(x^m-1)/(x-1)=y^n+1$, *Math. Proc. Cambridge Phil. Soc.* **116** (1994), 385–389.

[23] A.K. Lenstra, H.W. Lenstra, Jr., L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* **261** (1982), 515–534.

[24] F. J. van der Linden, Class Number Computations of Real Abelian Number Fields, *Math. Comp.* **39** (1982), 693–707.

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

[26] S. Louboutin, Majorations explicites de $|L(1,\chi)|$, *II*, *C. R. Acad. Sci. Paris Série I* **323** (1996), 443–446.

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

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

[29] M. Mignotte, On the diophantine equation $(x^n-1)/(x-1)=y^q$, Proceedings of the Number Theory Conference held in Graz. À paraître.

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

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

[32] 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.

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

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

[35] N. Saradha et T. N. Shorey, The equation $(x^n-1)/(x-1)=y^q$ with x square, *Math. Proc. Cambridge Philos. Soc.* **125** (1999), 1–19.

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

[37] T. N. Shorey, Perfect powers in values of certain polynomials at integer points, *Math. Proc. Cambridge Phil. Soc.* **99** (1986), 195–207.

[38] T. N. Shorey, On the equation $z^q=(x^n-1)/(x-1)$, *Indag. Math.* **48** (1986), 345–351.

[39] T. N. Shorey. Exponential diophantine equations involving product of consecutive integers and related equations. À paraître.

[40] T. N. Shorey et R. Tijdeman. New applications of Diophantine approximations to Diophantine equations, *Math. Scand.* **39** (1976), 5–18.

[41] T. N. Shorey et R. Tijdeman. *Exponential Diophantine equations*, Cambridge Tracts in Mathematics 87 (1986), Cambridge University Press, Cambridge.

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

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

[44] B.M.M. de Weger, Solving exponential diophantine equations using lattice basis reduction algorithms, *J. Number Th.* **26** (1987), 325–367.

[45] B.M.M. de Weger, Algorithms for diophantine equations, CWI-Tract no. 65, Centre for Math. and Comp. Sci., Amsterdam, 1989.

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

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

Guillaume Hanrot
Projet POLKA
INRIA Lorraine & LORIA
615, rue du Jardin Botanique
54602 VILLERS-LÈS-NANCY CEDEX

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