DIOPHANTINE EQUATIONS AND DIOPHANTINE APPROXIMATION

JAN-HENDRIK EVERTSE

1. Introduction

Originally, Diophantine approximation is the branch of number theory dealing with problems such as whether a given real number is rational or irrational, or whether it is algebraic or transcendental. More generally, for a given irrational number one may ask how well it is approximable by a rational number, and for a given transcendental number one may ask how well it can be approximated by algebraic numbers. The basic techniques from Diophantine approximation have been vastly generalized and today, there are some very powerful results with many applications, in particular to Diophantine equations. In this note we will discuss linear equations whose unknowns are taken from a multiplicative group of finite rank. The results we will mention about these equations are consequences of a central theorem in Diophantine approximation, the so-called *Subspace Theorem* of W.M. Schmidt. We will also give some results on linear recurrence sequences. In the last section we will mention some recent developments in Diophantine geometry.

2. Linear equations with unknowns from a multiplicative group

We introduce some terminology. Let $\mathbb{C}^*$ be the multiplicative group of non-zero complex numbers. Let Γ be a subgroup of $\mathbb{C}^*$. Γ is said to be a torsion group if all its elements have finite order, that is, are roots of unity. In that case we say that Γ has rank 0. More generally, Γ is said to be *of finite rank* if there are $a_1, \dots, a_r \in \Gamma$ with the following property: for every $x \in \Gamma$ there exist integers $z_1, \dots, z_r$ and a positive integer m such that $x^m = a_1^{z_1} \cdots a_r^{z_r}$. If Γ is not a torsion group then the smallest r for which such $a_1, \dots, a_r$ exist is called the rank of Γ.

For instance, the group

$$\begin{aligned}\Gamma &= \{x \in \mathbb{C}^* : \exists m \in \mathbb{N},\, z_1, z_2 \in \mathbb{Z} : \, x^m = 2^{z_1} \cdot 3^{z_2}\} \\ &= \{\zeta \sqrt[m]{2^{z_1} 3^{z_2}} : \zeta \text{ root of unity}, \; m \in \mathbb{N},\, z_1, z_2 \in \mathbb{Z}\}\end{aligned}$$

has rank 2. More generally, any subgroup of Γ containing $2, 3$ has rank 2.

First let a, b be non-zero rational numbers and let $\Gamma = \{p_1^{z_1} \cdots p_r^{z_r} : \, z_i \in \mathbb{Z}\}$ be the multiplicative group generated by the prime numbers $p_1, \dots, p_r$. In 1933, Mahler [17] showed that the equation

$$ax + by = 1 \quad \text{in } x, y \in \Gamma \tag{2.1}$$

has only finitely many solutions. In 1960, Lang [13] showed that for any $a, b \in \mathbb{C}^*$ and any subgroup Γ of $\mathbb{C}^*$ of finite rank, the number of solutions of equation (2.1) is finite.

For subgroups Γ of $\mathbb{Q}^*$ there are reasonably efficient algorithms to determine all solutions of (2.1). For instance, consider the equation

$$x + y = 1 \quad \text{in } x, y \in \Gamma = \{2^{z_1} 3^{z_2} 5^{z_3} 7^{z_4} 11^{z_5} 13^{z_6} : \, z_i \in \mathbb{Z}\} \text{ with } x \leqslant y.$$

We give some solutions: $(\frac{1}{2}, \frac{1}{2})$, $(\frac{3}{7}, \frac{4}{7})$, $(\frac{2}{13}, \frac{11}{13})$, $(\frac{3993}{20800}, \frac{16807}{20800}) = (\frac{3 \cdot 11^3}{2^6 \cdot 5^2 \cdot 13}, \frac{7^5}{2^6 \cdot 5^2 \cdot 13})$. In his thesis, [30, Section 6.5], de Weger determined all solutions of this equation, and showed that there are precisely 545 of them.

Our concern is not to determine the solutions of equations of the shape (2.1), but to give uniform upper bounds for the number of their solutions, depending on as few parameters as possible. In 1984, the author [4] showed that in Mahler's case, that is, with $a, b \in \mathbb{Q}^*$ and with Γ the group generated by prime numbers $p_1, \dots, p_r$, equation (2.1) has at most $3 \times 7^{2r+3}$ solutions. This bound is independent of the primes $p_1, \dots, p_r$ and of the coefficients a, b. Building further on work of Schlickewei, in 1996 Beukers and Schlickewei [BS96] proved the following general result:
For any subgroup Γ of $\mathbb{C}^*$ of finite rank r, and any $a, b \in \mathbb{C}^*$, equation (2.1) has at most $2^{16(r+1)}$ solutions.

We mention that in 1988, Erdős, Stewart and Tijdeman [3] proved a result in the other direction:
Let a, b be non-zero rational numbers. Then for every $\varepsilon > 0$ and every sufficiently large r, there is a subgroup Γ of $\mathbb{Q}^*$ of rank r such that (2.1) has at least $e^{(4-\varepsilon) r^{1/2} (\log r)^{-1/2}}$ solutions.

We now turn to equations in $n \geqslant 3$ variables, namely

$$a_1x_1 + \cdots + a_nx_n = 1 \quad \text{in } x_1, \dots, x_n \in \Gamma, \tag{2.2}$$

where Γ is a subgroup of $\mathbb{C}^*$ of finite rank, and $a_1, \dots, a_n \in \mathbb{C}^*$. Assume that Γ is not finite. A solution of equation (2.2) is called *non-degenerate*, if each subsum of the left-hand side is non-zero, i.e.,

$$a_{i_1}x_{i_1} + \cdots + a_{i_t}x_{i_t} \neq 0 \quad \text{for each subset } \{i_1, \dots, i_t\} \text{ of } \{1, \dots, n\}.$$

This non-degeneracy condition is rather natural, since each degenerate solution gives rise to an infinite family of solutions. For instance, if $(x_1, \dots, x_n)$ is a solution of (2.2) with $a_1x_1 + \cdots + a_mx_m = 0$, $a_{m+1}x_{m+1} + \cdots + a_nx_n = 1$, then for every $x \in \Gamma$, $(xx_1, \dots, xx_m, x_{m+1}, \dots, x_n)$ is also a solution of (2.2).

It follows from work of van der Poorten and Schlickewei, the author, and Laurent from the 1980's that (2.2) has only finitely many solutions. The major tool in the proof of this result is W.M. Schmidt's *Subspace Theorem* (see next section).

We mention that in contrast to the two-variable case, no algorithm is known which allows in principle to determine all non-degenerate solutions of (2.2). On the other hand, there are satisfactory explicit upper bounds for the number of non-degenerate solutions of (2.2). In 1990, Schlickewei [24] was the first to give such an upper bound, but only in the special case that Γ is contained in an algebraic number field. Schlickewei's bound depended, apart from the number of variables n and the rank of Γ, on several other parameters and when his work appeared, it was an open problem to deduce a uniform upper bound depending only on n and the rank of Γ. After several intermediate results, Schlickewei, Schmidt and the author ([8], see also the survey paper [6]) succeeded in proving the following theorem:

Theorem 1. *Let Γ be a subgroup of $\mathbb{C}^*$ of finite rank r, and let $a_1, \dots, a_n \in \mathbb{C}^*$. Then equation (2.2) has at most $e^{(6n)^{5n}(r+1)}$ non-degenerate solutions.*

The basic tool was a new quantitative version of Schmidt's Subspace Theorem, obtained by Schlickewei and the author (see [7] or the survey paper [6]). The upper bound in Theorem 1 is probably far from best possible, but one can show that the theorem does not remain valid if the upper bound is replaced by a bound independent of r or n.

We mention that recently, Moree, Stewart, Tijdeman and the author [5] and independently Granville (unpublished) proved the following generalization of the result of Erdős, Stewart and Tijdeman mentioned above:

Theorem 2. *Let $a_1 \dots, a_n$ be non-zero rationals. Then for every $\varepsilon > 0$ and every sufficiently large r there is a subgroup Γ of $\mathbb{Q}^*$ of rank r such that* (2.2) *has at least* $\exp\big((1-\varepsilon)\frac{n^2}{n-1}r^{1-(1/n)}(\log r)^{-(1/n)}\big)$ *non-degenerate solutions.*

The proof is not based on Diophantine approximation but uses instead some analytic number theory.

3. Linear recurrence sequences

The by far best known example of a linear recurrence sequence is the Fibonacci sequence $\{F_n\}_{n=0}^{\infty}$ given by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geqslant 2$. In general a linear recurrence sequence is a sequence $U = \{U_n\}_{n=0}^{\infty}$ of complex numbers given by initial values $U_0, \dots, U_{k-1}$ and by a linear recurrence relation

$$U_n = c_1 U_{n-1} + c_2 U_{n-2} + \cdots + c_k U_{n-k} \quad (n \geqslant k) \tag{3.1}$$

where $c_1, \dots, c_k$ are fixed complex numbers. One may show that there is only one recurrence relation satisfied by U for which k is minimal. Assuming that in relation (3.1), k is minimal, we call k the *order*, and $F_U := X^k - c_1 X^{k-1} - \cdots - c_k$ the *companion polynomial* of U. Write $F_U = (X-\alpha_1)^{e_1} \cdots (X-\alpha_t)^{e_t}$, where $\alpha_1, \dots, \alpha_t$ are the distinct roots of f_U and where $e_1, \dots, e_t$ are positive integers. A basic fact for linear recurrence relations states that there are polynomials $f_i \in \mathbb{C}[X]$ of degree $< e_i$ $(i = 1, \dots, t)$ such that

$$U_n = f_1(n)\alpha_1^n + \cdots + f_t(n)\alpha_t^n \quad \text{for } n \in \mathbb{Z}_{\geqslant 0}. \tag{3.2}$$

The sequence U is called *simple* if all multiplicities e_i are 1, and *non-degenerate* if none of the quotients α_i/α_j $(1 \leqslant i < j \leqslant t)$ is a root of unity (non-degeneracy implies that for any positive integer k, the number of zeros of the companion polynomial of $U^{(k)} := \{U_{nk}\}_{n=0}^{\infty}$ is equal to the number of zeros of the companion polynomial of U).

We are interested in the Diophantine equation $U_n = 0$, that is,

$$f_1(n)\alpha_1^n + \cdots + f_t(n)\alpha_t^n = 0 \quad \text{in } n \in \mathbb{Z}_{\geqslant 0}. \tag{3.3}$$

The classical Skolem-Mahler-Lech theorem (cf. [16]) states that the number of solutions of (3.3) is finite if U is non-degenerate. The proof was by means of p-adic analysis. Denote the number of solutions of (3.3) by N_U. An old conjecture attributed to Ward states that N_U can be bounded above by a quantity depending on the order of U only. Throughout the last decades several partial solutions to this problem have been obtained (Beukers, Tijdeman, Schlickewei, Schmidt). We will mention only the most recent result of Schmidt [27], which completely settles Ward's conjecture.

Theorem (Schmidt). *Suppose U is a non-degenerate linear recurrence sequence of order k. Then $N_U \leqslant \exp\exp\exp(3k\log k)$.*

In his proof, Schmidt used the quantitative version of the Subspace Theorem of Schlickewei and the author mentioned above. But apart from that there were some formidable technical difficulties which Schmidt managed to deal with. We mention that for simple linear recurrence sequences, the polynomials f_i in (3.2) are all constants. So in that case equation (3.3) is just a special case of equation (2.2) and then Theorem 1 implies an upper bound for N_U depending only on k. The case that not all polynomials f_i are constants turned out to be much harder.

4. The Subspace Theorem

We start with some history. Let α be a real irrational algebraic number of degree d and let $\kappa > 0$. In 1909, Thue [28] proved that for any $\kappa > \frac{1}{2}d + 1$, the inequality

$$|\alpha - \frac{x_1}{x_2}| \leqslant \max(|x_1|, |x_2|)^{-\kappa} \tag{4.1}$$

has only finitely many solutions in pairs of integers (x_1, x_2) with $x_2 > 0$. After improvements of Thue's result by Siegel, Gel'fond and Dyson, in 1955 Roth [22] proved that (4.1) has only finitely many solutions in pairs of integers (x_1, x_2) with $x_2 > 0$ already when $\kappa > 2$. This lower bound 2 for κ is best possible, since by a result of Dirichlet from 1842, for any irrational real number α there are infinitely many pairs of integers (x_1, x_2) with

$$|\alpha - \frac{x_1}{x_2}| \leqslant x_2^{-2}, \quad x_2 > 0\,.$$

In a sequence of papers from 1965-1972, W.M. Schmidt proved a far reaching higher dimensional generalization of Roth's theorem, now known as the Subspace Theorem. For a full proof of the Subspace Theorem as well as of the other results mentioned above we refer to Schmidt's lecture notes [25]. Below we have stated the version of the Subspace Theorem which is most convenient for us. We define the norm of $\mathbf{x} = (x_1, \dots, x_n) \in \mathbb{Z}^n$ by $\|\mathbf{x}\| := \max(|x_1|, \dots, |x_n|)$.

Subspace Theorem (Schmidt). *Let*

$$L_1 = \alpha_{11}X_1 + \cdots + \alpha_{1n}X_n, \dots, L_n = \alpha_{n1}X_1 + \cdots + \alpha_{nn}X_n$$

be n linearly independent linear forms with real or complex algebraic coefficients α_{ij}. Let $c_1, \dots, c_n$ be reals with

$$c_1 + \cdots + c_n < 0\,.$$

Consider the system of inequalities

$$|L_1(\mathbf{x})| \leqslant \|\mathbf{x}\|^{c_1}, \dots, |L_n(\mathbf{x})| \leqslant \|\mathbf{x}\|^{c_n} \tag{4.2}$$

to be solved simultaneously in integer vectors $\mathbf{x} \in \mathbb{Z}^n$.
Then there are proper linear subspaces $T_1, \dots, T_t$ of $\mathbb{Q}^n$ such that the set of solutions of (4.2) is contained in $T_1 \cup \cdots \cup T_t$.

Roth's Theorem follows by taking $n = 2$, $L_1 = X_1 - \alpha X_2$, $L_2 = X_2$, $c_1 = 1 - \kappa$, $c_2 = 1$. Thus, if $\mathbf{x} = (x_1, x_2)$ is a solution of (4.1) with $x_2 \neq 0$ then $\mathbf{x}$ also satisfies (4.2).

We give another example to illustrate the Subspace Theorem. Consider the system

$$\left\{\begin{array}{lcl} |x_1 + \sqrt{2}x_2 + \sqrt{3}x_3| & \leqslant & \max(|x_1|, |x_2|, |x_3|)^{3/2} \\ |x_1 - \sqrt{2}x_2 + \sqrt{3}x_3| & \leqslant & \max(|x_1|, |x_2|, |x_3|)^{-1} \\ |x_1 - \sqrt{2}x_2 - \sqrt{3}x_3| & \leqslant & \max(|x_1|, |x_2|, |x_3|)^{-1} \end{array}\right. \tag{4.3}$$

The Pell equation $x_1^2 - 2x_2^2 = 1$ has infinitely many solutions in positive integers x_1, x_2. It is easy to see that if (x_1, x_2) is a solution of the Pell equation with $x_2 \geqslant 2$ and if $x_3 = 0$, then (x_1, x_2, x_3) is a solution of (4.3). Thus, the subspace $x_3 = 0$ contains infinitely many solutions of (4.3). One can prove something more precise than predicted by the Subspace Theorem, that is, that (4.3) has only finitely many solutions with $x_3 \neq 0$.

In 1977, Schlickewei [23] proved a so-called p-adic version of the Subspace Theorem, involving, apart from the usual absolute value, a finite number of p-adic absolute values. Given a rational number $\alpha \in \mathbb{Q}$ and a prime number p, we define $|\alpha|_p := p^{-w}$ where w is the exponent such that $\alpha = p^w \cdot a/b$ with a, b integers not divisible by p. For instance, $|9/8|_2 = 8$ and $|9/8|_3 = 1/9$. The p-adic absolute value $|\cdot|_p$ defines a metric on $\mathbb{Q}$. By taking the metric completion we obtain a field $\mathbb{Q}_p$. Let $\mathbb{C}_p$ denote the algebraic closure of $\mathbb{Q}_p$. The p-adic absolute value can be extended uniquely to $\mathbb{C}_p$. To get a uniform notation, we write $|\cdot|_\infty$ for the usual absolute value $|\cdot|$, and $\mathbb{C}_\infty$ for $\mathbb{C}$. We call ∞ the infinite prime of $\mathbb{Q}$. We will use the index p to indicate either ∞ or a prime number. Then we get:

p-adic Subspace Theorem (Schlickewei). *Let $S = \{\infty, p_1, \dots, p_t\}$ consist of the infinite prime and a finite number of primes numbers. For $p \in S$, let*

$$L_{1p} = \alpha_{11p}X_1 + \cdots + \alpha_{1np}X_n, \dots, L_{np} = \alpha_{n1p}X_1 + \cdots + \alpha_{nnp}X_n$$

be linearly independent linear forms with coefficients $\alpha_{ijp} \in \mathbb{C}_p$ which are algebraic over $\mathbb{Q}$. Further, let c_{ip} $(i = 1, \dots, n,\ p \in S)$ be reals satisfying

$$\sum_{p \in S} \sum_{i=1}^{n} c_{ip} < 0\,.$$

Consider the system of inequalities

$$|L_{ip}(\mathbf{x})|_p \leqslant \|\mathbf{x}\|^{c_{ip}} \quad (p \in S,\ i = 1, \dots, n) \tag{4.4}$$

to be solved simultaneously in $\mathbf{x} \in \mathbb{Z}^n$.
Then there are proper linear subspaces $T_1, \dots, T_t$ of $\mathbb{Q}^n$ such that the set of solutions of (4.4) is contained in $T_1 \cup \cdots \cup T_t$.

There is a further generalization of this result, which we shall not state, dealing with systems of inequalities to be solved in vectors consisting of integers from a given algebraic number field. This generalization has a wide range of applications, such as finiteness results for Diophantine equations of the type considered in the previous sections, finiteness results for all sorts of Diophantine inequalities, transcendence results, finiteness results for integral points on surfaces, etc.

As an illustration, we consider the equation

$$2^{z_1} + 2^{z_2} - 11^{z_3} = 1 \tag{4.5}$$

to be solved in $z_1, z_2, z_3 \in \mathbb{Z}$. It is easy to see that (4.5) has only solutions with non-negative z_1, z_2, z_3. Notice that $(2^{z_1}, 2^{z_2}, 11^{z_3})$ is a solution of $x_1 + x_2 - x_3 = 1$ in $x_1, x_2, x_3 \in \Gamma = \{2^u 11^v : u, v \in \mathbb{Z}\}$. Hence equation (4.5) may be viewed as a special case of (2.2).
Put $x_1 = 2^{z_1}$, $x_2 = 2^{z_2}$, $x_3 = 11^{z_3}$, $\xi = \log x_1/\log x_3$, $\eta = \log x_2/\log x_3$, $\mathbf{x} = (x_1, x_2, x_3)$. Then $\|\mathbf{x}\| = x_3$ and $0 \leqslant \xi, \eta \leqslant 1$. Hence there are $k, l \in \{0, 1, 2\}$ such that $\frac{k}{3} \leqslant \xi \leqslant \frac{k+1}{3}$ and $\frac{l}{3} \leqslant \eta \leqslant \frac{l+1}{3}$. We consider those solutions with fixed values of k, l. Notice that these solutions satisfy the inequalities

$$\begin{aligned}
&|x_1 + x_2 - x_3|_\infty \leqslant \|\mathbf{x}\|^0, \quad |x_1|_\infty \leqslant \|\mathbf{x}\|^{(k+1)/3}, \quad |x_2|_\infty \leqslant \|\mathbf{x}\|^{(l+1)/3}\\
&|x_1|_2 \leqslant \|\mathbf{x}\|^{-k/3}, \quad |x_2|_2 \leqslant \|\mathbf{x}\|^{-l/3}, \quad |x_3|_2 \leqslant \|\mathbf{x}\|^0\\
&|x_1|_{11} \leqslant \|\mathbf{x}\|^0, \quad |x_2|_{11} \leqslant \|\mathbf{x}\|^0, \quad |x_3|_{11} \leqslant \|\mathbf{x}\|^{-1}.
\end{aligned}$$

This system is a special case of (4.4), and since the sum of the exponents is $-1/3 < 0$ we can apply the p-adic Subspace Theorem with $n = 3$.
Taking into consideration the possibilities for k, l, we see that $\mathbf{x} = (x_1, x_2, x_3) = (2^{z_1}, 2^{z_2}, 11^{z_3})$ is contained in the union of finitely many proper linear subspaces of $\mathbb{Q}^3$. Considering the solutions in a single subspace, we can eliminate one of the variables x_1, x_2, x_3 and obtain an equation of the same type as (4.5), but in only two variables. Applying again the p-adic Subspace Theorem but now with $n = 2$, we obtain that the solutions lie in finitely many one-dimensional subspaces, etc. Eventually we obtain that (4.5) has only finitely many solutions.

In 1989, Schmidt [26] obtained a quantitative version of his Subspace Theorem, giving an explicit upper bound for the number of subspaces t. Since then, his result has been refined and improved in several directions. In particular Schlickewei obtained quantitative versions of his p-adic Subspace Theorem which enabled him to prove weaker versions of Theorem 1 with an upper bound depending on r, n and other parameters and of Schmidt's theorem on linear recurrences with an upper bound depending on k and other parameters. Finally, Schlickewei and the author [7] managed to prove a quantitative version of the p-adic Subspace Theorem with unknowns taken from the ring of integers of a number field which was strong enough to imply the upper bounds mentioned in the previous sections. We will not give the rather complicated statement of this result.

By using a suitable specialization argument from algebraic geometry one may reduce Theorem 1 to the case that $a_1, \dots, a_n$ and the group Γ are contained in an algebraic number field, and then subsequently one may reduce equation (2.2) to a finite number of systems (4.4) by a similar argument as above. By applying the quantitative p-adic Subspace Theorem to each of these systems and adding together the upper bounds for the number of subspaces for each system, one obtains an explicit upper bound for the number of subspaces containing the solutions of (2.2). Considering the solutions of (2.2) in one of these subspaces, then by eliminating one of the variables one obtains an equation of the shape (2.2) in $n-1$ variables to which a similar argument can be applied. By repeating this, Theorem 1 follows.
The proof of Schmidt's theorem on linear recurrence sequences has a similar structure, but there the argument is much more involved.

5. Diophantine geometry

We mention some recent developments in Diophantine geometry which are related to the results from Section 2. This section is more specialized.

We write $\mathbb{G}_m^n(\mathbb{C})$ for the multiplicative group $(\mathbb{C}^*)^n$ with coordinatewise multiplication $(x_1, \dots, x_n)(y_1, \dots, y_n) = (x_1 y_1, \dots, x_n y_n)$. The group $\mathbb{G}_m^n(\mathbb{C})$ is the group of complex points of a group variety $\mathbb{G}_m^n$, called the n-dimensional linear torus. Lang ([14, p. 220]) proposed the following conjecture:
Let A be either $\mathbb{G}_m^n$ or an abelian variety defined over $\mathbb{C}$. Let Γ be a subgroup of $A(\mathbb{C})$ of finite rank (i.e., Γ has a finitely generated subgroup Γ_0 such that Γ/Γ_0 is a torsion group). Further, let X be an algebraic subvariety of A defined over $\mathbb{C}$ and let $Z(X)$ denote the exceptional set of X, that is the union of all translates of positive dimensional algebraic subgroups of A which are contained in X. Then the intersection $(X \backslash Z(X)) \cap \Gamma$ is finite.

For instance, if $A = \mathbb{G}_m^n$ and X is a hyperplane given by $a_1 x_1 + \cdots + a_n x_n = 1$ then $X(\mathbb{C}) \cap \Gamma$ is the set of solutions of $a_1 x_1 + \cdots + a_n x_n = 1$ in $(x_1, \dots, x_n) \in \Gamma$, that is, we have an equation of type (2.2). The non-degenerate solutions of this equation (i.e., with non-vanishing subsums) are precisely the points in $(X \backslash Z(X)) \cap \Gamma$. So Lang's conjecture implies that (2.2) has only finitely many non-degenerate solutions.
Let X be a projective curve of genus $\geqslant 2$ defined over an algebraic number field K, let A be the Jacobian of X, and let $\Gamma = A(K)$. We assume that $X \subset A$. We know

that $Z(X)=\emptyset$ and that $A(K)$ is finitely generated (the Mordell-Weil Theorem). Thus Lang's conjecture implies Mordell's conjecture that $X(K)$ is finite.

In the 1980's, Laurent [15] proved Lang's conjecture in the case that $A=\mathbb{G}_m^n$. Laurent's proof was based on the p-adic Subspace Theorem. In 1983, Faltings [9] proved Mordell's conjecture. Unlike Laurent, Faltings did not use Diophantine approximation. In 1991, Vojta [29] gave a totally different proof of Mordell's conjecture based on Diophantine approximation. Then by extending Vojta's ideas to higher dimensions, Faltings [10],[11] achieved the following breakthrough, which almost settled Lang's conjecture for abelian varieties:

Let A be an abelian variety, and let X be a projective subvariety of A, both defined over an algebraic number field K. Then $(X\backslash Z(X))(K)$ is finite.

Subsequently, the proof of Lang's conjecture was completed by McQuillan [18]. We refer to the books [12], [2] for an introduction.

Very recently, Rémond proved the following remarkable quantitative version of Lang's conjecture. Rémond used Faltings' arguments, but he managed to simplify them considerably.

If $A=\mathbb{G}_m^n$ we assume that $A\subset\mathbb{P}^n$ by identifying $(x_1,\dots,x_n)\in\mathbb{G}_m^n$ with the point $(1,x_1,\dots,x_n)\in\mathbb{P}^n$. if A is an abelian variety we assume that A is contained in some projective space $\mathbb{P}^N$ and that the line sheaf $\mathcal{O}_A(1)$ is symmetric. Further we assume that A is defined over the field of algebraic numbers. In both cases, A has dimension n, X is an algebraic subvariety of A of dimension m and degree d (with respect to the embeddings chosen above) defined over the algebraic numbers, and Γ is a subgroup of $A(\overline{\mathbb{Q}})$ of finite rank r.

Theorem (Rémond). *(i) Let $A=\mathbb{G}_m^n$. Then $(X\backslash Z(X))\cap\Gamma$ has cardinality at most $(2d)^{n^2(m+1)^{4m^2}(r+1)}$ ([21]).*
(ii) Let A be an abelian variety. Then $(X\backslash Z(X))\cap\Gamma$ has cardinality at most $\big(c_A\cdot d\big)^{n^{5(m+1)^2}(r+1)}$, where c_A is an effectively computable constant depending on A ([19], [20]).

References

[1] F. Beukers, H.P. Schlickewei, *The equation $x+y=1$ in finitely generated groups*, Acta Arith. 78 (1996) 189-199.

[2] B. Edixhoven, J.-H. Evertse (eds.), *Diophantine Approximation and Abelian Varieties, Introductory Lectures*, LNM 1566, Springer Verlag, 1993.

[3] P. Erdős, C.L. Stewart, R. Tijdeman, *some Diophantine equations with many solutions*, Compos. Math. 36 (1988), 37-56.

[4] J.-H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. 75 (1984), 561-584.

[5] J.-H. Evertse, P. Moree, C.L. Stewart, R. Tijdeman, *Multivariate Diophantine equations with many solutions*, Acta Arith., to appear.

[6] J.-H. Evertse, H.P. Schlickewei, *The Absolute Subspace Theorem and linear equations with unknowns from a multiplicative group*, In: Number Theory in Progress, Proc. conf. number theory in honor of the 60th birthday of Prof. Andrzej Schinzel, K. Győry, H. Iwaniec, J. Urbanowicz (eds.), 121-142. Walter de Gruyter, 1999.

[7] J.-H. Evertse, H.P. Schlickewei, *A quantitative version of the Absolute Subspace Theorem*, J. reine angew. Math. 548 (2002), 21-127.

[8] J.-H. Evertse, H.P. Schlickewei, W.M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. Math. 155 (2002), 1-30.

[9] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349-366.

[10] G. Faltings, *Diophantine approximation on abelian varieties*, Ann. Math. 133 (1991), 549-576.

[11] G. Faltings, *The general case of S. Lang's conjecture*, in: Barsotti symposium in algebraic geometry, V. Christante, W. Messing (eds.), pp. 175-182. Perspectives in Mathematics, vol. 15, Academic press, 1994.

[12] M. Hindry, J.H. Silverman, *Diophantine Geometry, An Introduction*, Springer Verlag 2000.

[13] S. Lang, *Integral points on curves*, Pub. Math. IHES, 1960.

[14] S. Lang, *Fundamentals of Diophantine Geometry*, Springer Verlag, 1983.

[15] M. Laurent, *Equations diophantiènnes exponentielles*, Invent. Math. 78 (1984), 299-327.

[16] C. Lech, *A note on recurring series*, Ark. Math. 2 (1953), 417-421.

[17] K. Mahler, *Zur Approximation algebraischer Zahlen, I. (Über den grössten Primteiler binärer Formen)*, Math. Ann. 107 (1933), 691-730.

[18] M. McQuillan, *Division points on semi-abelian varieties*, Invent. Math. 120 (1995), 143-159.

[19] G. Rémond, *Inegalité de Vojta en dimension supérieure*, Ann. Scuola Norm. Sup. Pisa, Ser. IV 29(2000), 101-151.

[20] G. Rémond, *Décompte dans une conjecture de Lang*, Invent. Math. 142 (2000), 513-545.

[21] G. Rémond, *Sur les sous-variétés des tores*, Compos. Math. 134 (2002), 337-366.

[22] K.F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), 1-20.

[23] H.P. Schlickewei, *The $\wp$-adic Thue-Siegel-Roth-Schmidt theorem*, Arch. Math. 29 (1977), 267-270.

[24] H.P. Schlickewei, *S-unit equations over number fields*, Invent. math. 102 (1990), 95-107.

[25] W.M. Schmidt, *Diophantine Approximation*, LNM 785, Springer Verlag 1980.

[26] W.M. Schmidt, *The Subspace Theorem in Diophantine approximations*, Compos. Math. 69 (1989), 121-173.

[27] W.M. Schmidt, *The zero multiplicity of linear recurrence sequences*, Acta Math. 182 (1999), 243-282.

[28] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. reine angew. Math. 135 (1909), 284-305.

[29] P.A. Vojta, *Siegel's theorem in the compact case*, Ann. Math. 133 (1991), 509-548.

[30] B.M.M. de Weger, *Algorithms for Diophantine equations*, Ph.D.-thesis, Leiden ,1988.

Universiteit Leiden, Mathematisch Instituut, Postbus 9512, NL-2300 RA Leiden
E-mail address: evertse@math.leidenuniv.nl