8. Une extension du théorème de Nagell et Ljunggren

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

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

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

PDF erstellt am: **21.09.2024**

prendre des valeurs arbitrairement grandes. Toutefois, une légère modification de l'argument précédent nous a permis [16, 18] de résoudre (9) et plus généralement de résoudre (1) pour tout x assez petit.

THÉORÈME 13. *Si l'équation* (1) *possède une quatrième solution* (z^t, y, n, q), *alors* $z > 10000$ *si* $t \geq 1$, *et* $z > 10^6$ *si* $t = 1$.

Pour démontrer ce résultat, on commence par appliquer le Théorème 12, et on se retrouve alors avec un petit nombre d'équations à traiter du type

$$\frac{z^{tn} - 1}{z^t - 1} = y^q ,$$

où q divise $\varphi(z)$, que l'on traite à l'aide de la méthode décrite dans [16].

8. UNE EXTENSION DU THÉORÈME DE NAGELL ET LJUNGGREN

Le Théorème 5 affirme que (1) n'a qu'un nombre fini de solutions (x, y, n, q) pour lesquelles n est divisible par un nombre premier p ; cependant, (1) n'est complètement résolue que dans le cas $p = 3$ (cf. Théorème 1). La méthode que nous présentons maintenant et qui fait l'objet de [14] permet d'étendre les résultats de Nagell et Ljunggren aux nombres premiers $p = 5, 7, 11$ et 13, ainsi que de résoudre (1) pour certaines petites valeurs de p et q.

THÉORÈME 14. *Si* (x, y, n, q) *est une éventuelle quatrième solution de* (1) *et si* p *est un diviseur premier impair de* n, *alors ou bien* $p \geq 29$, *ou bien* $(p, q) \in \{(17, 17), (19, 19), (23, 23)\}$. *En outre, on a* $(p, q) \notin \{(29, 5), (29, 19), (29, 23), (31, 23), (37, 5), (37, 7), (37, 11), (67, 5)\}$, *et si* $q = 3$, *alors* $p \geq 101$.

Nous indiquons maintenant les grandes lignes de la démonstration. Soient $p \geq 5$ un nombre premier et n un multiple de p. Le Théorème 3 entraîne que si l'équation (1) a une solution (x, y, n, q), alors l'une des équations

$$\frac{x^p - 1}{x - 1} = y^q, \qquad \frac{x^p - 1}{x - 1} = p\, y^q \tag{10}$$

admet une solution vérifiant $x \geq 2$. Il nous suffit donc de résoudre ces deux équations pour les couples (p, q) figurant dans l'énoncé du Théorème 14. Au premier abord, cela semble irréaliste car les bornes théoriques pour la taille des solutions des équations superelliptiques $f(x) = ay^m$ sont très élevées, et, sauf dans certains cas bien particuliers *ad hoc*, l'ordinateur ne peut les résoudre dès que, disons, $m \times \deg(f)$ excède 20. Cependant, dans les deux exemples qui nous intéressent, le polynôme f est cyclotomique et possède ainsi de nombreuses propriétés que l'on peut exploiter, pourvu que p soit différent de q et que q ne divise pas le nombre de classes relatif du p-ième corps cyclotomique. Cette méthode, dont l'origine remonte à des travaux de Bilu [6] et Bilu et Hanrot [7], et qui a également été utilisée avec succès dans le cadre de l'équation de Catalan [13], permet de majorer x par une borne de l'ordre de $p^q q^{pq}$, et il suffit alors d'une simple énumération pour achever la résolution des équations (10).

Par ailleurs, un résultat classique de la théorie des équations diophantiennes exponentielles affirme que, pour les équations (10), on sait majorer q en fonction de p. Les bornes reposent entre autres sur des minorations de formes linéaires en ≥ 3 logarithmes, et sont de ce fait très élevées : supérieures à $(3p)^{10p}$ si l'on applique les meilleures estimations actuelles [8]. Or, grâce aux propriétés des polynômes cyclotomiques, il s'avère en fait possible de ne faire appel qu'à des formes linéaires en deux logarithmes pour borner q en fonction de p dans les équations (10) : on obtient alors par exemple $q \leq 5521$ pour $p = 5$, et $q \leq 9000p^2 \log^4 p$ pour tout p premier. Il ne reste alors plus qu'un nombre raisonnable de couples $(5, q)$ à traiter, pour lesquels on applique la méthode décrite dans le précédent paragraphe... si toutefois p n'est pas égal à q ! Dans le cas contraire, on se voit contraint d'utiliser les techniques développées par Bilu et Hanrot [7] et, malgré de multiples astuces de programmation, les capacités actuelles des ordinateurs ne nous permettent pas de résoudre (10) dès que $p = q \geq 17$.

9. AUTRES RÉSULTATS

On désigne par $\omega(n)$ le nombre de facteurs premiers distincts de l'entier rationnel $n \geq 2$. Shorey [44, 45] a démontré des versions plus faibles des Théorèmes 8 et 9 (sa conclusion est la finitude du nombre de solutions et non la résolution complète), desquelles il a déduit de nouvelles informations relatives à (1). En examinant ses démonstrations, il s'avère que, grâce aux Théorèmes 8 et 9, on peut maintenant démontrer le résultat suivant.