Hawai'i Conference in Algebraic Number Theory,
Arithmetic Geometry and Modular Forms

Some remarks on Diophantine equations and Diophantine approximation

(joint work with Claude Levesque)

Michel Waldschmidt

Université Pierre et Marie Curie (Paris 6)
Institut de Mathématiques de Jussieu

This file is available on the internet at the URL
http://www.math.jussieu.fr/∼miw/

Abstract

The main tool for solving Diophantine equations is to study Diophantine approximation. In this talk we explain the connection between the two topics, and we survey some of the related results. Among the very powerful tools is Schmidt's Subspace Theorem, which has a large variety of applications, but does not yield effective results so far.

Liouville's inequality

Liouville's inequality. *Let α be an algebraic number of degree $d \geq 2$, $P \in \mathbf{Z}[X]$ its minimal polynomial, $c = |P'(\alpha)|$ and $\epsilon > 0$. There exists q_0 such that, for any $p/q \in \mathbf{Q}$ with $q \geq q_0$,*

$$\left|\alpha - \frac{p}{q}\right| \geq \frac{1}{(c+\epsilon)q^d}.$$

Joseph Liouville, 1844

Improvements of Liouville's inequality

In the lower bound

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

for α real algebraic number of degree $d \geq 3$, the exponent d of q in the denominator of the right hand side was replaced by κ with

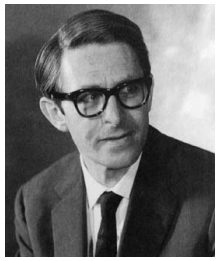
- any $\kappa > (d/2) + 1$ by A. Thue (1909),
- $2\sqrt{d}$ by C.L. Siegel in 1921,
- $\sqrt{2d}$ by F. Dyson and A.O. Gel'fond in 1947,
- any $\kappa > 2$ by K.F. Roth in 1955.

Thue–Siegel–Roth Theorem

Axel Thue (1863 - 1922)

Carl Ludwig Siegel (1896 - 1981)

Klaus Friedrich Roth (1925 –)



For any real algebraic number α, for any $\epsilon > 0$, the set of $p/q \in \mathbf{Q}$ with $|\alpha - p/q| < q^{-2-\epsilon}$ is finite.

Thue–Siegel–Roth Theorem

An equivalent statement is that, for any real algebraic number α and for any $\epsilon > 0$, there exists $q_0 > 0$ such that, for $p/q \in \mathbf{Q}$ with $q \geq q_0$, we have

$$|\alpha - p/q| > q^{-2-\epsilon}.$$

Schmidt's Subspace Theorem (1970)

For $m \geq 2$ let $L_0, \ldots, L_{m-1}$ be m independent linear forms in m variables with algebraic coefficients. Let $\epsilon > 0$. Then the set

$$\{\mathbf{x} = (x_0, \ldots, x_{m-1}) \in \mathbf{Z}^m \; ;$$

$$|L_0(\mathbf{x}) \cdots L_{m-1}(\mathbf{x})| \leq |\mathbf{x}|^{-\epsilon}\}$$

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

Wolfgang M. Schmidt

Schmidt's Subspace Theorem

For $\mathbf{x} = (x_0, \ldots, x_{m-1}) \in \mathbf{Z}^m$, define $|\mathbf{x}| = \max\{|x_0|, \ldots, |x_{m-1}|\}$.

W.M. Schmidt (1970) : *For $m \geq 2$ let $L_0, \ldots, L_{m-1}$ be m independent linear forms in m variables with algebraic coefficients. Let $\epsilon > 0$. Then the set*

$$\{\mathbf{x} = (x_0, \ldots, x_{m-1}) \in \mathbf{Z}^m \; ; \; |L_0(\mathbf{x}) \cdots L_{m-1}(\mathbf{x})| \leq |\mathbf{x}|^{-\epsilon}\}$$

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

Example : $m = 2$, $L_0(x_0, x_1) = x_0$, $L_1(x_0, x_1) = \alpha x_0 - x_1$.
Roth's Theorem : *for any real algebraic irrational number α, for any $\epsilon > 0$, the set of $p/q \in \mathbf{Q}$ with $|\alpha - p/q| < q^{-2-\epsilon}$ is finite.*

An exponential Diophantine equation

The only solutions of the equation

$$2^a + 3^b = 5^c$$

where the unknowns a, b, c are nonnegative integers are $(a, b, c) = (1, 1, 1), (2, 0, 1), (4, 2, 2)$:

$$2 + 3 = 5, \quad 4 + 1 = 5, \quad 16 + 9 = 25.$$

The more general exponential Diophantine equation

$$2^{a_1}3^{a_2} \pm 3^{b_1}5^{b_2} \pm 5^{c_1}2^{c_2} = 0$$

has only finitely many solutions in nonnegative integers $a_1, a_2, b_1, b_2, c_1, c_2$.

S–unit equations – rational case

Let $S = \{p_1, \ldots, p_s\}$ be a finite set of prime numbers. Then the equation

$$u_1 + u_2 = u_3,$$

where the unknowns u_1, u_2, u_3 are relatively prime integers divisible only by the prime numbers in S, has only finitely many solutions.

Notice that for any prime number p, the equation

$$u_1 + u_2 + u_3 = u_4$$

has infinitely many solutions in rational integers u_1, u_2, u_3 divisible only by p and $\gcd(u_1, u_2, u_3, u_4) = 1$: for instance

$$p^a + (-p^a) + 1 = 1.$$

A consequence of Schmidt's Subspace Theorem

Let $S = \{p_1, \ldots, p_s\}$ be a finite set of prime numbers. Then the equation

$$u_1 + u_2 + \cdots + u_s = 1,$$

where the unknowns $u_1, u_2, \cdots, u_s$ are rational numbers with numerators and denominators divisible only by the prime numbers in S for which no nontrivial subsum

$$\sum_{\substack{i \in I \\ \emptyset \neq I \subset \{1,\ldots,s\}}} u_i$$

vanishes, has only finitely many solutions.

Schmidt's subspace Theorem – Several places

Let $m \geq 2$ be a positive integer, S a finite set of places of $\mathbf{Q}$ containing the infinite place. For each $v \in S$ let $L_{0,v}, \ldots, L_{m-1,v}$ be m independent linear forms in m variables with algebraic coefficients in the completion of $\mathbf{Q}$ at v. Let $\epsilon > 0$. Then the set of $\mathbf{x} = (x_0, \ldots, x_{m-1}) \in \mathbf{Z}^m$ such that

$$\prod_{v \in S} |L_{0,v}(\mathbf{x}) \cdots L_{m-1,v}(\mathbf{x})|_v \leq |\mathbf{x}|^{-\epsilon}$$

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

Diophantine equations

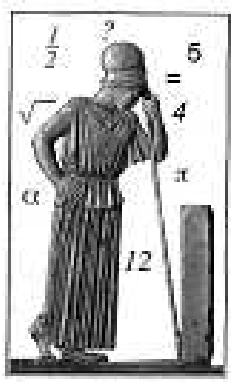
A Diophantine equation is an equation of the form

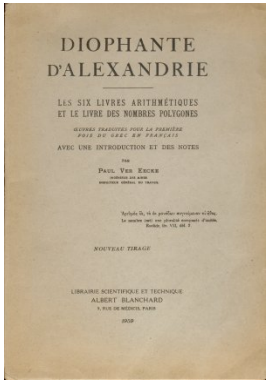
$$f(x_1, \ldots, x_n) = 0$$

where $f(X_1, \ldots, X_n) \in \mathbf{Z}[X_1, \ldots, X_n]$ is a given polynomial and the variables $X_1, \ldots, X_n$ take their values $x_1, \ldots, x_n$ in $\mathbf{Z}^n$ (integer points) or in $\mathbf{Q}^n$ (rational points).

We will mainly consider integral points.

Diophantus of Alexandria (250 ±50)





Pierre de Fermat (1601–1665)

Fermat's Last Theorem .

Historical survey

Pierre de Fermat (1601 - 1665)

Leonhard Euler (1707 - 1783)

Joseph Louis Lagrange (1736 - 1813)

XIXth Century : Hurwitz, Poincaré

Thue equation and Diophantine approximation

Liouville's estimate for the rational Diophantine approximation of $\sqrt[3]{2}$:

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{9q^3}$$

for sufficiently large q.

Mike Bennett (1997) : *for any* $p/q \in \mathbf{Q}$,

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \geq \frac{1}{4\ q^{2.5}}.$$

Mike Bennett

http://www.math.ubc.ca/∼bennett/

For any $p/q \in \mathbf{Q}$,

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \geq \frac{1}{4\ q^{2.5}}.$$

For any $(x, y) \in \mathbf{Z}^2$ *with* $x > 0$,

$$|x^3 - 2y^3| \geq \sqrt{x}.$$

Connection between Diophantine approximation and Diophantine equations

Let κ satisfy $0 < \kappa \leq 3$.
The following conditions are equivalent :
(i) There exists $c_1 > 0$ *such that*

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \geq \frac{c_1}{q^\kappa}$$

for any $p/q \in \mathbf{Q}$.
(ii) There exists $c_2 > 0$ *such that*

$$|x^3 - 2y^3| \geq c_2\ x^{3-\kappa}$$

for any $(x, y) \in \mathbf{Z}^2$ *having* $x > 0$.

Thue's equation and approximation

Let $f \in \mathbf{Z}[X]$ 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 integer $k \neq 0$, the set of $(x, y) \in \mathbf{Z}^2$ verifying

$$F(x, y) = k$$

is finite.
(ii) For any real number $\kappa > 0$ and for any root $\alpha \in \mathbf{C}$ of f, the set of rational numbers p/q verifying

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

is finite.

Thue equation

Condition (i) above :

For any integer $k \neq 0$, the set of $(x, y) \in \mathbf{Z}^2$ verifying

$$F(x, y) = k$$

is finite.

can also be phrased by stating that for any positive integer k, the set of $(x, y) \in \mathbf{Z}^2$ verifying

$$0 < |F(x, y)| \leq k$$

is finite.

Number fields, ring of integers

We denote by

- K a *number field*,
- by $\mathbf{Z}_K$ the *ring of integers of* K
- and by $\mathbf{Z}_K^\times$ the *group of units* of $\mathbf{Z}_K$ (algebraic units in K).

Mordell's equation

- (M)

For any number field K and for any non–zero element k in K, the Mordell equation

$$Y^2 = X^3 + k$$

has but a finite number of solutions $(x, y) \in \mathbf{Z}_K \times \mathbf{Z}_K$.

Elliptic equation

- (E)

For any number field K and for any polynomial f in $K[X]$ of degree 3 with three distinct complex roots, the elliptic equation

$$Y^2 = f(X)$$

has but a finite number of solutions $(x, y) \in \mathbf{Z}_K \times \mathbf{Z}_K$.

Hyperelliptic equation

• (HE)
For any number field K and for any polynomial f in $K[X]$ with at least three simple complex roots, the hyperelliptic equation

$$Y^2 = f(X)$$

has but a finite number of solutions $(x, y) \in \mathbf{Z}_K \times \mathbf{Z}_K$.

Superelliptic equation

• (SE)
For any number field K, for any integer $m \geq 3$ and for any polynomial f in $K[X]$ with at least two distinct complex roots whose orders of multiplicity are prime to m, the superelliptic equation

$$Y^m = f(X)$$

has but a finite number of solutions $(x, y) \in \mathbf{Z}_K \times \mathbf{Z}_K$.

Thue's equation

• (T)
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 $\mathrm{Card}\{\alpha_1, \ldots, \alpha_n\} \geq 3$, the Thue equation

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

has but a finite number of solutions $(x, y) \in \mathbf{Z}_K \times \mathbf{Z}_K$.

Siegel's unit equation

• (S)
For any number field K and for any elements a_1 and a_2 in K with $a_1 a_2 \neq 0$, the Siegel equation

$$a_1 E_1 + a_2 E_2 = 1$$

has but a finite number of solutions $(\varepsilon_1, \varepsilon_2) \in \mathbf{Z}_K^\times \times \mathbf{Z}_K^\times$.

Finiteness of the number of solutions

- (M) Mordell equation
$$Y^2 = X^3 + k.$$
- (E) Elliptic equation : f in $K[X]$ of degree 3
$$Y^2 = f(X).$$
- (HE) Hyperelliptic equation : f in $K[X]$ of degree ≥ 3
$$Y^2 = f(X).$$
- (SE) Superelliptic equation
$$Y^m = f(X).$$
- (T) Thue equation
$$(X - \alpha_1 Y) \cdots (X - \alpha_n Y) = k.$$
- (S) Siegel S–unit equation
$$a_1 E_1 + a_2 E_2 = 1.$$

Proof of the equivalence

$$\begin{array}{ccccc} (SE) & \Longrightarrow & (M) & \Longleftarrow & (E) \\ \Uparrow & & \Downarrow & & \Uparrow \\ (T) & \Longleftarrow & (S) & \Longrightarrow & (HE) \end{array}$$

The three implications which are not so easy to prove are

$$(T) \Longrightarrow (SE), \quad (S) \Longrightarrow (T) \quad \text{and} \quad (S) \Longrightarrow (HE).$$

Siegel's Theorem on integral points on curves

A further result which is equivalent to the six previous statements is Siegel's fundamental theorem on the finiteness of integral points on a curve of genus ≥ 1.

But the six previous statements can be made effective, while Siegel's Theorem is not yet effective, even for the special case of genus 2.

Thue–Mahler equation – rational case

Back to $K = \mathbf{Q}$.

(i) For any finite set $S = \{p_1, \ldots, p_s\}$ of prime numbers, for any $k \in \mathbf{Q}^\times$ and for any binary homogeneous form $F(X, Y) \in \mathbf{Q}[X, Y]$ with the property that the polynomial $F(X, 1) \in \mathbf{Q}[X]$ has at least three linear factors involving three distinct roots in $\mathbf{Q}$, the Thue-Mahler equation

$$F(X, Y) = \pm k p_1^{Z_1} \cdots p_s^{Z_s}$$

has only finitely many solutions $(x, y, z_1, \ldots, z_s)$ in $\mathbf{Z}^{2+s}$ with $\gcd(xy, p_1 \cdots p_s) = 1$.

Thue–Mahler - special cubic rational case

(ii) For any finite set $S = \{p_1, \dots, p_s\}$ of prime numbers, the Thue-Mahler equation

$$XY(X - Y) = \pm k p_1^{Z_1} \cdots p_s^{Z_s}$$

has but a finite number of solutions $(x, y, z_1, \dots, z_s)$ in $\mathbf{Z}^{2+s}$ with $\gcd(xy, p_1 \cdots p_s) = 1$.

S–integers - rational case

(iii) For any finite set $S = \{p_1, \dots, p_s\}$ of prime numbers, the S–unit equation

$$E_1 + E_2 = 1$$

has but a finite number of solutions $(\varepsilon_1, \varepsilon_2)$ in $(S^{-1}\mathbf{Z})^\times \times (S^{-1}\mathbf{Z})^\times$.

$$(S^{-1}\mathbf{Z})^\times := \left\{ \pm p_1^{a_1} \cdots p_s^{a_s} \mid a_1, \dots, a_s \in \mathbf{Z} \right\} \subset \mathbf{Q}^\times \qquad (S\text{–units}),$$

$$S^{-1}\mathbf{Z} := \left\{ a/b \mid a \in \mathbf{Z},\ b \in (S^{-1}\mathbf{Z})^\times \right\} \subset \mathbf{Q} \qquad (S\text{–integers}).$$

Siegel's S–unit equation - rational case

(iv) For any finite set $S = \{p_1, \dots, p_s\}$ of prime numbers, every set of S–integral points of $\mathbf{P}^1(\mathbf{Q})$ minus three points is finite.

S–integers – rational case

Finiteness of the set of integral points .
(i) Thue-Mahler equation over $\mathbf{Z}^{2+s}$

$$F(X, Y) = \pm k p_1^{Z_1} \cdots p_s^{Z_s}.$$

(ii) Thue-Mahler equation over $\mathbf{Z}^{2+s}$

$$XY(X - Y) = \pm k p_1^{Z_1} \cdots p_s^{Z_s}.$$

(iii) Siegel's S–unit equation over $((S^{-1}\mathbf{Z})^\times)^2$

$$E_1 + E_2 = 1.$$

(iv) S–integral points of $\mathbf{P}^1(\mathbf{Q}) \setminus \{0, 1, \infty\}$.

S–integers - number fields

We will consider an algebraic number field K and a finite set S of places of K containing all the archimedean places. Moreover F will denote a binary homogeneous form with coefficients in K. We will consider the Thue–Mahler equations $F(X, Y) = E$ where the two unknowns X, Y take respectively values x, y in a given set $\mathcal{O}_S$ of S–integers of K while the unknown E takes its values ε in the set $\mathcal{O}_S^\times$ of S–units of K. If (x, y, ε) is a solution and if m denotes the degree of F, then, for all $\eta \in \mathcal{O}_S^\times$, the triple $(\eta x, \eta y, \eta^m \varepsilon)$ is also a solution.

Definition. Two solutions (x, y, ε) and (x', y', ε') in $\mathcal{O}_S^2 \times \mathcal{O}_S^\times$ of the equation $F(X, Y) = E$ are said to be *equivalent modulo* $\mathcal{O}_S^\times$ if the points of $\mathbf{P}^1(K)$ with projective coordinates $(x : y)$ and $(x' : y')$ are the same.

Thue–Mahler equation – general form

Let K be an algebraic number field.

The following four assertions are equivalent.
(i) For any finite set S of places of K containing all the archimedean places, for every $k \in K^\times$ and for any binary homogeneous form $F(X, Y)$ with the property that the polynomial $F(X, 1) \in K[X]$ has at least three linear factors involving three distinct roots in K, the Thue-Mahler equation

$$F(X, Y) = kE$$

has but a finite number of classes of solutions $(x, y, \varepsilon) \in \mathcal{O}_S^2 \times \mathcal{O}_S^\times$.

Thue–Mahler equation – special cubic form

(ii) For any finite set S of places of K containing all the archimedean places, the Thue-Mahler equation

$$XY(X - Y) = E$$

has but a finite number of classes of solutions $(x, y, \varepsilon) \in \mathcal{O}_S^2 \times \mathcal{O}_S^\times$.

Siegel S–unit equation

(iii) For any finite set S of places of K containing all the archimedean places, the S–unit equation

$$E_1 + E_2 = 1$$

has but a finite number of solutions $(\varepsilon_1, \varepsilon_2)$ in $\mathcal{O}_S^\times \times \mathcal{O}_S^\times$.

Vojta

(iv) For any finite set S of places of K containing all the archimedean places, every set of S–integral points of $\mathbf{P}^1(K)$ minus three points is finite.

Thue, Mahler, Siegel, Vojta

Let K be an algebraic number field. Finiteness of the set of integral points .

(i) Thue–Mahler equation over $\mathcal{O}_S^2 \times \mathcal{O}_S^\times$:

$$F(X, Y) = kE.$$

(ii) Thue-Mahler equation over $\mathcal{O}_S^2 \times \mathcal{O}_S^\times$:

$$XY(X - Y) = E.$$

(iii) Siegel's S–unit equation over $(\mathcal{O}_S^\times)^2$:

$$E_1 + E_2 = 1.$$

(iv) S–integral points on $\mathbf{P}^1(K) \setminus \{0, 1, \infty\}$.

Generalized Siegel unit equation and integral points

Let K be a number field. The following two assertions are equivalent.

(i) Let $n \geq 1$ be an integer and let S a finite set of places of K including the archimedean places. Then the equation

$$E_0 + \cdots + E_n = 0$$

has only finitely many classes modulo $\mathcal{O}_S^\times$ of solutions $(\varepsilon_0, \ldots, \varepsilon_n) \in (\mathcal{O}_S^\times)^{n+1}$ for which no proper subsum $\sum_{i \in I} \varepsilon_i$ vanishes, with I being a subset of $\{0, \ldots, n\}$, with at least two elements and at most n.

(ii) Let $n \geq 1$ be an integer and let S a finite set of places of K including the archimedean places. Then for any set of $n + 2$ distinct hyperplanes $H_0, \ldots, H_{n+1}$ in $\mathbf{P}^n(K)$, the set of S–integral points of $\mathbf{P}^n(K) \setminus (H_0 \cup \cdots \cup H_{n+1})$ is contained in a finite union of hyperplanes of $\mathbf{P}^n(K)$.

Reference

Claude Levesque and Michel Waldschmidt
Some remarks on diophantine equations and diophantine approximation ;
Vietnam Journal of Mathematics 39 :3 (2011) 343–368.

The PDF file is made freely available by the editors until the end of 2012
`http://www.math.ac.vn/publications/vjm/VJM_39/toc_39_3.htm`

Hawai'i Conference in Algebraic Number Theory,
Arithmetic Geometry and Modular Forms

Some remarks on Diophantine equations and Diophantine approximation

(joint work with Claude Levesque)

Michel Waldschmidt

Université Pierre et Marie Curie (Paris 6)
Institut de Mathématiques de Jussieu

This file is available on the internet at the URL
http://www.math.jussieu.fr/∼miw/