4. Un outil important : les formes linéaires de logarithmes

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). □

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

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

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

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

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

$$|(b+1)x^m - by^m| = 1, \quad \text{en inconnues } b \geq 2,\ x > 0,\ y > 0,$$

qui conduit à estimer la quantité

$$\frac{1}{by^m} = \left| \frac{b+1}{b} \left(\frac{x}{y}\right)^m - 1 \right|.$$

De (5) découle la minoration

$$-m \log y \geq -10^8 \log(b+1) \log y \log m,$$

mais, comme $(b+1)/b$ et x/y sont très proches de 1 quand x, y et b sont grands, on peut appliquer le raffinement et, par conséquent, obtenir (par exemple en utilisant [26], où l'on observe cependant que le « $\log m$ » de (5) est alors remplacé par « $\log^2 m$ »)

$$-m \log y \geq -10^8 \log y \log^2 m,$$

soit une majoration de m indépendante de b, résultat dû originellement à Mignotte [33], puis raffiné par Bennett et de Weger [5], qui ont démontré le théorème suivant.

THÉORÈME 6. *Soient a, b et n des entiers vérifiant $a > b \geq 1$ et $n \geq 3$. Alors l'équation*

$$|ax^n - by^n| = 1$$

admet au plus une solution en entiers positifs (x, y), sauf éventuellement si $a = b+1$, $2 \leq b \leq \min\{0.3\,n, 83\}$ et $17 \leq n \leq 347$.

Le Théorème 6 a été démontré indépendamment par Delone [22] et Nagell [38] pour $n = 3$ et par Ljunggren [32] dans le cas $n = 4$.

Tout d'abord, il convient de souligner que le cas $(a, b) = (2, 1)$ du Théorème 6 est une conséquence d'un résultat difficile de Darmon et Mérel [21], qui ont prouvé que l'équation diophantienne $X^n + Y^n = 2Z^n$ avec $n \geq 3$ n'admet comme solutions entières que les solutions triviales. Leur démonstration reprend des idées développées par Wiles afin de résoudre la conjecture de Fermat.

A l'exception de ce cas particulier, le Théorème 6 fait appel à trois techniques d'approximation diophantienne, que l'on présente brièvement sous l'hypothèse additionnelle $a = b+1$, destinée uniquement à simplifier les explications. La première, les formes linéaires en deux logarithmes, a été évoquée plus haut: elle permet de majorer n indépendamment de b. La seconde repose sur l'observation suivante. Si $|(b+1)x^n - by^n| = 1$, alors

$$\left|\sqrt[n]{1+\frac{1}{b}}-\frac{x}{y}\right|<\frac{1}{bny^n} \tag{6}$$

et donc le nombre algébrique $\sqrt[n]{1+1/b}$ admet une très bonne approximation rationnelle, en l'occurrence x/y. Or, à l'aide de techniques basées sur la construction explicite des approximants de Padé de la fonction $z \mapsto \sqrt[n]{1-z}$, il est possible, pour certaines valeurs de b et de n, de construire une suite de rationnels $(p_m/q_m)_m$ qui contient *toutes* les bonnes approximations rationnelles de $\sqrt[n]{1+1/b}$. En outre, on contrôle bien les différences $\left|\sqrt[n]{1+1/b}-p_m/q_m\right|$, et on peut ainsi en déduire qu'aucun rationnel x/y ne vérifie (6). Cette méthode est efficace quand n et b ne sont pas trop petits, mais elle reste d'un emploi délicat, et son succès n'est pas *a priori* assuré.

Le troisième outil utilisé par Bennett et de Weger est la théorie algorithmique des nombres : à l'aide de calculs sur ordinateur, utilisant des algorithmes astucieux, ils ont complètement résolu les équations appelées *équations de Thue* $|(b+1)x^n - by^n| = \pm 1$, pour $(b,n) \in \{(2,5),(2,7),(2,11),(2,13),(3,13)\}$. Cela illustre bien les limites de ce que l'on savait faire vers 1996. A l'heure actuelle, on peut imaginer pouvoir résoudre par cette méthode toutes les paires (b,n) avec $17 \leq n \leq 21$ et $2 \leq b \leq 0.3n$.

Au prix de longs efforts, le Théorème 6 a été amélioré par Bennett [4], qui a raffiné la seconde technique et prouvé le résultat remarquable suivant.

THÉORÈME 7. *Soient a, b et n des entiers vérifiant $a > b \geq 1$ et $n \geq 3$. Alors l'équation*

$$|ax^n - by^n| = 1$$

admet au plus une solution en entiers positifs (x,y).

Il est alors facile d'en déduire un résultat démontré indépendamment par Mignotte [34], mais par une autre méthode.

THÉORÈME 8. *La seule solution (x,y,n,q) de l'équation (1) avec $n \equiv 1 \pmod{q}$ est $(3,11,5,2)$.*

Démonstration. Au vu du Théorème 1, on peut supposer que q est un nombre premier impair. Posons $n = \nu q + 1$, l'équation (1) s'écrit alors $x(x^\nu)^q - (x-1)y^q = 1$, et il suffit d'appliquer le Théorème 7 pour constater qu'il n'y a alors pas de solution. □

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

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