PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 2, *Number* 1, *March* 2017, *pages* 1-12

Michel Waldschmidt

Some Results on Diophantine equations

Written by Louis Nantenaina Andrianaivo

1 Introduction

Let $k \in \mathbb{Q}$, $k \neq 0$, $d \geq 3$ a positive integer and consider an irreducible bivariate form $F(X,Y) = \sum_{i=1}^{d} a_i X^{d-i} Y^i \in \mathbb{Z}[X,Y]$. In 1908, Axel Thue initiated the study of the Diophantine equations of the form $F(X,Y) = k$; this is the reason why they are called **Thue Equations**. Thue obtained one fundamental theorem:

Theorem 1 (Thue 1908) *Let $F \in \mathbb{Z}[X,Y]$ be a homogeneous irreducible form of degree $d \geq 3$:*

$$F(X,Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_{d-1} X Y^{d-1} + a_d Y^d.$$

Let $k \in \mathbb{Z}$, $k \neq 0$. Then there are only finitely many integer solutions $(X,Y) \in \mathbb{Z} \times \mathbb{Z}$ of the Diophantine equation $F(X,Y) = k$.

Since then, the above theorem has been improved by many mathematicians. In this exoposition, we concentrate on the family constructed by E.Thomas, and later generalized by C. Levesque and M. Waldschmidt. One of the first result in diophantine approximation is:

Theorem 2 (Liouville's inequality 1844) *Let α be an algebraic number of degree $d \geq 2$. There exists $c(\alpha) > 0$ such that, for any $\frac{p}{q} \in \mathbb{Q}$ with $q > 0$,*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha)}{q^d}.$$

The inequality of Theorem 2 can be improved for algebraic numbers α of degree $d > 2$. In fact the exponent d in the denominator is best possible for $d = 2$ but it is not for $d \neq 3$. In 1909, Thue proved the following theorem:

Theorem 3 (Thue 1909) *Let α be an algebraic number of degree $d > 2$ and let $\kappa > (\frac{d}{2}) + 1$. Then there exists $c(\alpha, \kappa) > 0$ such that, for any $\frac{p}{q} \in \mathbb{Q}$ with $q > 0$,*

$$\left|\alpha - \frac{p}{q}\right| > \frac{c(\alpha, \kappa)}{q^\kappa}.$$

Later, the exponent κ in the denominator above has been improved:

1921: C.L. Siegel, with $\kappa = 2\sqrt{d}$;

1947: F.J. Dyson and A.O. Gel'fond; with $\kappa = \sqrt{2d}$

1955: K.F. Roth, with any $\kappa > 2$.

There is a close relation between the finiteness of the number of solutions of the Thue's equation and approximation of rational numbers. For example in [2] one can find the proof of the following:

Theorem 4 *Let $f \in \mathbb{Z}[X]$ be an irreducible polynomial of degree d and let $F(X, Y) = Y^d f(X/Y)$ be the associated homogeneous binary form of degree d. Then the following two assertions are equivalent:*
(i) For any $k \in \mathbb{Z}^\times$, $F(X, Y) = k$ has only finitely many solutions in $\mathbb{Z}^2$
(ii) For any real number $\kappa > 0$ and for any root $\alpha \in \mathbb{C}$ of f, there are only finitely many rational numbers $\frac{p}{q}$ such that

$$\left|\alpha - \frac{p}{q}\right| > \frac{\kappa}{q^d}.$$

Note that (i) can be rephrased as:
For any positive integer $k \neq 0$, the set of $(X, Y) \in \mathbb{Z}^2$ verifying

$$0 < |F(X, Y)| \leq k.$$

is finite. Also, for any number field K, for any non-zero element $k \in K$ and for any elements $\alpha_1, \ldots, \alpha_n \in K$ with Card$\{\alpha_1, \ldots, \alpha_n\} \geq 3$, the Thue equation

$$(X - \alpha_1 Y) \cdots (X - \alpha_n Y) = k.$$

has only a finite number of solutions $(X, Y) \in \mathbb{Z} \times \mathbb{Z}$.
Now, one will describe some approach which has been used to deal with Thue equations and discuss a further results related on it.

Theorem 5 (Schmidt's Subspace Theorem 1970) *Let* $L_0, \ldots,$ L_{m-1} *be* $m \geq 2$ *independent linear forms in* m *variables with algebraic coefficients. Let* $\epsilon > 0$*. Then the set*

$$\{X = (X_0, \ldots, X_{m-1}) \in \mathbb{Z}^m : |L_0(X) \cdots L_{m-1}(X)| \leq |X|^{-\epsilon}\}.$$

is contained in the union of finitely many proper subspaces of $\mathbb{Q}^m$.

One can use the above theorem to prove the following celebrated result:

Theorem 6 (Thue, Siegel and Roth) *For any real algebraic number* α*, and for any* $\epsilon > 0$*, there are only finitely many* $o\frac{p}{q} \in \mathbb{Q}$ *with* $q > 0$ *such that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}.$$

In fact, the proof of Thue-Siegel-Roth Theorem can be used to produce an upper bound of the number of solutions of a Diophantine equation in the above family, but no upper bound for the sizes of solutions can be derived. R. Baker and N. I. Fel'dman developed an effective method introduced by A.O. Gel'fond, involving lower bounds for linear combinations of logarithms of algebraic numbers with algebraic coefficients.

Since $e^z - 1 \sim z$ for $z \longrightarrow 0$, determining lower bounds for the following two non-vanishing numbers is equivalent:

$$\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1 \qquad\qquad b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n.$$

The first nontrivial lower bounds were obtained by A.O. Gel'fond. His estimates were effective only for $n = 2$; for $n \geq 3$, he needed to use estimates related to the Thue-Siegel-Roth Theorem.

In 1968, A. Baker succeeded to extend to any $n \geq 2$ the transcendence method used by A.O. Gel'fond for $n = 2$. As a consequence, effective upper bounds for the solutions of Thue's equations have been derived. In the same year, A. Schinzel computed explicitly the constants introduced by A.O. Gel'fond in his lower bound for $|\alpha_1^{b_1} \alpha_2^{b_2} - 1|$.

The approach for solving Thue equations, given by Gel'fond and Baker, is based on the exploitation of Siegel's unit equation: assume $\alpha_1, \alpha_2, \alpha_3$ are algebraic integers and X, Y rational integer such that:$(X - \alpha_1 Y)(X - \alpha_2 Y)(X - \alpha_3 Y) = 1$. The elements $u_1 = X - \alpha_1 Y$,$u_2 = X - \alpha_2 Y$,$u_3 = X - \alpha_3 Y$ are units. By eliminating X and Y in the three linear relations above, we obtain

$$u_1(\alpha_2 - \alpha_3) + u_2(\alpha_3 - \alpha_1) + u_3(\alpha_1 - \alpha_2) = 0.$$

We write it as a Siegel's unit equation in the form

$$\frac{u_1(\alpha_2 - \alpha_3)}{u_2(\alpha_1 - \alpha_3)} - 1 = \frac{u_3(\alpha_2 - \alpha_1)}{u_2(\alpha_1 - \alpha_3)}\cdot$$

By identifying, the quantity $\alpha_1^{b_1} \cdots \alpha_n^{b_n}$ in Gel'fond-Baker Diophantine inequality with the quotient $\frac{u_1(\alpha_2 - \alpha_3)}{u_2(\alpha_1 - \alpha_3)}\cdot$, one can then apply the theory of Siegel's unit equations.

2 Families of Thue equations

There are several families of Thue equations which many mathematicians tried to solve. The first family of Thue equation was given by Thue himself:

$$(a + 1)X^n - aY^n = 1.$$

For n prime and a sufficiently large in term of n (for instance, $n = 3$ and for $a \geq 386$), the only one solution in positive integers X, Y is $X = Y = 1$.

E. Thomas considered the family of the Thue equations $F_n(x, y) = \pm 1$ where $F_n(X, Y) = X^3 - (n-1)X^2Y - (n+2)X - Y^3$. In 1990, he proved in some effective way that the set of $(X, Y, n) \in \mathbb{Z}^3$ such that $n \geq 0$, $\max\{|x|, |y|\} \geq 2$, and $F_n(x, y) = \pm 1$ is finite. In [4] he completely solved the equation $F_n(X, Y) = 1$, for $n \geq 1.365 \cdot 10^7$; the only solutions are $(0, -1)$, $(1, 0)$ and $(-1, 1)$.

D. Shanks introduced the simplest cubic fields $\mathbb{Q}(\lambda)$ by studying the field $\mathbb{Q}(\omega)$ where ω is a solution of

$$F_n(X, 1) = X^3 - (n-1)X^2 - (n+2)X - 1. \tag{1}$$

He proved that if λ is one of the solutions of equation (1), then $\mathbb{Q}(\lambda)$ is a real Galois field.

In 1993, M. Mignotte [5] completed this result by solving this equation for each n. For $n \geq 4$ and for $n = 2$, the only solutions to $F_n(X, Y) = 1$ are $(0, -1)$, $(1, 0)$ and $(-1, 1)$.

M. Mignotte worked with A. Lethö and F. Lemmermeyer. In 1996, they studied, in [6], the family of Diophantine equations $F_n(X, Y) = k$, for $k \neq 0$. They obtained the following theorem,

Theorem 7 (Mignotte, Pethö and Lemmermeyer 1996) *For $n \geq 2$, when X, Y are rational integers verifying*

$$0 <|F_n(X, Y)|\leq k \quad (k \in \mathbb{Z})$$

then

$$\log|y|< c(\log n)(\log n + \log k).$$

with an effectively computable absolute constante c.

When k is a given positive integer, there exists an integer n_0 depending upon k such that $|F_n(X, Y)|\leq k$ with $n \geq 0$ and $|Y|> \sqrt[3]{k}$ implies $n \leq n_0$. But, for $0 \leq|t|\leq \sqrt[3]{m}$, $(-t, t)$ and $(t, -t)$ are solutions, therefore

the condition $|Y|> \sqrt[3]{k}$ cannot be omitted.
Note that Theorem 7 gives an upper bound for $\max\{|x|,|y|\}$ which depends on k and n while we would like a bound only depending on k.
We now come to the main goal of this work: presenting Claude Levesque and Michel Waldschmidt' s approach for solving families of diophantine Thue equation. In 2010, C. Levesque proposed to consider the following version Thomas's family of cubic Thue equations:

$$F_{n,2}(X,Y) = (X - \lambda_{0n}^2 Y)(X - \lambda_{1n}^2 Y)(X - \lambda_{2n}^2 Y).$$

where λ_{in} are units in the totally real cubic field $\mathbb{Q}(\lambda_{0n})$. The natural question was: Does Thomas result hold?
Given any irreducible binary form $F \in \mathbb{Z}[X,Y]$, α a root of $F(X,1)$, and ϵ a unit in the field $\mathbb{Q}(\alpha)$, consider the family of Diophantine equations, $F_a(X,Y) = k$, ($a \in \mathbb{Z}$), where $F_a(X,Y)$ is deduced from $F(X,Y) = \prod_{i=1}^{d}(X - \sigma_i(\alpha)Y)$, by twisting with ϵ^a, assuming $\mathbb{Q}(\alpha) = \mathbb{Q}(\alpha\epsilon^a)$. Here $F_a(X,1)$ is the irreducible polynomial of $\alpha\epsilon^a$ and

$$F_a(X,Y) = \prod_{i=1}^{d}(X - \sigma_i(\alpha\epsilon^a)Y).$$

By using Schmidt's subspace theorem, their first result was: Given α to be an algebraic number of degree $d \geq 3$ and K=$\mathbb{Q}(\alpha)$. Let ϵ be a unit of K such that $\alpha\epsilon$ has degree d, $f_\epsilon(X)$ be the irreducible polynomial of $\alpha\epsilon$ and $F_\epsilon(X,Y)$ be its homogeneous version. Then for all but finitely many of these units, the Thue equation $F_\epsilon(X,Y) = \pm 1$ has only the trivial solution X, Y in $\mathbb{Z}$ where $XY = 0$. Now, let consider

$$F_{n,a}(X,Y) = (X - \lambda_{0n}^a Y)(X - \lambda_{1n}^a Y)(X - \lambda_{2n}^a Y) \quad \in \mathbb{Z}[X,Y].$$

with a new parameter $a \in \mathbb{Z}$.

Q 1 *Are there only finitely many (n, a, X, Y) satisfying $F_{n,a}(X,Y)= \pm 1$?*

For the next result, we need the *absolute logarithmic height h* which is defined by $h(\alpha) = \frac{1}{d} \log M(\alpha)$ where M is the *Malher measure*

$$M(\alpha) = a_0 \prod_{1 \le i \le d} \max\{1, |\sigma_i(\alpha)|\}$$

and a_0 is the leading coefficient of the irreducible polynomial of α over $\mathbb{Z}$.

In 2013, C. Levesque and M. Waldschmidt stated the following conjecture in [3].

Conjecture 1 (Levesque and Waldschmidt 2013) *There exists $\kappa > 0$, constant depending only on α, such that, for any $k \ge 2$, all solutions (X, Y, ϵ) in $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_k^{\times}$ of the inequality*

$$|F_\epsilon(X, Y)| \le k, \text{ with } XY \ne 0 \text{ and } [\mathbb{Q}(\alpha\epsilon) : \mathbb{Q}] = 3,$$

satisfy

$$\max\{|X|, |Y|, e^{h(\alpha\epsilon)}\} \le k^{\kappa}.$$

One year later, they proved the following theorem which is one of the main result presented here. The key point of the proof, is an approach for finding the upper bound for the solution which does not depend on n which we sketch below a complete proof can be found in [1].

Theorem 8 (Levesque and Waldschmidt 2014) *There is an effectively computable absolute constant $c > 0$ such that, if (X, Y, n, a) are nonzero rational integers with* $\max\{|X|\,|Y|\} \ge 2$ *and $F_{n,a}(x, y) = \pm 1$, then* $\max\{|a|\,|n|, |X|\,|X|\} \le c$. *Furthermore, for all $n \ge 0$, the trivial solution with $a \le 2$ are* $(0, 1), (1, 0)$ *and for $a = 2$ is* $(1, 1)$.

Proof. Let us write λ_i for λ_{in} for $i = 0, 1, 2$. Then

$$F_n(X, Y) = X^3 - (n - 1)X^2Y - (n + 2)XY^2 - Y^2.$$

can be written as $F_n(X, Y) = (X - \lambda_0 Y)(X - \lambda_1 Y)(X - \lambda_2 Y)$

so we have: $\begin{cases} n + \frac{1}{n} & \le & \lambda_0 & \le & n + \frac{2}{n}, \\ -\frac{1}{n+1} & \le & \lambda_1 & \le & -\frac{1}{n+2}, \\ -1 - \frac{1}{n} & \le & \lambda_2 & \le & -1 - \frac{1}{n+1}. \end{cases}$

- One defines $\gamma_i = X - \lambda_i^a Y$, $(i = 0, 1, 2)$, so $F_{n,a}(X, Y) = \pm 1$ becomes $\gamma_0\gamma_1\gamma_2 = \pm 1$. By writing γ_i to be γ_{i_0}, we have the bound $|\gamma_{i_0}| \leq \frac{m}{Y^2\lambda_0^a}$. Also we have $\min\{|\gamma_{i_1}|, |\gamma_{i_2}|\} > Y|\lambda_0^a|$.

- By considering the group of units of $\mathbb{Q}(\lambda_0)$, and taking λ_1, λ_2 as a base, there exist $\delta = \pm 1$ and rational integers A and B which verify
$$|A| + |B| \leq \kappa\left(\frac{\log Y}{\log \lambda_0} + a\right),$$
where, $\begin{cases} \gamma_{0,a} &= \delta\lambda_0^A\lambda_2^B, \\ \gamma_{1,a} &= \delta\lambda_1^A\lambda_0^B &= \delta\lambda_0^{-A+B}\lambda_2^{-A}, \\ \gamma_{2,a} &= \delta\lambda_2^A\lambda_1^B &= \delta\lambda_0^{-B}\lambda_2^{A-B}. \end{cases}$

- Transform the following Siegel unit equation,
$$\gamma_{i_0,a}(\lambda_{i_1}^a - \lambda_{i_2}^a) + \gamma_{i_1,a}(\lambda_{i_2}^a - \lambda_{i_0}^a) + \gamma_{i_2,a}(\lambda_{i_0}^a - \lambda_{i_1}^a) = 0,$$
as
$$\frac{\gamma_{i_1,a}(\lambda_{i_2}^a - \lambda_{i_0}^a)}{\gamma_{i_2,a}(\lambda_{i_1}^a - \lambda_{i_0}^a)} - 1 = -\frac{\gamma_{i_0,a}(\lambda_{i_{100}}^a - \lambda_{i_2}^a)}{\gamma_{i_2,a}(\lambda_{i_1}^a - \lambda_{i_0}^a)}.$$
we have the estimate
$$0 < \left|\frac{\gamma_{i_1,a}(\lambda_{i_2}^a - \lambda_{i_0}^a)}{\gamma_{i_2,a}(\lambda_{i_1}^a - \lambda_{i_0}^a)} - 1\right| \leq \frac{2}{Y^3\lambda_0^a}.$$

At the end we have to separate two cases, first, when n is large, the completion of the proof is from the lower bound for a linear form in logarithms of algebraic numbers (Baker's method).
For n bounded, we have results which are valid for the family of Thue equations of Thomas and the completion of the proof follows from the following Lemma,

Lemma 1 *Consider a monic irreducible cubic polynomial $f(X) \in \mathbb{Z}[X]$ with $f(0) = \pm 1$ and write,*
$$F(X, Y) = Y^3 f(X/Y) = (X - \epsilon_1 Y)(X - \epsilon_2 Y)(X - \epsilon_3 Y).$$

For $a \in \mathbb{Z}$, $a \neq 0$, define

$$F_a(X, Y) = (X - \epsilon_1^a Y)(X - \epsilon_2^a Y)(X - \epsilon_3^a Y).$$

Then there exists an effectively computable constant $\kappa > 0$ depending only on f, such that, for any $k \geq 2$, any (x, y, a) in the set

$$\Big\{(X, Y, a) \in \mathbb{Z}^2 \times \mathbb{Z} \mid XYa \neq 0, \max\{|X|, |Y|\} \geq 2, F_a(X, Y) \leq k\Big\}$$

satisfies $\max\{|X|, |Y|, e^{|a|}\} \leq k^\kappa$. □

In 2015, further results were proved in [1]. The following is one of those.

Theorem 9 (Levesque and Waldschmidt 2015) *Let $k \geq 1$. There exists an absolute effectively computable constant κ such that, if there exists $(n, a, k, X, Y) \in \mathbb{Z}^2$ with $a \neq 0$ verifying $0 < |F_{n,a}(X, Y)| \leq k$,*

- *then*
$$\log\{|X|, |Y|\} \leq \kappa\mu.$$
with $\mu = \begin{cases} (\log k + |a| \log|n|)(\log|n|)^2 \log\log|n| & \textit{for } |n| \geq 3, \\ \log k + |a| & \textit{for } |n| \leq 2. \end{cases}$
Note that if $a = 1$, this follows from Theorem 7.

- *if $n \geq 0$, $a \geq 1$ and $|y| \geq 2\sqrt[3]{k}$, then $a \leq \kappa\mu'$ with*
$\mu' = \begin{cases} (\log k + \log n)(\log n) \log\log n & \textit{for } |n| \geq 3, \\ 1 + \log k & \textit{for } n = 0, 1, 2. \end{cases}$

- *if $XY \neq 0$ and $n \geq 0$ and $a \geq 1$, then*
$$a \leq \kappa \max\left\{1, (1 + \log|X|) \log\log(n + 3), \log|Y|, \frac{\log k}{\log(n + 2)}\right\}.$$

References

[1] Claude Levesque and Michel Waldschmidt, *A family of Thue equations involving powers of units of the simplest cubic fields*, 2015.
http://arxiv.org/abs/1505.06708

[2] Claude Levesque and Michel Waldschmidt, *Some remarks on diophantine equations and diophantine approximation*, 2013.
http://arxiv.org/abs/1312.7200

[3] Claude Levesque and Michel Waldschmidt, *Solving effectively some families of Thue Diophantine equations*, 2013.
http://arkiv.org/1312.7205

[4] Emery Thomas, *Complete solutions to a family of cubic Diophantine equations*, Journal of Number Theory, **34**, 235–250, 1990.

[5] Maurice Mignotte, *Verification of a Conjecture of E. Thomas*, Journal of Number Theory, **44**, 172–177, 1993.

[6] Maurice Mignotte, Attila Pethő and Franz Lemmermeyer, *On the family of Thue equations* $x^3-(n-1)x^2y-(n+2)xy^2-y^3=k$, Acta Arithmetica, **76**, 245–269, 1996.

Louis Nantenaina Andrianaivo
Dipartimento di Matematica e Fisica
Università degli studi Roma Tre.
Largo S. L. Murialdo, 1
00146, Roma, Italy.
email: landrianaivo@mat.uniroma3.it