5. Un exemple de résolution complète de l'équation (1)

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **48 (2002)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **21.07.2024**

Le Théorème 8 se trouve énoncé dans [30], mais la démonstration qu'en donne Le est erronée, ainsi d'ailleurs que les démonstrations de [52], comme le remarque Ping-Zhi Yuan [53] (voir aussi [4]).

Le Théorème 7 permet également de retrouver un résultat de Le [28], démontré par Inkeri [25] lorsque $q=3$.

THÉORÈME 9. *L'équation* (1) *ne possède aucune solution* (x,y,n,q) *où* x *est une puissance* q*-ième.*

Démonstration. Supposons qu'il existe $z>1$, $y>1$, $q\geq 2$ et $n\geq 3$ tels que $z^{qn}-1=(z^q-1)\,y^q$. D'après le Théorème 1 (i), on a $q\geq 3$ et il suffit d'appliquer le Théorème 7 à l'équation $z^q Z^q-(z^q-1)\,Y^q=1$ pour conclure. □

Les Théorèmes 8 et 9 jouent un rôle très important dans les démonstrations des résultats présentés dans les chapitres suivants.

5. Un exemple de résolution complète de l'équation (1)

Une question naturelle consiste à se demander si (1) admet une solution (x,y,n,q), où x est une puissance pure. D'après le Théorème 9, on sait déjà que x ne peut en aucun cas être une puissance q-ième. Le résultat suivant montre que x n'est pas non plus un carré.

THÉORÈME 10. *L'équation* (1) *n'admet aucune solution* (x,y,n,q) *où* x *est un carré.*

Le Théorème 10 a été obtenu indépendamment et au moyen de deux méthodes différentes par Bennett [4] et Bugeaud, Mignotte, Roy et Shorey [20], complétant des résultats antérieurs de Saradha et Shorey [42]. Nous choisissons de détailler les étapes principales de la démonstration de [20], qui ne fait appel ni au Théorème 7, ni au Théorème 8.

Le Théorème 1 (i) couvre le cas $q=2$ et un argument facile de factorisation montre qu'il suffit de prouver le Théorème 10 quand n est impair. Supposons donc que les entiers $z\geq 2$, $n\geq 5$, $q\geq 3$ et $y\geq 2$ avec n impair vérifient l'équation

$$\frac{z^{2n}-1}{z^2-1}=y^q\,.$$

Alors, il existe deux entiers y_1 et y_2 tels que

$$\frac{z^n - 1}{z - 1} = y_1^q \quad \text{et} \quad \frac{z^n + 1}{z + 1} = y_2^q . \tag{7}$$

PREMIÈRE ÉTAPE.

Eliminant z^n du système (7), on obtient l'équation

$$(z + 1)\, y_2^q - (z - 1)\, y_1^q = 2 ,$$

à laquelle on peut appliquer le raffinement des formes linéaires de logarithmes mentionné plus haut. Ainsi, on borne q et on obtient que q est majoré par 200, indépendamment de $z \geq 5$, et par 132, indépendamment de $z \geq 12$.

DEUXIÈME ÉTAPE.

Avant toute chose, on observe que Saradha et Shorey [42] ont démontré que l'on a nécessairement $(z\,\varphi(z), q) = 1$, où φ est l'indicateur d'Euler. Or cette information supplémentaire nous permet d'appliquer un lemme de nature hypergéométrique, démontré par Le [27] puis raffiné par Saradha et Shorey [42]. On obtient ainsi une très bonne majoration de z en fonction de q, à savoir $z \leq 1.61\, q^{1/2}$. En réalité, on démontre des estimations plus précises, lesquelles, combinées au résultat de la première étape, entraînent $z \leq 11$. Par conséquent, on est ramené à étudier un nombre fini de paires (z, q).

TROISIÈME ÉTAPE.

Pour chaque paire (z, q) restante, on vérifie que n est congru à 1 modulo q. Pour cela, on regarde l'équation $x^n - 1 = (x - 1)\, y^q$, avec x et q fixés. Si p est un nombre premier de la forme $kq + 1$, alors $(y^q)^k \equiv 1 \pmod p$, donc y^q ne prend qu'un petit nombre de valeurs modulo p. Ainsi n ne prend également qu'un petit nombre de valeurs modulo $p - 1$, en particulier modulo q. Pour obtenir le résultat souhaité, l'expérience montre qu'il suffit de considérer en général deux ou trois tels nombres premiers p, en tout cas rarement plus de six.

QUATRIÈME ÉTAPE.

Compte tenu des trois étapes précédentes, on est ramené à considérer un nombre fini d'équations de la forme

$$xX^q - (x - 1)Y^q = \pm 1 .$$

Plus précisément, il ne reste à traiter que les équations

$$\begin{aligned} 5X^q - 4Y^q &= 1, && 17 \leq q \leq 71\,, \\ 6X^q - 5Y^q &= 1, && 17 \leq q \leq 67\,, \\ 7X^q - 8Y^q &= -1, && 17 \leq q \leq 61\,. \end{aligned}$$

Ce sont toutes des équations de Thue, dont on sait majorer explicitement la taille des solutions, et par conséquent *en principe*, les déterminer toutes. Or les meilleures bornes actuellement connues sont de l'ordre de $10^{10^{500}}$, donc bien trop élevées pour envisager une résolution complète. Qu'à cela ne tienne ! Comme, grâce à l'étape précédente, on sait que n est de la forme $\nu q + 1$, on cherche en fait à montrer que ces équations ne possèdent aucune solution (X, Y) avec X ou Y une puissance ν-ième. On a donc une majoration de ν, puis de n, de l'ordre de 10^{500}. Pour conclure, on utilise à nouveau des arguments modulaires afin de montrer que n est nécessairement congru à 1 modulo un entier M, suffisamment grand (i.e. $> 10^{500}$).

6. OÙ APPARAISSENT LES FORMES LINÉAIRES DE LOGARITHMES p-ADIQUES

Comme on l'a vu dans la partie 4, les formes linéaires de logarithmes permettent de minorer non trivialement la distance d'un produit de nombres algébriques à 1. On travaille alors avec la valeur absolue archimédienne, et on peut raisonnablement se demander si un énoncé du même style est valable pour les valeurs absolues p-adiques. La réponse est oui (cf. les travaux de Van der Poorten et de Kunrui Yu), et on déduit du résultat principal de [15] la minoration suivante pour la distance p-adique entre deux puissances de nombres rationnels.

THÉORÈME 11. *Soient p un nombre premier, x_1/y_1 et x_2/y_2 deux nombres rationnels non nuls et multiplicativement indépendants, que l'on suppose être des unités p-adiques. Soient m_1 et m_2 deux entiers rationnels strictement positifs. Notons $m = \max\{m_1, m_2, 2\}$ et désignons par H_i, $i = 1, 2$, deux nombres réels tels que $H_i \geq \max\{|x_i|, |y_i|, 2\}$. Alors, la valuation p-adique $v_p(\Lambda)$ de*

$$\Lambda = \left(\frac{x_1}{y_1}\right)^{m_1} - \left(\frac{x_2}{y_2}\right)^{m_2}$$

est majorée par

$$v_p(\Lambda) \leq 2000\, p \, \log H_1 \, \log H_2 \, \log^2 m\,.$$