2. Les résultats de Nagell et Ljunggren

2. Les résultats de Nagell et Ljunggren

L'énoncé suivant regroupe les résultats obtenus par Nagell [36, 37] puis complétés par Ljunggren [31], qui traitent plusieurs cas particuliers de (1).

THÉORÈME 1. *A l'exception des solutions* (S), *l'équation* (1) *ne possède aucune solution* (x, y, n, q) *si l'une des hypothèses suivantes est vérifiée :*

(i) $q = 2$,

(ii) 3 *divise* n,

(iii) 4 *divise* n,

(iv) $q = 3$ *et* $n \not\equiv 5 \pmod 6$.

Les démonstrations sont élémentaires, en ce sens qu'elles ne font appel à aucune autre théorie que l'arithmétique des anneaux $\mathbf{Z}[i]$ et $\mathbf{Z}[(1 + i\sqrt{3})/2]$. Elles sont cependant trop longues pour être détaillées ici, et le lecteur intéressé est invité à consulter l'ouvrage de Ribenboim [40]. Pour (iii), nous mentionnons simplement que si (x, y, n, q) est solution de (1) avec $n = 2^a m$, $a \geq 1$ et $m \geq 3$ impair, alors il existe un entier y_1 divisant y tel que (x, y_1, m, q) est solution de (1). Les démonstrations de (i) et (ii) reposent sur un semblable résultat de factorisation, qui s'avère d'ailleurs très utile pour d'autres questions, et dont nous reprenons ci-dessous un énoncé très général obtenu par Shorey [45]. Quant à (iv), sa démonstration fait appel à un résultat de Nagell [38].

NOTATIONS. On convient de noter (a, b) le plus grand diviseur commun aux entiers a et b et de désigner par φ l'indicateur d'Euler. En outre, pour tout entier $n \geq 1$, on note $G(n)$ la partie sans facteur carré de n et $Q_n := \varphi(G(n))$ le nombre d'entiers compris entre 1 et $G(n)$ et premiers avec $G(n)$.

THÉORÈME 2. *Soit* (x, y, n, q) *une solution de* (1) *avec* n *impair. Si le diviseur* D *de* n *vérifie* $(D, n/D) = (D, Q_{n/D}) = 1$, *alors il existe des entiers* y_1 *et* y_2 *tels que* $y_1 y_2 = y$ *et*

$$\frac{(x^D)^{n/D} - 1}{x^D - 1} = y_1^q \quad \text{et} \quad \frac{x^D - 1}{x - 1} = y_2^q .$$

Soit (x, y, n, q) est une solution de (1) avec n pair, et posons $n = 2m$. Le cas n multiple de 4 étant couvert par le Théorème 1, on peut supposer m impair et il est facile de voir qu'il existe alors un entier y_1 divisant y tel

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*

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

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