Université
franco-allemande
Deutsch-Französische
Hochschule

Résumé:

Cette thèse examine quelques approches aux équations diophantiennes, en particulier les connexions entre l'analyse diophantienne et la théorie des corps cyclotomiques.

Tout d'abord, nous proposons une introduction très sommaire et rapide aux méthodes d'analyse diophantienne que nous avons utilisées dans notre travail de recherche. Nous rappelons la notion de hauteur et présentons le PGCD logarithmique.

Ensuite, nous attaquons une conjecture, formulée par Skolem en 1937, sur une equation diophantienne exponentielle. Pour cette conjecture, soit $\mathbb{K}$ un corps de nombres, $\alpha_1, \dots, \alpha_m, \lambda_1, \dots, \lambda_m$ des éléments non-nuls de $\mathbb{K}$, et S un ensemble fini de places de $\mathbb{K}$ (qui contient toutes les places infinies), de telle sorte que l'anneau de S-entiers

$$\mathcal{O}_S = \mathcal{O}_{\mathbb{K},S} = \{\alpha \in \mathbb{K} : |\alpha|_v \le 1 \text{ for places } v \notin S\}$$

contienne $\lambda_1, \dots, \lambda_m, \alpha_1, \dots, \alpha_m, \alpha_1^{-1}, \dots, \alpha_m^{-1}$. Pour chaque $n \in \mathbb{Z}$, soit $A(n) = \lambda_1\alpha_1^n + \dots + \lambda_m\alpha_m^n \in \mathcal{O}_S$. Skolem a suggéré [S1]:

Conjecture 0.1 (Principe local-global exponentiel)**.** *Supposons que pour chaque ideal non-nul $\mathfrak{a}$ de l'anneau $\mathcal{O}_S$, il existe $n \in \mathbb{Z}$ tel que $A(n) \equiv 0 \bmod \mathfrak{a}$. Alors il existe $n \in \mathbb{Z}$ tel que $A(n) = 0$.*

Soit Γ le groupe multiplicatif engendré par $\alpha_1, \dots, \alpha_m$. Alors Γ est le produit d'un groupe abélien fini et d'un groupe libre de rang fini. Nous démontrons que cette conjecture est vraie lorsque le rang de Γ est un.

Après cela, nous généralisons un résultat précédent de Mourad Abouzaid ([A]). Soit $F(X,Y) \in \mathbb{Q}[X,Y]$ un $\mathbb{Q}$-polynôme irréductible. En 1929, Skolem [S2] a démontré le beau théorème suivant:

Theorem 0.2 (Skolem)**.** *Supposons que*

$$F(0,0) = 0.$$

Alors, pour tout entier non-nul d, l'équation n'adment qu'un nombre fini de solutions entières $(X,Y) \in \mathbb{Z}^2$ telles que $\operatorname{pgcd}(X,Y) = d$.

En 2008, Mourad Abouzaid [A] a généralisé ce résultat en travaillant avec des entiers algébriques arbitraires et en obtenant une relation asymptotique entre les hauteurs des coordonnées et leur PGCD logarithmique. Il a démontré le théorème suivant:

Theorem 0.3 (Abouzaid)**.** *Supposons que $(0,0)$ soit un point non-singulier de la courbe plane $F(X,Y) = 0$. Soit $m = \deg_X F$, $\quad n = \deg_Y F$, $\quad M = \max\{m,n\}$. Soit ε tel que $0 < \varepsilon < 1$. Alors, pour toute solution $(\alpha, \beta) \in \bar{\mathbb{Q}}^2$ de $F(X,Y) = 0$, nous avons soit*

$$\max\{\mathrm{h}(\alpha), \mathrm{h}(\beta)\} \le 56M^8\varepsilon^{-2}\mathrm{h}_p(F) + 420M^{10}\varepsilon^{-2}\log(4M),$$

soit

$$\max\{|\mathrm{h}(\alpha) - n\mathrm{lgcd}(\alpha,\beta)|,|\mathrm{h}(\beta) - m\mathrm{lgcd}(\alpha,\beta)|\} \leq \varepsilon \max\{\mathrm{h}(\alpha),\mathrm{h}(\beta)\}+ \\ + 742M^7\varepsilon^{-1}\mathrm{h}_p(F) + 5762M^9\varepsilon^{-1}\log(2m+2n).$$

Cependant, il a imposé la condition que $(0,0)$ soit un point non-singulier de la courbe plane $F(X,Y) = 0$. En utilisant des versions quelque peu différentes du lemme “absolu” de Siegel et du Lemme d’Eisenstein, nous avons pu lever la condition et démontrer le théorème de façon générale. Nous démontrons le théorème suivant:

Theorem 0.4. *Soit $F(X,Y) \in \bar{\mathbb{Q}}[X,Y]$ un polynôme absolument irréductible qui satisfasse $F(0,0) = 0$. Soit $m = \deg_X F$, $n = \deg_Y F$ et $r = \min\left\{i+j : \frac{\partial^{i+j}F}{\partial^i X \partial^j Y}(0,0) \neq 0\right\}$. Soit ε tel que $0 < \varepsilon < 1$. Alors, pour tout $\alpha,\beta \in \bar{\mathbb{Q}}$ tel que $F(\alpha,\beta) = 0$, nous avons soit*

$$\mathrm{h}(\alpha) \leq 200\varepsilon^{-2}mn^6(\mathrm{h}_p(F) + 5)$$

ou

$$\left|\frac{\mathrm{lgcd}(\alpha,\beta)}{r} - \frac{\mathrm{h}(\alpha)}{n}\right| \leq \frac{1}{r}(\varepsilon\mathrm{h}(\alpha) + 4000\varepsilon^{-1}n^4(\mathrm{h}_p(F) + \log(mn) + 1) + \\ + 30n^2m(\mathrm{h}_p(F) + \log(nm))).$$

Ensuite, nous donnons un aperçu des outils que nous avons utilisés dans les corps cyclotomiques. Nous tentons de développer une approche systématique pour un certain genre d’équations diophantiennes. Nous proposons quelques résultats sur les corps cyclotomiques, les anneaux de groupe et les sommes de Jacobi, qui nous seront utiles pour ensuite décrire l’approche.

Finalement, nous développons une application de l’approche précédemment expliquée. Nous considérerons l’équation diophantienne

(1) $$X^n - 1 = BZ^n,$$

où $B \in \mathbb{Z}$ est un paramètre. Definissons $\varphi^*(B) := \varphi(\mathrm{rad}\ (B))$, où $\mathrm{rad}\ (B)$ est le radical de B, et supposons que

(2) $$(n, \varphi^*(B)) = 1.$$

où $\mathrm{rad}\ (B)$ est le radical de B. Pour $B \in \mathbb{N}_{>1}$ fixé, soit

$$\mathcal{N}(B) = \{n \in \mathbb{N}_{>1} \mid \exists\, k > 0 \text{ tel que } n|\varphi^*(B)^k\}.$$

Si p est un premier impair, nous appellerons CF les conditions combinées

I La conjecture de Vandiver est vraie pour p, c’est-à-dire que le nombre de classe h_p^+ du sous-corps réel maximal du corps cyclotomique $\mathbb{Q}[\zeta_p]$, n’est pas divisible par p.

II Nous avons $i_r(p) < \sqrt{p}-1$, en d’autre mots, il y a au plus $\sqrt{p}-1$ entiers impairs $k < p$ tels que le nombre de Bernouilli $B_k \equiv 0 \bmod p$.

Les résultats actuels sur (1) sont restreints aux valeurs de B composées du produit de deux premiers petits $p \leq 13$ [BGMP] et de solutions complètes pour $B < 235$ ([BBGP]). Si nous pensons que l'équation n'a pas de solutions , – avec l'exception potentielle de quelques exemples isolés – il est naturel de considérer le cas où l'exposant n est premier. Bien sûr, l'existence de solutions (X, Z) pour n composé implique l'existence de quelques solutions pour n premier, en élevant X, Z à une puissance.

La contribution principale de notre travail a été de trouver un lien entre (1) lorsque n est premier et que (2) est vérifié, à l'équation diagonale de Nagell – Ljunggren,

$$\frac{X^n - 1}{X - 1} = n^e Y^n, \quad e = \begin{cases} 0 & \text{si } X \not\equiv 1 \bmod n, \\ 1 & \text{sinon.} \end{cases}$$

Ainsi, nous pouvons appliquer des résultats de [M] et démontrer le théorème suivant:

Theorem 0.5. *Soit n un nombre premier et $B > 1$ un entier tel que $(\varphi^*(B), n) = 1$. Supposons que l'équation (1) admette une solution entière non-triviale, différente de $n = 3$ et $(X, Z; B) = (18, 7; 17)$. Soit $X \equiv u \bmod n,\ 0 \leq u < n$ et $e = 1$ si $u = 1$ et $e = 0$ sinon. Alors:*

1. $n > 163 \cdot 10^6$.
2. $X - 1 = \pm B/n^e$ et $B < n^n$.
3. Si $u \notin \{-1, 0, 1\}$, alors la condition CF (II) n'est pas vérifiée pour n et

$$\begin{array}{rcll} 2^{n-1} & \equiv & 3^{n-1} \equiv 1 \mod n^2, & \text{et} \\ r^{n-1} & \equiv & 1 \mod n^2 & \text{pour tout } r | X(X^2 - 1). \end{array}$$

Si $u \in \{-1, 0, 1\}$, alors la condition CF (I) n'est pas vérifiée pour n.

Sur la base de ce théorème, nous démontrons ensuite:

Theorem 0.6. *Si l'équation (1) admet une solution pour B fixé vérifiant les conditions (2), alors, soit $n \in \mathcal{N}(B)$, ou bien il y a un nombre premier p, premier avec $\varphi^*(B)$ et un $m \in \mathcal{N}(B)$ tels que $n = p \cdot m$. De plus X^m, Y^m sont une solution de (1) pour l'exposant premier p et donc vérifient les conditions du théorème 0.5.*

Cela est une amélioration très considérable par rapport aux résultats actuellement connus.

Comme nous utilisons de façon intensive l'article [M], nous avons rajouté en annexe des résultats nouveaux qui permettent de justifier pleinement les résultats annoncés en [M][Theorem 3].

MOTS CLEF

Equations diophantiennes, corps cyclotomiques, equations de Nagell-Ljunggren, Skolem, Abouzaid, equations diophantiennes exponentielles, inégalité de Baker, théorème du sous-espace.

REFERENCES

[A] M. ABOUZAID, *Heights and logarithmic gcd on algebraic curves*, *Int. J. Number Th.* **4**, pp. 177–197 (2008).

[BBGP] A.BAZSO AND A.BÉRCZES AND K.GYÖRY AND A.PINTÉR, *On the resolution of equations $Ax^n - By^n = C$ in integers x , y and n $\geq$ 3, II*, *Publicationes Mathematicae Debrecen* **76**, pp. 227 – 250 (2010).

[BGMP] M. A. BENNETT, K. GYŐRY, M. MIGNOTTE AND Á. PINTÉR, *Binomial Thue equations and polynomial powers*, *Compositio Math.* **142**, pp. 1103–1121 (2006).

[M] P. MIHĂILESCU *Class Number Conditions for the Diagonal Case of the Equation of Nagell and Ljunggren*, *Diophantine Approximation*, Springer Verlag, Development in Mathematics **16**, pp. 245–273 (2008).

[S1] TH. SKOLEM, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*, *Avhdl. Norske Vid. Akad. Oslo I* **12**, pp. 1–16 (1929).

[S2] T. SKOLEM, *Lösung gewisser Gleichungssysteme in ganzen Zahlen oder ganzzahligen Polynomen mit beschrnktem gemeinschaftlichen Teiler*, *Oslo Vid. Akar. Skr. I*, **12** (1929).