February 13, 2012

Diophantine approximation and Diophantine equations: an introduction.

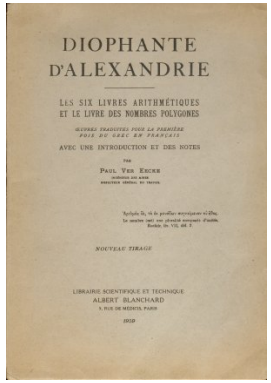
Michel Waldschmidt

Université Pierre et Marie Curie (Paris 6)
Institut de Mathématiques de Jussieu
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 meaning of these words, the connection between the two topics, and we survey some of the main results and some of the main conjectures. 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.

Diophantus of Alexandria (250 ±50)



Rational approximation

The rational numbers are dense in the real numbers :
For any x in $\mathbf{R}$ and any $\epsilon > 0$, there exists $p/q \in \mathbf{Q}$ such that

$$\left| x - \frac{p}{q} \right| < \epsilon.$$

Numerical approximation : starting from the rational numbers, compute the maximal number of digits of x with the minimum of operations.

Rational approximation : given x and ϵ, find p/q with q minimal such that $|x - p/q| < \epsilon$.

Rational approximation to real numbers

Easy : for any $x \in \mathbf{Q}$ and any $q \geq 1$, there exists $p \in \mathbf{Z}$ with $|qx - p| \leq 1/2$.
Solution : take for p the nearest integer to qx.

This inequality

$$\left| x - \frac{p}{q} \right| < \frac{1}{2q}$$

is best possible when qx is half an integer. We want to investigate stronger estimates : hence we need to exclude rational numbers.

Rational approximation to rational numbers

A rational number has an excellent rational approximation : itself !
But there is no other good approximation : if x is rational, there exists a constant $c = c(x) > 0$ such that, for any $p/q \in \mathbf{Q}$ with $p/q \neq x$,

$$\left| x - \frac{p}{q} \right| \geq \frac{c}{q}.$$

Proof : Write $x = a/b$ and set $c = 1/b$: since $aq - bp$ is a nonzero integer, it has absolute value at least 1, and

$$\left| x - \frac{p}{q} \right| = \frac{|aq - bp|}{bq} \geq \frac{1}{bq}$$

Criterion for irrationality

Consequence. *Let $\vartheta \in \mathbf{R}$. Assume that for any $\epsilon > 0$, there exists $p/q \in \mathbf{Q}$ with*

$$0 < |q\vartheta - p| < \epsilon.$$

Then ϑ is irrational.

Rational approximation to irrational real numbers

Any irrational real number x has much better rational approximations than those of order $1/q$, namely there exist approximations of order $1/q^2$ (hence p will always be the nearest integer to qx).

For any $x \in \mathbf{R} \setminus \mathbf{Q}$, there exists infinitely many p/q with

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{q^2}.$$

Pigeonhole Principle

More holes than pigeons

More pigeons than holes

Gustave Lejeune–Dirichlet (1805–1859)

G. Dirichlet

1842 : Box (pigeonhole) principle
A map $f : E \to F$ with $\mathrm{Card}E > \mathrm{Card}F$ is not injective.
A map $f : E \to F$ with $\mathrm{Card}E < \mathrm{Card}F$ is not surjective.

Existence of rational approximations

For any $\vartheta \in \mathbf{R}$ and any real number $Q > 1$, there exists $p/q \in \mathbf{Q}$ with

$$|q\vartheta - p| \leq \frac{1}{Q}$$

and $0 < q < Q$.

Proof. For simplicity assume $Q \in \mathbf{Z}$. Take

$$E = \{0, \{\vartheta\}, \{2\vartheta\}, \ldots, \{(Q-1)\vartheta\}, 1\} \subset [0,1],$$

where $\{x\}$ denotes the fractional part of x and let F be the partition

$$\left[0, \frac{1}{Q}\right), \left[\frac{1}{Q}, \frac{2}{Q}\right), \ldots, \left[\frac{Q-2}{Q}, \frac{Q-1}{Q}\right), \left[\frac{Q-1}{Q}, 1\right],$$

of $[0,1]$, so that

$$\mathrm{Card}E = Q + 1 > Q = \mathrm{Card}F,$$

and $f : E \to F$ maps $x \in E$ to $I \in F$ with $I \ni x$.

Hermann Minkowski (1864-1909)

H. Minkowski

1896 : Geometry of numbers.
Let $\vartheta \in \mathbf{R}$. The set
$\mathcal{C} = \{(u,v) \in \mathbf{R}^2 ; |v| \leq Q, |v\vartheta - u| \leq 1/Q\}$
is convex, symmetric, compact, with volume 4.
Hence $\mathcal{C} \cap \mathbf{Z}^2 \neq \{(0,0)\}$.

Adolf Hurwitz (1859–1919)

A. Hurwitz

1891
For any $\vartheta \in \mathbf{R} \setminus \mathbf{Q}$, there exists a sequence $(p_n/q_n)_{n\geq 0}$ of rational numbers with

$$0 < |q_n\vartheta - p_n| < \frac{1}{\sqrt{5}q_n}$$

and $q_n \to \infty$.
Methods : Continued fractions, Farey sections.

Best possible for the Golden ratio

$$\frac{1+\sqrt{5}}{2} = 1.618\,033\,988\,749\,9\ldots$$

Irrationality criterion

Let ϑ be a real number. The following conditions are equivalent.
(i) ϑ *is irrational.*
(ii) For any $\epsilon > 0$, there exists $p/q \in \mathbf{Q}$ such that

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{\epsilon}{q}.$$

(iii) For any real number $Q > 1$, there exists an integer q in the interval $1 \leq q < Q$ and there exists an integer p such that

$$0 < \left|\vartheta - \frac{p}{q}\right| < \frac{1}{qQ}.$$

(iv) There exist infinitely many $p/q \in \mathbf{Q}$ satisfying

$$\left|\vartheta - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}.$$

Criteria for linear and algebraic independence

Linear independence :
Yu.V. Nesterenko, S. Fischler and W. Zudilin, A. Chantanasiri.

Algebraic independence : A.O. Gel'fond, G.V. Chudnovski, P. Philippon, Yu.V. Nesterenko.

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

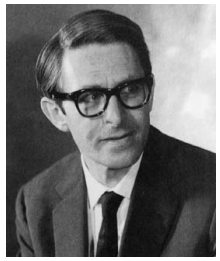
- any $\kappa > (d/2) + 1$ by A. Thue (1909),
- $2\sqrt{d}$ by C.L. Siegel in 1921,
- $\sqrt{2d}$ by Dyson and Gel'fond in 1947,
- any $\kappa > 2$ by K.F. Roth in 1955.

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)

W.M. Schmidt

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 $\mathbf{Q}^m$.

Schmidt's Subspace Theorem

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 $(a, b, c) = (1, 1, 1), (2, 0, 1), (4, 2, 2)$:

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

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.

Diophantine equations

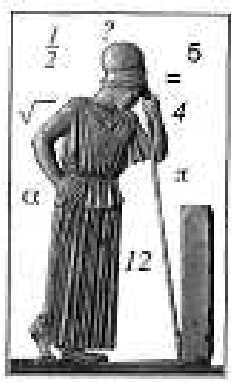
A Diophantine equation is an equation of the form

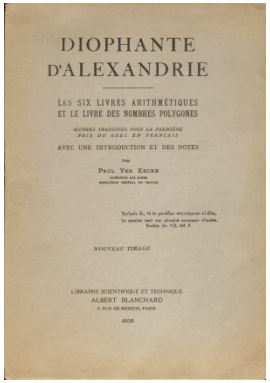
$$f(x_1, \ldots, x_n) = 0$$

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) 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 (subfield of $\mathbf{C}$ which is a finite dimensional vector space over $\mathbf{Q}$ – equivalently $K = \mathbf{Q}(\alpha)$ where α is an algebraic number), by $\mathbf{Z}_K$ the ring of integers of K (elements of K having an irreducible monic polynomial with integer coefficients).

For instance when $K = \mathbf{Q}(i)$ we have $\mathbf{Z}_K = \mathbf{Z}[i]$.

More generally for $K = \mathbf{Q}(\zeta)$ where ζ is a root of unity we have $\mathbf{Z}_K = \mathbf{Z}[\zeta]$.

But for $\Phi = (1 + \sqrt{5})/2$, the field $K = \mathbf{Q}(\Phi)$ is the same as $\mathbf{Q}(\sqrt{5})$ and we have $\mathbf{Z}_K = \mathbf{Z}[\Phi]$.

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

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

S–integers - rational case

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

$$E_1 + E_2 = 1$$

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

Siegel's S–unit equation - rational case

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

S–integers - rational case

The following four assertions are equivalent :
(i) Thue-Mahler equation

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

(ii) Thue-Mahler equation

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

(iii) Siegel's S–unit equation

$$E_1 + E_2 = 1.$$

(iv) Finitely many 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 of S–integers of K while the unknown E takes its values ε in the set 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, Volta

Let K be an algebraic number field. The following four assertions are equivalent :
(i) Thue–Mahler equation :

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

(ii) Thue-Mahler equation

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

(iii) Siegel's S–unit equation

$$E_1 + E_2 = 1$$

(iv) Finitely many 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`

Hilbert's 8th Problem

August 8, 1900

Second International Congress of Mathematicians in Paris.

David Hilbert (1862 - 1943)

Twin primes,

Goldbach's Conjecture,

Riemann Hypothesis

Hilbert's tenth problem

D. Hilbert (1900) — *Problem :* to give an algorithm in order to decide whether a diophantine equation has an integer solution or not.

If we do not succeed in solving a mathematical problem, the reason frequently consists in our failure to recognize the more general standpoint from which the problem before us appears only as a single link in a chain of related problems. After finding this standpoint, not only is this problem frequently more accessible to our investigation, but at the same time we come into possession of a method which is applicable also to related problems.

Negative solution to Hilbert's tenth problem

J. Robinson (1952)

J. Robinson, M. Davis, H. Putnam (1961)

Yu. Matijasevic (1970) – Fibonacci sequence

$$1,\ 1,\ 2,\ 3,\ 5,\ 8,\ 13,\ 21,\ 34,\ 55,\ 89,\ 144\ldots$$

$$F_1 = 1, \quad F_2 = 1, \quad F_n = F_{n-1} + F_{n-2}.$$

The relation $b = F_a$ between two integers a and b is *a diophantine relation with exponential growth.*

Remark : the analog for rational points of Hilbert's tenth problem is not yet solved :
to give an algorithm in order to decide whether a diophantine equation has a rational solution or not.

Historical survey

Thue (1908) : finitely many integer solutions of

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

when F is homogeneous irreducible over $\mathbf{Q}$ of degree ≥ 3.

Mordell's Conjecture (1922) : rational points

Siegel's Theorem (1929) : integral points

Faltings' Theorem(1983) : finiteness of rational points on an algebraic curve of genus ≥ 2 over a number field.

Andrew Wiles (1993) : proof of Fermat's last Theorem

$$a^n + b^n = c^n \qquad (n \geq 3)$$

G. Rémond (2000) : explicit upper bound for the number of solutions in Faltings' Theorem.

Rational points on varieties

When f is a polynomial in n variables with coefficients in a field k, solving the equation $f(x_1, \ldots, x_n) = 0$ in k^n is finding the rational points over k on the affine hypersurface $Z(f)$ in k^n.

Let k be a number field (a finite extension of $\mathbf{Q}$, that is a finite $\mathbf{Q}$-vector space) and V an algebraic variety over k. Diophantine geometry investigates the following questions :

- Is $V(k)$ empty ?
- Is $V(k)$ infinite ? or Zariski dense in V ?
- Is $V(k)$ dense in $V(\mathbf{C})$?

Serge Lang (1927–2005)

Serge Lang Number Theory III, Diophantine Geometry, Russian encyclopaedia of Springer Verlag, 1991. (=Survey of Diophantine Geometry, 1997) :

Thus we behold the grand unification of algebraic geometry, analysis and PDE, Diophantine approximation, Nevanlinna theory and classical Diophantine problems about rational and integral points.

Chulalongkorn University Faculty of Science
Department of Mathematics and Computer Science

Diophantine approximation and Diophantine equations an introduction

Michel Waldschmidt

February 13, 2012

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

February 13, 2012

Diophantine approximation and Diophantine equations: an introduction.

Michel Waldschmidt

Université Pierre et Marie Curie (Paris 6)
Institut de Mathématiques de Jussieu
http://www.math.jussieu.fr/~miw/