Université
franco-allemande
Deutsch-Französische
Hochschule

Summary:

This thesis examines some approaches to address Diophantine equations, specifically we focus on the connection between the Diophantine analysis and the theory of cyclotomic fields.

First, we propose a quick introduction to the methods of Diophantine approximation we have used in this research work. We remind the notion of height and introduce the logarithmic gcd.

Then, we address a conjecture, made by Thoralf Skolem in 1937, on an exponential Diophantine equation. For this conjecture, let $\mathbb{K}$ be a number field, $\alpha_1, \ldots, \alpha_m, \lambda_1, \ldots, \lambda_m$ non-zero elements in $\mathbb{K}$, and S a finite set of places of $\mathbb{K}$ (containing all the infinite places) such that the ring of S-integers

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

contains $\lambda_1, \ldots, \lambda_m, \alpha_1, \ldots, \alpha_m, \alpha_1^{-1}, \ldots, \alpha_m^{-1}$. For every $n \in \mathbb{Z}$, let $A(n) = \lambda_1\alpha_1^n + \cdots + \lambda_m\alpha_m^n \in \mathcal{O}_S$. Skolem suggested [S1]:

Conjecture 0.1 (Exponential Local-Global Principle)**.** *Assume that for every non zero ideal $\mathfrak{a}$ of the ring $\mathcal{O}_S$, there exists $n \in \mathbb{Z}$ such that $A(n) \equiv 0 \bmod \mathfrak{a}$. Then there exists $n \in \mathbb{Z}$ such that $A(n) = 0$.*

Let Γ be the multiplicative group generated by $\alpha_1, \ldots, \alpha_m$. Then Γ is the product of a finite abelian group and a free abelian group of finite rank. We prove that the conjecture is true when the rank of Γ is one.

After that, we generalize a result previously published by Abouzaid ([A]). Let $F(X,Y) \in \mathbb{Q}[X,Y]$ be a $\mathbb{Q}$-irreducible polynomial. In 1929 Skolem [S2] proved the following beautiful theorem:

Theorem 0.2 (Skolem)**.** *Assume that*

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

Then for every non-zero integer d, the equation $F(X,Y) = 0$ has only finitely many solutions in integers $(X,Y) \in \mathbb{Z}^2$ with $\gcd(X,Y) = d$.

In 2008, Abouzaid [A] generalized this result by working with arbitrary algebraic numbers and by obtaining an asymptotic relation between the heights of the coordinates and their logarithmic $\gcd$. He proved the following theorem:

Theorem 0.3 (Abouzaid)**.** *Assume that $(0,0)$ is a non-singular point of the plane curve $F(X,Y) = 0$. Let $m = \deg_X F$, $\quad n = \deg_Y F$, $\quad M = \max\{m,n\}$. Let ε satisfy $0 < \varepsilon < 1$. Then for any solution $(\alpha,\beta) \in \bar{\mathbb{Q}}^2$ of $F(X,Y) = 0$, we have either*

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

or

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

However, he imposed the condition that $(0,0)$ be a non-singular point of the plane curve $F(X,Y)=0$. Using a somewhat different version of Siegel's "absolute" Lemma and of Eisenstein's Lemma, we could remove the condition and prove it in full generality. We prove the following theorem:

Theorem 0.4. *Let $F(X,Y)\in\bar{\mathbb{Q}}[X,Y]$ be an absolutely irreducible polynomial satisfying $F(0,0)=0$. Let $m=\deg_X F$, $n=\deg_Y F$ and $r=\min\left\{i+j:\frac{\partial^{i+j}F}{\partial^i X\partial^j Y}(0,0)\neq 0\right\}$. Let ε satisfy $0<\varepsilon<1$. Then, for any $\alpha,\beta\in\bar{\mathbb{Q}}$ such that $F(\alpha,\beta)=0$, we have either:*

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

or

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

Then, we give an overview of the tools we have used in cyclotomic fields. We try there to develop a systematic approach to address a certain type of Diophantine equations. We discuss on cyclotomic extensions and give some basic but useful properties, on group-ring properties and on Jacobi sums.

Finally, we show a very interesting application of the approach developped in the previous chapter. There, we consider the Diophantine equation

$$X^n-1=BZ^n, \tag{1}$$

where $B\in\mathbb{Z}$ is understood as a parameter. Define $\varphi^*(B):=\varphi(\mathrm{rad}\ (B))$, where $\mathrm{rad}\ (B)$ is the radical of B, and assume that

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

For a fixed $B\in\mathbb{N}_{>1}$ we let

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

If p is an odd prime, we shall denote by CF the combined condition requiring that

I The Vandiver Conjecture holds for p, so the class number h_p^+ of the maximal real subfield of the cyclotomic field $\mathbb{Q}[\zeta_p]$ is not divisible by p.

II We have $i_r(p)<\sqrt{p}-1$, in other words, there is at most $\sqrt{p}-1$ odd integers $k<p$ such that the Bernoulli number $B_k\equiv 0 \bmod p$.

Current results on Equation (1) are restricted to values of B which are built up from two small primes $p\leq 13$ [BGMP] and complete solutions for

$B < 235$ ([BBGP]). If expecting that the equation has no solutions, – possibly with the exception of some isolated examples – it is natural to consider the case when the exponent n is a prime. Of course, the existence of solutions (X, Z) for composite n imply the existence of some solutions with n prime, by raising X, Z to a power.

The main contribution of our work has been to relate (1) in the case when n is a prime and (2) holds, to the diagonal Nagell – Ljunggren equation,

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

This way, we can apply results from [M] and prove the following:

Theorem 0.5. *Let n be a prime and $B > 1$ an integer with $(\varphi^*(B), n) = 1$. Suppose that equation (1) has a non trivial integer solution different from $n = 3$ and $(X, Z; B) = (18, 7; 17)$. Let $X \equiv u \bmod n, 0 \le u < n$ and $e = 1$ if $u = 1$ and $e = 0$ otherwise. Then:*

1. $n > 163 \cdot 10^6$.
2. $X - 1 = \pm B/n^e$ *and* $B < n^n$.
3. If $u \notin \{-1, 0, 1\}$, then condition CF (II) fails for n and

$$\begin{array}{lcll} 2^{n-1} & \equiv & 3^{n-1} \equiv 1 \mod n^2, & \textit{and} \\ r^{n-1} & \equiv & 1 \mod n^2 & \textit{for all } r|X(X^2-1). \end{array}$$

If $u \in \{-1, 0, 1\}$, then Condition CF (I) fails for n.

Based on this theorem, we also prove the following:

Theorem 0.6. *If equation (1) has a solution for a fixed B verifying the conditions (2), then either $n \in \mathcal{N}(B)$ or there is a prime p coprime to $\varphi^*(B)$ and a $m \in \mathcal{N}(B)$ such that $n = p \cdot m$. Moreover X^m, Y^m are a solution of (1) for the prime exponent p and thus verify the conditions in Theorem 0.5.*

This is a strong improvement of the currently known results.

As we have made heavy use of [M], at the end of this thesis we have added an appendix to expose some new result that allows for a full justification of Theorem 3 of [M].

Keywords

Diophantine Equations, Cyclotomic Fields, Nagell-Ljunggren Equation, Skolem, Abouzaid, Exponential Diophantine Equation, Baker's Inequality, Subspace Theorem.

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 $\ge$ 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).