3. Application des formes linéaires de logarithmes : RÉSULTATS DE FINITUDE

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **25.05.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

que $x^m + 1 = y_1^q$. On retrouve alors l'équation de Catalan, qui n'admet qu'un nombre fini de solutions (cf. Tijdeman [50]), mais, même si l'on dispose d'informations très précises relatives aux éventuelles solutions non triviales de cette équation (cf. entre autres l'ouvrage de Ribenboim [40] et le survol de Mignotte [35]), la résolution complète de (1) sous l'hypothèse n pair demeure un problème ouvert.

Par applications successives du Théorème 2 en prenant pour D la puissance du plus grand facteur premier de n qui divise exactement n, on démontre la première partie de l'énoncé suivant, la seconde étant détaillée dans [40].

THÉORÈME 3. *Si l'équation* (1) *possède une solution* (x, y, n, q) *et si* n *s'écrit comme produit de facteurs premiers* $n = 2^a p_1^{u_1} \dots p_\ell^{u_\ell}$, *avec* $a \in \{0, 1\}$ *et* $u_i > 0$, *alors, pour tout* $1 \leq i \leq \ell$, *il existe un entier* y_i *tel que*

$$\frac{x^{p_i^{u_i}} - 1}{x - 1} = y_i^q .$$

En outre, il existe des entiers $w_i \geq 2$ *et* $z_i \geq 2$ *tels que*

$$\frac{w_i^{p_i} - 1}{w_i - 1} = z_i^q \quad ou \quad p_i z_i^q ,$$

la deuxième possibilité ne pouvant se produire que si q *divise* u_i.

Il découle facilement de ce qui précède qu'afin de démontrer la Conjecture B il suffit de prouver que (1) ne possède qu'un nombre fini de solutions (x, y, p^a, q) où p est premier et $a \geq 1$.

3. APPLICATION DES FORMES LINÉAIRES DE LOGARITHMES : RÉSULTATS DE FINITUDE

La théorie des formes linéaires de logarithmes, initialement développée par Baker [1, 2], s'est avérée, et continue à s'avérer, très riche d'applications dans le domaine des équations diophantiennes. A la différence des résultats d'approximation diophantienne obtenus par Thue, Siegel et Roth, elle conduit à des énoncés effectifs, en ce sens qu'elle permet non seulement d'affirmer que certaines équations n'ont qu'un nombre fini de solutions, mais également d'expliciter une borne numérique, certes souvent très élevée, pour la taille des éventuelles solutions. En outre, la théorie des formes linéaires de logarithmes permet d'apporter de précieuses informations sur certaines équations

exponentielles, dont par exemple l'équation de Catalan, pour lesquelles les méthodes antérieures se révélaient inopérantes. Avant d'expliquer en quelques lignes dans la partie suivante de quoi il retourne, nous présentons deux énoncés issus de cette théorie et montrons comment ils s'appliquent à (1).

THÉORÈME 4. *Soient a_1 et a_2 deux entiers non nuls premiers entre eux tels que $|a_1 a_2| \geq 2$. Soit $f(X) \in \mathbf{Z}[X]$ un polynôme irréductible de degré ≥ 3 (resp. ≥ 2) et soit b un entier non nul. Alors les équations*

$$a_1^n \pm a_2^n = b\,y^q \text{ en inconnues } n \geq 0,\ y \in \mathbf{Z} \setminus \{0\} \text{ et } q \geq 2$$

et

$$f(x) = b\,y^q \text{ en inconnues } x \in \mathbf{Z},\ y \in \mathbf{Z} \setminus \{0\} \text{ et } q \geq 2 \text{ (resp. } q \geq 3)$$

ne possèdent qu'un nombre fini de solutions, dont on peut explicitement majorer les valeurs absolues.

La démonstration du Théorème 4 se trouve par exemple dans l'ouvrage de Shorey et Tijdeman [48], où figure également le résultat suivant, qui s'en déduit relativement facilement.

THÉORÈME 5. *L'équation* (1) *n'admet qu'un nombre fini de solutions (x, y, n, q) si l'une au moins des conditions suivantes est vérifiée :*

(i) *x est fixé,*

(ii) *n a un diviseur premier fixé p,*

(iii) *y a un diviseur premier fixé p.*

Démonstration. Pour prouver l'assertion (i), il suffit de remarquer que (1) s'écrit $x^n - 1 = (x-1)\,y^q$ et donc que le Théorème 4 s'applique, avec $a_1 = x$, $a_2 = 1$ et $b = x - 1$.

Le cas $p = 2$ de (ii) ayant déjà été considéré au cours de la partie précédente, on peut supposer p impair. Un argument de factorisation montre alors qu'il existe deux entiers positifs r et s, avec $rs \leq p$, et un entier $y_1 > 0$ divisant y tels que $(x^{n/p}, y_1, q)$ soit solution de l'équation

$$r\,\frac{z^p - 1}{z - 1} = s\,Y^q, \tag{4}$$

en inconnues $z > 2$, $Y > 1$ et $q \geq 2$. Si $p \geq 5$ ou si $p = 3$ et $q \geq 3$, il découle du Théorème 4 que (4) n'admet qu'un nombre fini de solutions.

Ainsi, il ne reste plus qu'à examiner le cas $p = 3$ et $q = 2$, pour lequel de simples considérations de congruences conduisent au résultat (cf. [48]).

Démontrons maintenant (iii). Si p divise $x - 1$, alors $(x^n - 1)/(x - 1) \equiv n \pmod{p}$, donc p divise n et on est ramené à (ii). Dans le cas contraire, soit $t > 1$ le plus petit entier $u > 1$ tel que p divise $x^u - 1$. Il est clair que t divise $p - 1$. En outre, t divise n puisque $x^n - 1 \equiv 0 \pmod{p}$. Ainsi, n est multiple d'un des diviseurs premiers de $p - 1$ et on est également ramené à (ii). $\square$

4. Un outil important : les formes linéaires de logarithmes

Après avoir détaillé quelques-unes parmi les nombreuses conséquences des résultats de Baker, nous expliquons brièvement ce qu'est une forme linéaire de logarithmes, puis donnons un exemple de raffinement, a priori modeste, mais très riche de conséquences.

Soit $n \geq 1$ et, pour $1 \leq i \leq n$, soient x_i/y_i des nombres rationnels non nuls et m_i des entiers non nuls. Notons $m \geq 2$ un majorant des $|m_i|$ et $H_i \geq 3$ un majorant des quantités $|x_i|$ et $|y_i|$. On suppose que

$$\Lambda := \left| \left(\frac{x_1}{y_1}\right)^{m_1} \cdots \left(\frac{x_n}{y_n}\right)^{m_n} - 1 \right|$$

est non nul. Alors, par une simple estimation du dénominateur de Λ, on obtient

$$\log \Lambda \geq -\sum_{i=1}^{n} m_i \log |y_i| \geq -m \sum_{i=1}^{n} \log H_i .$$

La dépendance en les H_i est très satisfaisante, au contraire de celle en m. Or, pour résoudre de nombreux problèmes en théorie des nombres, on aimerait disposer d'une meilleure estimation du point de vue de m, quitte à faire quelques concessions relativement aux H_i. Baker [1, 2] a, le premier, démontré un tel résultat, et on sait maintenant (d'après Baker et Wüstholz [3]) que, sous les hypothèses précédentes, on a

$$\log \Lambda \geq -(50n)^{2n} \log H_1 \ldots \log H_n \log m , \tag{5}$$

et on conjecture que l'on peut remplacer le produit des $\log H_i$ par leur somme. Cela a été démontré par Shorey [43] (voir également les estimations de Waldschmidt [51], qui incluent tous les raffinements connus en 1993) dans le cas particulier où les rationnels x_i/y_i sont tous très proches de 1. Un exemple spectaculaire d'application est donné par l'équation