COMSATS IIT, Lahore Campus March 12, 2013

Diophantine approximation and Diophantine equations : old and new

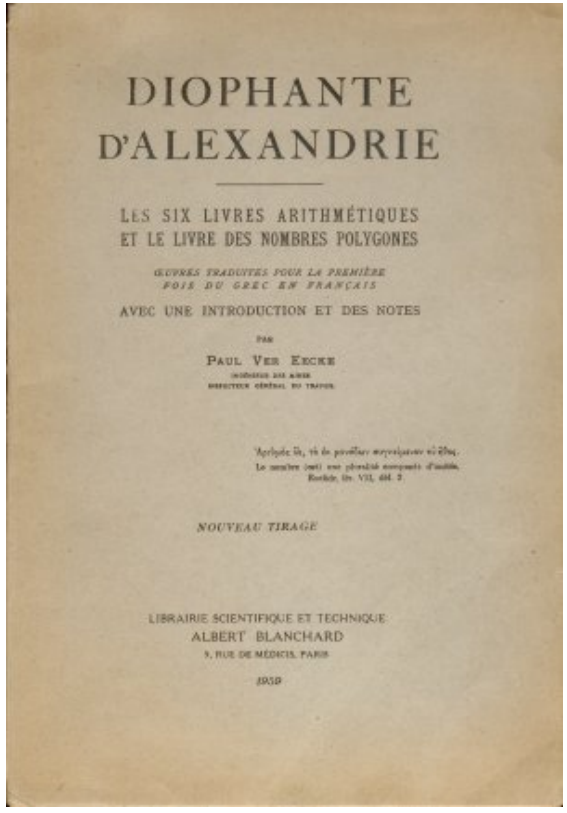
Michel Waldschmidt

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 meaning of these words, the connection between the two topics, and we survey some of the main results and some of the main conjectures.

Diophantus of Alexandria (250 $\pm$50)


DIOPHANTE
D'ALEXANDRIE

LES SIX LIVRES ARITHMÉTIQUES
ET LE LIVRE DES NOMBRES POLYGONES

OEUVRES TRADUITES POUR LA PREMIÈRE FOIS DU GREC EN FRANÇAIS

AVEC UNE INTRODUCTION ET DES NOTES

PAR

PAUL VER ECKE

NOUVEAU TIRAGE

LIBRAIRIE SCIENTIFIQUE ET TECHNIQUE
ALBERT BLANCHARD

Rational approximation

The set of rational numbers is dense in the set of 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

The set of rational numbers is dense in the set of 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

The set of rational numbers is dense in the set of 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 $|x - p/q| < \epsilon$.

History of rational approximation theory

Diophantine approximation is the study of the approximation of a real or complex number by rational or algebraic numbers.

It has its early sources in astronomy, with the study of movement of the celestials bodies, and in the computations of π.

History of rational approximation theory

Diophantine approximation is the study of the approximation of a real or complex number by rational or algebraic numbers.

It has its early sources in astronomy, with the study of movement of the celestials bodies, and in the computations of π.

Computation of π

Rhind Papyrus : $2^5/3^4 = 3.1604\ldots$

Baudhāyana (Sulvasūtras) : $3,088$

Suryaprajnapati (Jaina mathematician) : $\sqrt{10} = 3.162\ldots$

Archimedes : 3.1418

Chan Hong Wang Fan, Liu Hui, Zu Chongzhi (Tsu Ch'ung-Chih) : $355/113 = 3.1415929\ldots$

Aryabhaṭīya, Āryabhaṭa I : $3,1416$ (suggests $\pi \notin \mathbf{Q}$)

Bhāskara I : suggests a negative solution to the problem of squaring the circle.

Bhāskarācārya (Bhāskara II) : $3927/1250 = 3,1416\ldots$

Madhava (1380–1420) : series, 11 exact decimals 3.14159265359 (Viète 1579 : 9 decimals only).

Computation of π

Rhind Papyrus : $2^5/3^4 = 3.1604\ldots$

Baudhāyana (Sulvasūtras) : $3,088$

Suryaprajnapati (Jaina mathematician) : $\sqrt{10} = 3.162\ldots$

Archimedes : 3.1418

Chan Hong Wang Fan, Liu Hui, Zu Chongzhi (Tsu Ch'ung-Chih) : $355/113 = 3.1415929\ldots$

Aryabhaṭīya, Āryabhaṭa I : $3,1416$ (suggests $\pi \notin \mathbf{Q}$)

Bhāskara I : suggests a negative solution to the problem of squaring the circle.

Bhāskarācārya (Bhāskara II) : $3927/1250 = 3,1416\ldots$

Madhava (1380–1420) : series, 11 exact decimals 3.14159265359 (Viète 1579 : 9 decimals only).

Computation of π

Rhind Papyrus : $2^5/3^4 = 3.1604\ldots$

Baudhāyana (Sulvasūtras) : $3,088$

Suryaprajnapati (Jaina mathematician) : $\sqrt{10} = 3.162\ldots$

Archimedes : 3.1418

Chan Hong Wang Fan, Liu Hui, Zu Chongzhi (Tsu Ch'ung-Chih) : $355/113 = 3.1415929\ldots$

Aryabhaṭīya, Āryabhaṭa I : $3,1416$ (suggests $\pi \notin \mathbf{Q}$)

Bhāskara I : suggests a negative solution to the problem of squaring the circle.

Bhāskarācārya (Bhāskara II) : $3927/1250 = 3,1416\ldots$

Madhava (1380–1420) : series, 11 exact decimals 3.14159265359 (Viète 1579 : 9 decimals only).

Computation of π

Rhind Papyrus : $2^5/3^4 = 3.1604\ldots$

Baudhāyana (Sulvasūtras) : $3,088$

Suryaprajnapati (Jaina mathematician) : $\sqrt{10} = 3.162\ldots$

Archimedes : 3.1418

Chan Hong Wang Fan, Liu Hui, Zu Chongzhi (Tsu Ch'ung-Chih) : $355/113 = 3.1415929\ldots$

Aryabhaṭīya, Āryabhaṭa I : $3,1416$ (suggests $\pi \notin \mathbf{Q}$)

Bhāskara I : suggests a negative solution to the problem of squaring the circle.

Bhāskarācārya (Bhāskara II) : $3927/1250 = 3,1416\ldots$

Madhava (1380–1420) : series, 11 exact decimals 3.14159265359 (Viète 1579 : 9 decimals only).

Computation of π

Rhind Papyrus : $2^5/3^4 = 3.1604\ldots$

Baudhāyana (Sulvasūtras) : $3,088$

Suryaprajnapati (Jaina mathematician) : $\sqrt{10} = 3.162\ldots$

Archimedes : 3.1418

Chan Hong Wang Fan, Liu Hui, Zu Chongzhi (Tsu Ch'ung-Chih) : $355/113 = 3.1415929\ldots$

Aryabhaṭīya, Āryabhaṭa I : $3,1416$ (suggests $\pi \notin \mathbf{Q}$)

Bhāskara I : suggests a negative solution to the problem of squaring the circle.

Bhāskarācārya (Bhāskara II) : $3927/1250 = 3,1416\ldots$

Madhava (1380–1420) : series, 11 exact decimals 3.14159265359 (Viète 1579 : 9 decimals only).

Computation of π

Rhind Papyrus : $2^5/3^4 = 3.1604\ldots$

Baudhāyana (Sulvasūtras) : $3,088$

Suryaprajnapati (Jaina mathematician) : $\sqrt{10} = 3.162\ldots$

Archimedes : 3.1418

Chan Hong Wang Fan, Liu Hui, Zu Chongzhi (Tsu Ch'ung-Chih) : $355/113 = 3.1415929\ldots$

Aryabhaṭīya, Āryabhaṭa I : $3,1416$ (suggests $\pi \notin \mathbf{Q}$)

Bhāskara I : suggests a negative solution to the problem of squaring the circle.

Bhāskarācārya (Bhāskara II) : $3927/1250 = 3,1416\ldots$

Madhava (1380–1420) : series, 11 exact decimals 3.14159265359 (Viète 1579 : 9 decimals only).

Computation of π

Rhind Papyrus : $2^5/3^4 = 3.1604\ldots$

Baudhāyana (Sulvasūtras) : $3,088$

Suryaprajnapati (Jaina mathematician) : $\sqrt{10} = 3.162\ldots$

Archimedes : 3.1418

Chan Hong Wang Fan, Liu Hui, Zu Chongzhi (Tsu Ch'ung-Chih) : $355/113 = 3.1415929\ldots$

Aryabhaṭīya, Āryabhaṭa I : $3,1416$ (suggests $\pi \notin \mathbf{Q}$)

Bhāskara I : suggests a negative solution to the problem of squaring the circle.

Bhāskarācārya (Bhāskara II) : $3927/1250 = 3,1416\ldots$

Madhava (1380–1420) : series, 11 exact decimals 3.14159265359 (Viète 1579 : 9 decimals only).

Computation of π

Rhind Papyrus : $2^5/3^4 = 3.1604\ldots$

Baudhāyana (Sulvasūtras) : $3,088$

Suryaprajnapati (Jaina mathematician) : $\sqrt{10} = 3.162\ldots$

Archimedes : 3.1418

Chan Hong Wang Fan, Liu Hui, Zu Chongzhi (Tsu Ch'ung-Chih) : $355/113 = 3.1415929\ldots$

Aryabhaṭīya, Āryabhaṭa I : $3,1416$ (suggests $\pi \notin \mathbf{Q}$)

Bhāskara I : suggests a negative solution to the problem of squaring the circle.

Bhāskarācārya (Bhāskara II) : $3927/1250 = 3,1416\ldots$

Madhava (1380–1420) : series, 11 exact decimals 3.14159265359 (Viète 1579 : 9 decimals only).

Computation of π

Rhind Papyrus : $2^5/3^4 = 3.1604\ldots$

Baudhāyana (Sulvasūtras) : $3,088$

Suryaprajnapati (Jaina mathematician) : $\sqrt{10} = 3.162\ldots$

Archimedes : 3.1418

Chan Hong Wang Fan, Liu Hui, Zu Chongzhi (Tsu Ch'ung-Chih) : $355/113 = 3.1415929\ldots$

Aryabhaṭīya, Āryabhaṭa I : $3,1416$ (suggests $\pi \notin \mathbf{Q}$)

Bhāskara I : suggests a negative solution to the problem of squaring the circle.

Bhāskarācārya (Bhāskara II) : $3927/1250 = 3,1416\ldots$

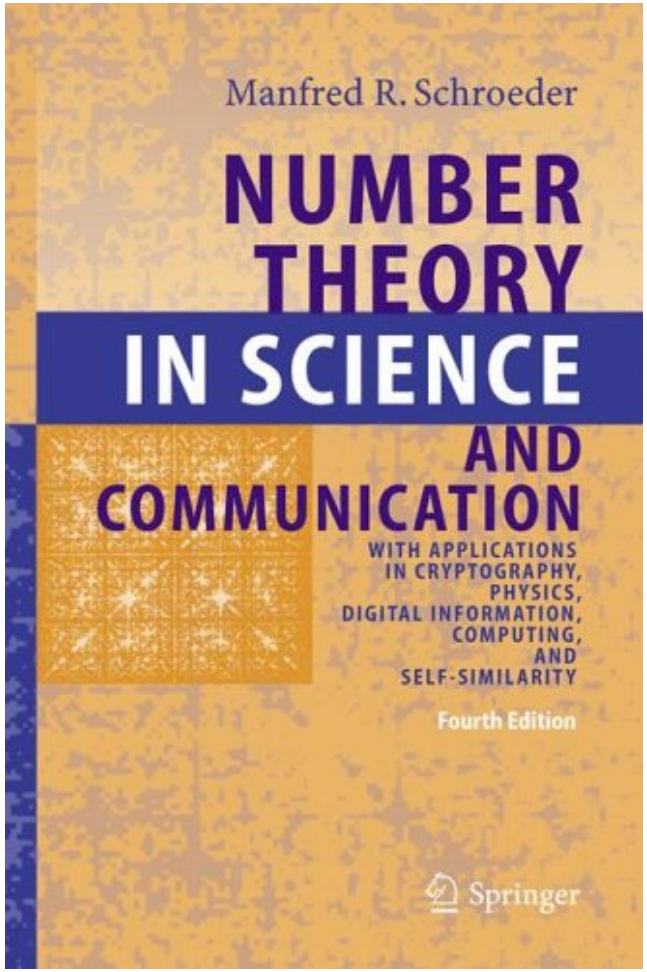
Madhava (1380–1420) : series, 11 exact decimals 3.14159265359 (Viète 1579 : 9 decimals only).

Diophantine approximation in the real life

Small divisors and dynamical systems (H. Poincaré)
Periods of Saturn orbits (Cassini divisions)
Stability of the solar system
Resonance in astronomy
Engrenages
Quasi-cristals
Acoustic of concert halls
Calendars : bissextile years

Number Theory in Science and communication

M.R. Schroeder.
Number theory in science and communication :
with applications in cryptography, physics, digital information, computing and self similarity
Springer series in information sciences **7** 1986.
4th ed. (2006) 367 p.



Further applications of Diophantine Approximation

Hua Loo Keng, Wang Yuan

Application of number theory to numerical analysis

Springer Verlag 1981

Equidistribution modulo 1, discrepancy, numerical integration, interpolation, approximate solutions to integral and differential equations.

Special case of Hermite–Lindemann Theorem

If a and b are positive rational numbers, then $e^b \neq a$.

Hermite (1873)

Lindemann (1882)

Mahler's problem (1967)

For a and b positive integers,

$$|e^b - a| > a^{-c}?$$

Stronger conjecture :

$$|e^b - a| > b^{-c}?$$

Mahler's problem (1967)

K. Mahler (1953, 1967), M. Mignotte (1974), F. Wielonsky (1997) :

$$|e^b - a| > b^{-20b}$$

Joint work with Yu.V. Nesterenko (1996) for a and b rational numbers, refinement by S. Khemira (2005).

Define $H(p/q) = \max\{|p|,\ q\}$. Then for a and b in $\mathbf{Q}$ with $b \neq 0$,

$$|e^b - a| \geq \exp\{-1,3 \cdot 10^5 (\log A)(\log B)\}$$

where $A = \max\{H(a),\ A_0\}$, $B = \max\{H(b),\ 2\}$.

Mahler's problem (1967)

K. Mahler (1953, 1967), M. Mignotte (1974), F. Wielonsky (1997) :

$$|e^b - a| > b^{-20b}$$

Joint work with Yu.V. Nesterenko (1996) for a and b rational numbers, refinement by S. Khemira (2005).

Define $H(p/q) = \max\{|p|,\ q\}$. Then for a and b in $\mathbf{Q}$ with $b \neq 0$,

$$|e^b - a| \geq \exp\{-1,3 \cdot 10^5 (\log A)(\log B)\}$$

where $A = \max\{H(a),\ A_0\}$, $B = \max\{H(b),\ 2\}$.

Mahler's problem (1967)

K. Mahler (1953, 1967), M. Mignotte (1974), F. Wielonsky (1997) :

$$|e^b - a| > b^{-20b}$$

Joint work with Yu.V. Nesterenko (1996) for a and b rational numbers, refinement by S. Khemira (2005).

Define $H(p/q) = \max\{|p|,\ q)$. Then for a and b in $\mathbf{Q}$ with $b \neq 0$,

$$|e^b - a| \geq \exp\{-1,3 \cdot 10^5 (\log A)(\log B)\}$$

where $A = \max\{H(a),\ A_0\}$, $B = \max\{H(b),\ 2\}$.

Exact rounding of the elementary functions

Applications in theoretical computer science :
Muller, J-M. ; Tisserand, A. –
Towards exact rounding of the elementary functions. Alefeld, Goetz (ed.) et al.,
Scientific computing and validated numerics.
Proceedings of the international symposium on scientific computing, computer arithmetic and validated numerics SCAN-95, Wuppertal, Germany, September 26-29, 1995.
Berlin : Akademie Verlag. Math. Res. 90, 59-71 (1996).

Applications in theoretical computer science

Computer Arithmetic

—

Arénaire project

http://www.ens-lyon.fr/LIP/Arenaire/

Validated scientific computing
Arithmetic. reliability, accuracy, and speed
Improvement of the available arithmetic on computers, processors, dedicated or embedded chips
Getting more accurate results or getting them more quickly
Power consumption, reliability of numerical software.

Rational Diophantine approximation

- For computing a number with a sharp accuracy, one wishes to get many decimals (or binary digits) with a small number of operations (products, say).
- For Diophantine questions, the cost is measured by the denominator q : one investigates how well ξ can be approximated in terms of q.
- A rational number has a single good approximation , itself ! Indeed *if $\xi = a/b$ is a given rational number, then for any $p/q \in \mathbf{Q}$ distinct from ξ,*

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

where $c = 1/b$. **Proof** : $|bq - ap| \geq 1$.

Rational Diophantine approximation

- For computing a number with a sharp accuracy, one wishes to get many decimals (or binary digits) with a small number of operations (products, say).
- For Diophantine questions, the cost is measured by the denominator q : one investigates how well ξ can be approximated in terms of q.
- A rational number has a single good approximation , itself ! Indeed *if $\xi = a/b$ is a given rational number, then for any $p/q \in \mathbf{Q}$ distinct from ξ,*

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

where $c = 1/b$. **Proof** : $|bq - ap| \geq 1$.

Rational Diophantine approximation

- For computing a number with a sharp accuracy, one wishes to get many decimals (or binary digits) with a small number of operations (products, say).
- For Diophantine questions, the cost is measured by the denominator q : one investigates how well ξ can be approximated in terms of q.
- A rational number has a single good approximation , itself !

Indeed *if $\xi = a/b$ is a given rational number, then for any $p/q \in \mathbf{Q}$ distinct from ξ,*

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

where $c = 1/b$. **Proof** : $|bq - ap| \geq 1$.

Rational Diophantine approximation

- For computing a number with a sharp accuracy, one wishes to get many decimals (or binary digits) with a small number of operations (products, say).
- For Diophantine questions, the cost is measured by the denominator q : one investigates how well ξ can be approximated in terms of q.
- A rational number has a single good approximation , itself !

Indeed *if $\xi = a/b$ is a given rational number, then for any $p/q \in \mathbf{Q}$ distinct from ξ,*

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

where $c = 1/b$. **Proof** : $|bq - ap| \geq 1$.

Rational Diophantine approximation

- For computing a number with a sharp accuracy, one wishes to get many decimals (or binary digits) with a small number of operations (products, say).
- For Diophantine questions, the cost is measured by the denominator q : one investigates how well ξ can be approximated in terms of q.
- A rational number has a single good approximation , itself ! Indeed *if* $\xi = a/b$ *is a given rational number, then for any* $p/q \in \mathbf{Q}$ *distinct from* ξ,

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

where $c = 1/b$. **Proof** : $|bq - ap| \geq 1$.

Rational Diophantine approximation

- For computing a number with a sharp accuracy, one wishes to get many decimals (or binary digits) with a small number of operations (products, say).
- For Diophantine questions, the cost is measured by the denominator q : one investigates how well ξ can be approximated in terms of q.
- A rational number has a single good approximation , itself ! Indeed *if* $\xi = a/b$ *is a given rational number, then for any* $p/q \in \mathbf{Q}$ *distinct from* ξ,

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

where $c = 1/b$. **Proof** : $|bq - ap| \geq 1$.

Rational approximation to real numbers

Result : for any $x \in \mathbf{R}$ and any $q \geq 1$, there exists $p \in \mathbf{Z}$ with $|qx - p| \leq 1/2$.

Proof : take for p the nearest integer to qx.

This inequality

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

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 real numbers

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

This inequality

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

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 real numbers

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

This inequality

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

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

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

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

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

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

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

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 for E the set $\{0, 1, \ldots, Q-1, Q\}$ and for F 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 $\mathrm{Card}E = Q + 1 > Q = \mathrm{Card}F$.

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 for E the set $\{0, 1, \ldots, Q-1, Q\}$ and for F 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 $\mathrm{Card}E = Q + 1 > Q = \mathrm{Card}F$.

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 for E the set $\{0, 1, \ldots, Q-1, Q\}$ and for F 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 $\mathrm{Card}E = Q + 1 > Q = \mathrm{Card}F$.

Existence of rational approximations

Next define $f : E \to F$ so that, for $1 \leq q < Q$, the interval $I = f(q)$ contains the fractional part $\{q\vartheta\}$ of $q\vartheta$, while $f(Q)$ is the interval $[(Q-1)/Q, 1]$.

Since f is not injective, there exists $q_1 < q_2$ with $f(q_1) = f(q_2)$. Let $q = q_2 - q_1$ and $I = f(q_1) = f(q_2)$.

Then we have $0 < q < Q$ (the case $q_1 = 0$, $q_2 = Q$ is ruled out).

Since $\{q_1\vartheta\}$ and $\{q_2\vartheta\}$ belong to the same subinterval $I \in F$, there exists $p \in \mathbf{Z}$ with

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

Existence of rational approximations

Next define $f : E \to F$ so that, for $1 \leq q < Q$, the interval $I = f(q)$ contains the fractional part $\{q\vartheta\}$ of $q\vartheta$, while $f(Q)$ is the interval $[(Q-1)/Q, 1]$.

Since f is not injective, there exists $q_1 < q_2$ with $f(q_1) = f(q_2)$. Let $q = q_2 - q_1$ and $I = f(q_1) = f(q_2)$.

Then we have $0 < q < Q$ (the case $q_1 = 0$, $q_2 = Q$ is ruled out).

Since $\{q_1\vartheta\}$ and $\{q_2\vartheta\}$ belong to the same subinterval $I \in F$, there exists $p \in \mathbf{Z}$ with

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

Existence of rational approximations

Next define $f : E \to F$ so that, for $1 \leq q < Q$, the interval $I = f(q)$ contains the fractional part $\{q\vartheta\}$ of $q\vartheta$, while $f(Q)$ is the interval $[(Q-1)/Q, 1]$.

Since f is not injective, there exists $q_1 < q_2$ with $f(q_1) = f(q_2)$. Let $q = q_2 - q_1$ and $I = f(q_1) = f(q_2)$.

Then we have $0 < q < Q$ (the case $q_1 = 0$, $q_2 = Q$ is ruled out).

Since $\{q_1\vartheta\}$ and $\{q_2\vartheta\}$ belong to the same subinterval $I \in F$, there exists $p \in \mathbf{Z}$ with

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

Existence of rational approximations

Next define $f : E \to F$ so that, for $1 \leq q < Q$, the interval $I = f(q)$ contains the fractional part $\{q\vartheta\}$ of $q\vartheta$, while $f(Q)$ is the interval $[(Q-1)/Q, 1]$.

Since f is not injective, there exists $q_1 < q_2$ with $f(q_1) = f(q_2)$. Let $q = q_2 - q_1$ and $I = f(q_1) = f(q_2)$.

Then we have $0 < q < Q$ (the case $q_1 = 0$, $q_2 = Q$ is ruled out).

Since $\{q_1\vartheta\}$ and $\{q_2\vartheta\}$ belong to the same subinterval $I \in F$, there exists $p \in \mathbf{Z}$ with

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

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 $d \geq 2$. There exists $c(\alpha) > 0$ such that, for any $p/q \in \mathbf{Q}$ with $q > 0$,*

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

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

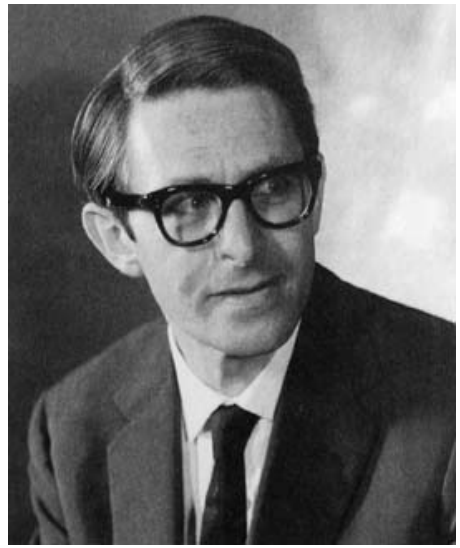
- any $\kappa > (d/2) + 1$ by A. Thue (1909),
- $2\sqrt{d}$ by C.L. Siegel in 1921,
- $\sqrt{2d}$ by F.J. Dyson and A.O. Gel'fond in 1947,
- any $\kappa > 2$ by K.F. Roth in 1955.

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 irrational 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 $\mathbf{Q}^m$.

W.M. Schmidt

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.*

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

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

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 and let $n \geq 2$. Then the equation

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

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

$$\sum_{i \in I} u_i \qquad \emptyset \neq I \subset \{1, \ldots, n\}$$

vanishes, has only finitely many solutions.

Finitely generated subgroup of $\mathbf{Q}^\times = \mathbf{Q} \setminus \{0\}$

If $S = \{p_1, \ldots, p_s\}$ be a finite set of prime numbers, the set of rational numbers with numerators and denominators divisible only by the prime numbers in S is a finitely generated subgroup of $\mathbf{Q}^\times$.

Indeed it is generated by $-1, p_1, \ldots, p_s, 1/p_1, \ldots, 1/p_s$.

Conversely, if G is a finitely generated subgroup of $\mathbf{Q}^\times$, then there exists a finite set $S = \{p_1, \ldots, p_s\}$ of prime numbers such that G is contained the set of rational numbers with numerators and denominators divisible only by the prime numbers in S.

Indeed, if $g_1, \ldots, g_t$ is a set of generators of G, then the set of prime divisors of the numerators and denominators of the g_i is a solution.

Finitely generated subgroup of $\mathbf{Q}^\times = \mathbf{Q} \setminus \{0\}$

If $S = \{p_1, \ldots, p_s\}$ be a finite set of prime numbers, the set of rational numbers with numerators and denominators divisible only by the prime numbers in S is a finitely generated subgroup of $\mathbf{Q}^\times$.

Indeed it is generated by $-1, p_1, \ldots, p_s, 1/p_1, \ldots, 1/p_s$.

Conversely, if G is a finitely generated subgroup of $\mathbf{Q}^\times$, then there exists a finite set $S = \{p_1, \ldots, p_s\}$ of prime numbers such that G is contained the set of rational numbers with numerators and denominators divisible only by the prime numbers in S.

Indeed, if $g_1, \ldots, g_t$ is a set of generators of G, then the set of prime divisors of the numerators and denominators of the g_i is a solution.

Finitely generated subgroup of $\mathbf{Q}^\times = \mathbf{Q} \setminus \{0\}$

If $S = \{p_1, \ldots, p_s\}$ be a finite set of prime numbers, the set of rational numbers with numerators and denominators divisible only by the prime numbers in S is a finitely generated subgroup of $\mathbf{Q}^\times$.

Indeed it is generated by $-1, p_1, \ldots, p_s, 1/p_1, \ldots, 1/p_s$.

Conversely, if G is a finitely generated subgroup of $\mathbf{Q}^\times$, then there exists a finite set $S = \{p_1, \ldots, p_s\}$ of prime numbers such that G is contained the set of rational numbers with numerators and denominators divisible only by the prime numbers in S.

Indeed, if $g_1, \ldots, g_t$ is a set of generators of G, then the set of prime divisors of the numerators and denominators of the g_i is a solution.

Finitely generated subgroup of $\mathbf{Q}^\times = \mathbf{Q} \setminus \{0\}$

If $S = \{p_1, \ldots, p_s\}$ be a finite set of prime numbers, the set of rational numbers with numerators and denominators divisible only by the prime numbers in S is a finitely generated subgroup of $\mathbf{Q}^\times$.

Indeed it is generated by $-1, p_1, \ldots, p_s, 1/p_1, \ldots, 1/p_s$.

Conversely, if G is a finitely generated subgroup of $\mathbf{Q}^\times$, then there exists a finite set $S = \{p_1, \ldots, p_s\}$ of prime numbers such that G is contained the set of rational numbers with numerators and denominators divisible only by the prime numbers in S.

Indeed, if $g_1, \ldots, g_t$ is a set of generators of G, then the set of prime divisors of the numerators and denominators of the g_i is a solution.

The generalized S–unit equation

Let K be a field of characteristic zero, let G be a finitely multiplicative subgroup of the multiplicative group $K^{\times} = K \setminus \{0\}$ and let $n \geq 2$. Then the equation

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

where the unknowns $u_1, u_2, \cdots, u_n$ are in G for which no nontrivial subsum

$$\sum_{i \in I} u_i \qquad \emptyset \neq I \subset \{1, \ldots, n\}$$

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.

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.

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

Joseph Louis Lagrange

Henri Poincaré

Historical survey

Pierre de Fermat (1601 - 1665)

Leonhard Euler (1707 - 1783)

Joseph Louis Lagrange (1736 - 1813)

XIXth Century : Hurwitz, Poincaré

Joseph Louis Lagrange

Henri Poincaré

Historical survey

Pierre de Fermat (1601 - 1665)

Leonhard Euler (1707 - 1783)

Joseph Louis Lagrange (1736 - 1813)

XIXth Century : Hurwitz, Poincaré

Joseph Louis Lagrange

Henri Poincaré

Historical survey

Pierre de Fermat (1601 - 1665)

Leonhard Euler (1707 - 1783)

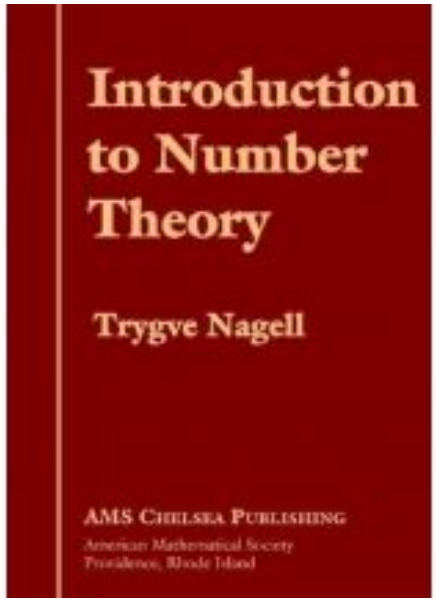
Joseph Louis Lagrange (1736 - 1813)

XIXth Century : Hurwitz, Poincaré

Joseph Louis Lagrange

Henri Poincaré

Ramanujan – Nagell Equation



Srinivasa Ramanujan (1887 – 1920)

Trygve Nagell (1895 – 1988)

Ramanujan – Nagell Equation

$$x^2 + 7 = 2^n$$

$$\begin{aligned}
1^2 + 7 &= 2^3 &&= 8 \\
3^2 + 7 &= 2^4 &&= 16 \\
5^2 + 7 &= 2^5 &&= 32 \\
11^2 + 7 &= 2^7 &&= 128 \\
181^2 + 7 &= 2^{15} &&= 32\,768
\end{aligned}$$

Ramanujan – Nagell Equation

$$x^2 + 7 = 2^n$$

$$\begin{aligned}
1^2 + 7 &= 2^3 &&= 8 \\
3^2 + 7 &= 2^4 &&= 16 \\
5^2 + 7 &= 2^5 &&= 32 \\
11^2 + 7 &= 2^7 &&= 128 \\
181^2 + 7 &= 2^{15} &&= 32\,768
\end{aligned}$$

$x^2 + D = 2^n$

Nagell (1948) : for $D = 7$, no further solution

Apéry (1960) : for $D > 0$, $D \neq 7$, the equation $x^2 + D = 2^n$ has at most 2 solutions.

Examples with 2 solutions :

$$D = 23 : \qquad 3^2 + 23 = 32, \quad 45^2 + 23 = 2^{11} = 2\,048$$

$$D = 2^{\ell+1} - 1,\ \ell \geq 3 : \qquad (2^\ell - 1)^2 + 2^{\ell+1} - 1 = 2^{2\ell}$$

$x^2 + D = 2^n$

Nagell (1948) : for $D = 7$, no further solution

Apéry (1960) : for $D > 0$, $D \neq 7$, the equation $x^2 + D = 2^n$ has at most 2 solutions.

Examples with 2 solutions :

$$D = 23 : \qquad 3^2 + 23 = 32, \quad 45^2 + 23 = 2^{11} = 2\,048$$

$$D = 2^{\ell+1} - 1,\ \ell \geq 3 : \qquad (2^\ell - 1)^2 + 2^{\ell+1} - 1 = 2^{2\ell}$$

$x^2 + D = 2^n$

Nagell (1948) : for $D = 7$, no further solution

Apéry (1960) : for $D > 0$, $D \neq 7$, the equation $x^2 + D = 2^n$ has at most 2 solutions.

Examples with 2 solutions :

$$D = 23 : \qquad 3^2 + 23 = 32, \quad 45^2 + 23 = 2^{11} = 2\,048$$

$$D = 2^{\ell+1} - 1,\ \ell \geq 3 : \qquad (2^\ell - 1)^2 + 2^{\ell+1} - 1 = 2^{2\ell}$$

$x^2 + D = 2^n$

Beukers (1980) : at most one solution otherwise.

M. Bennett (1995) : considers the case $D < 0$.

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 10th 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.

Hilbert's 10th 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 10th 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 10th problem is not yet solved :
to give an algorithm in order to decide whether a diophantine equation has a rational solution or not.

Negative solution to Hilbert's 10th 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 10th problem is not yet solved :
to give an algorithm in order to decide whether a diophantine equation has a rational solution or not.

Negative solution to Hilbert's 10th 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 10th problem is not yet solved :
to give an algorithm in order to decide whether a diophantine equation has a rational solution or not.

Negative solution to Hilbert's 10th 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 10th problem is not yet solved :
to give an algorithm in order to decide whether a diophantine equation has a rational solution or not.

Negative solution to Hilbert's 10th 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 10th 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) : there are only finitely many integer solutions of

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

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

Mordell's Conjecture (1922) : rational points

Siegel's Theorem (1929) : integral points

Faltings's 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's Theorem.

Historical survey

Thue (1908) : there are only finitely many integer solutions of

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

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

Mordell's Conjecture (1922) : rational points

Siegel's Theorem (1929) : integral points

Faltings's 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's Theorem.

Historical survey

Thue (1908) : there are only finitely many integer solutions of

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

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

Mordell's Conjecture (1922) : rational points

Siegel's Theorem (1929) : integral points

Faltings's 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's Theorem.

Historical survey

Thue (1908) : there are only finitely many integer solutions of

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

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

Mordell's Conjecture (1922) : rational points

Siegel's Theorem (1929) : integral points

Faltings's 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's Theorem.

Historical survey

Thue (1908) : there are only finitely many integer solutions of

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

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

Mordell's Conjecture (1922) : rational points

Siegel's Theorem (1929) : integral points

Faltings's 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's Theorem.

Historical survey

Thue (1908) : there are only finitely many integer solutions of

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

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

Mordell's Conjecture (1922) : rational points

Siegel's Theorem (1929) : integral points

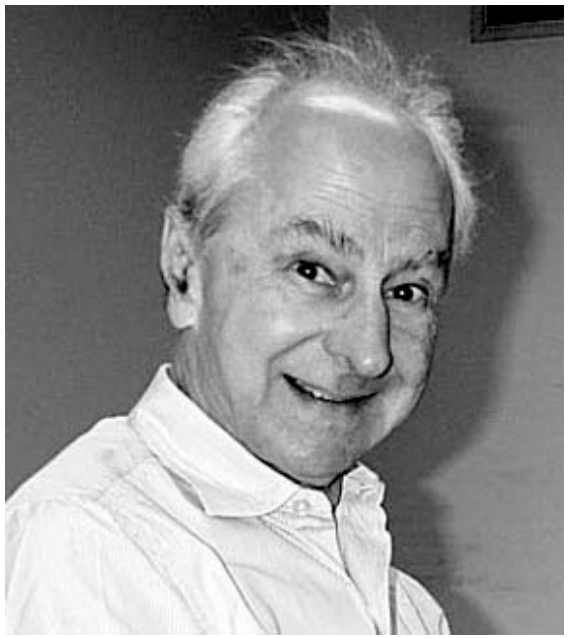
Faltings's Theorem(1983) : finiteness of rational points on an algebraic curve of genus ≥ 2 over a number field.

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's Theorem.

Serge Lang (1927–2005)



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.

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

Paul Vojta

Paul Vojta,
Diophantine Approximations and Value Distribution Theory,
Lecture Notes in Mathematics **1239**, Springer Verlag, 1987,

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* $p/q \in \mathbf{Q}$,

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

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* $p/q \in \mathbf{Q}$,

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

Mike Bennett

http://www.math.ubc.ca/∼bennett/

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

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

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*

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

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

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

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 $\mathbf{Z}_K = \mathbf{Z}[\Phi]$.

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 $\mathbf{Z}_K = \mathbf{Z}[\Phi]$.

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 $\mathbf{Z}_K = \mathbf{Z}[\Phi]$.

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 $\mathbf{Z}_K = \mathbf{Z}[\Phi]$.

Number fields, units

When K is a number field, $\mathbf{Z}_K^\times$ denotes the group of units (invertible elements) of the ring $\mathbf{Z}_K$.

An algebraic unit is an algebraic number which is a root of a monic polynomial in $\mathbf{Z}[X]$ with constant term ± 1.

Number fields, units

When K is a number field, $\mathbf{Z}_K^\times$ denotes the group of units (invertible elements) of the ring $\mathbf{Z}_K$.

An algebraic unit is an algebraic number which is a root of a monic polynomial in $\mathbf{Z}[X]$ with constant term ± 1.

Thue equation

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

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 $(\varepsilon_1, \varepsilon_2) \in \mathbf{Z}_K^\times \times \mathbf{Z}_K^\times$.

Thue–Mahler equations

Let $F \in \mathbf{Z}[X, Y]$ be a homogeneous polynomial with rational integer coefficients having at least 3 non proportional linear factors over the field of algebraic numbers. Let $m \in \mathbf{Z}$, $m \neq 0$.

Let $p_1, \ldots, p_s$ be prime numbers. Then the Diophantine equation

$$F(X, Y) = m p_1^{Z_1} \ldots p_s^{Z_s}$$

has only finitely many solutions $(x, y, z_1, \ldots, z_s) \in \mathbf{Z}^{2+s}$ with $z_j \geq 0$ for $j = 1, \ldots, s$, $xy \neq 0$ and $\gcd(xy, p_1 \cdots p_s) = 1$.

S–integers, S–units

Let K be a number field and S be a finite set of places of K containing the infinite places. The ring $\mathcal{O}_S$ of S-integers of K is defined by

$$\mathcal{O}_S = \{x \in K \mid |x|_v \leq 1 \text{ for each } v \notin S\}.$$

The group $\mathcal{O}_S^\times$ of S-units of K is the group of units of $\mathcal{O}_S$, namely

$$\mathcal{O}_S^\times = \{x \in K \mid |x|_v = 1 \text{ for each } v \notin S\}.$$

Two special cases

- For S the set of infinite places of K, $\mathcal{O}_S$ is the ring $\mathbf{Z}_K$ of integers of K and $\mathcal{O}_S^\times$ is the group $\mathbf{Z}_K^\times$ of units of K.

- For $K = \mathbf{Q}$, $S = \{\infty, p_1, \ldots, p_s\}$, with $s \geq 0$

$$\mathcal{O}_S = \{a/b \in \mathbf{Q} \mid b = p_1^{z_1} \cdots p_s^{z_s} \text{ with } z_1, \ldots, z_s \text{ in } \mathbf{Z},\ z_j \geq 0\}$$

and

$$\mathcal{O}_S^\times = \{p_1^{t_1} \cdots p_s^{t_s} \text{ with } t_1, \ldots, t_s \text{ in } \mathbf{Z}\}.$$

Hence

$$\mathcal{O}_S = \{a/b \in \mathbf{Q} \mid a \in \mathbf{Z},\ b \in \mathbf{Z} \cap \mathcal{O}_S^\times\}$$

Two special cases

- For S the set of infinite places of K, $\mathcal{O}_S$ is the ring $\mathbf{Z}_K$ of integers of K and $\mathcal{O}_S^\times$ is the group $\mathbf{Z}_K^\times$ of units of K.

- For $K = \mathbf{Q}$, $S = \{\infty, p_1, \ldots, p_s\}$, with $s \geq 0$

$$\mathcal{O}_S \;=\; \{a/b \in \mathbf{Q} \mid b = p_1^{z_1} \cdots p_s^{z_s} \text{ with } z_1, \ldots, z_s \text{ in } \mathbf{Z},\ z_j \geq 0\ \}$$

and

$$\mathcal{O}_S^\times \;=\; \{p_1^{t_1} \cdots p_s^{t_s} \text{ with } t_1, \ldots, t_s \text{ in } \mathbf{Z}\}.$$

Hence

$$\mathcal{O}_S \;=\; \{a/b \in \mathbf{Q} \mid a \in \mathbf{Z},\ b \in \mathbf{Z} \cap \mathcal{O}_S^\times\}$$

Thue–Mahler equations over a number field

We will consider the Thue–Mahler equations

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

where the two unknowns X, Y take respectively values x, y in the ring of S–integers of K while the unknown E takes its values ε in the group of S–units of K.

If (x, y, ε) is a solution, namely

$$F(x, y) = \varepsilon,$$

and if d denotes the degree of F, then, for all $\eta \in \mathcal{O}_S^\times$, the triple $(\eta x, \eta y, \eta^d \varepsilon)$ is also a solution :

$$F(\eta x, \eta y) = \eta^d \varepsilon.$$

Thue–Mahler equations over a number field

We will consider the Thue–Mahler equations

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

where the two unknowns X, Y take respectively values x, y in the ring of S–integers of K while the unknown E takes its values ε in the group of S–units of K.

If (x, y, ε) is a solution, namely

$$F(x, y) = \varepsilon,$$

and if d denotes the degree of F, then, for all $\eta \in \mathcal{O}_S^\times$, the triple $(\eta x, \eta y, \eta^d \varepsilon)$ is also a solution :

$$F(\eta x, \eta y) = \eta^d \varepsilon.$$

Equivalence classes

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.

In other terms, two solutions (x, y, ε) and (x', y', ε') are equivalent if there exists $\eta \in \mathcal{O}_S^\times$ such that

$$x' = \eta x, \quad y' = \eta y, \quad \varepsilon' = \eta^d \varepsilon$$

where d is the degree of F.

Equivalence classes

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.

In other terms, two solutions (x, y, ε) and (x', y', ε') are equivalent if there exists $\eta \in \mathcal{O}_S^\times$ such that

$$x' = \eta x, \quad y' = \eta y, \quad \varepsilon' = \eta^d \varepsilon$$

where d is the degree of F.

Thue–Mahler equations (continued)

For any finite set S of places of K containing all the archimedean places, for every $m \in K^\times$ 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

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

has but a finite number of classes of solutions
$(x, y, \varepsilon) \in \mathcal{O}_S^2 \times \mathcal{O}_S^\times$
(namely : the set of solutions $(x, y, \varepsilon) \in \mathcal{O}_S^2 \times \mathcal{O}_S^\times$ can be written as the union of a finite number of equivalence classes modulo $\mathcal{O}_S^\times$).

Thue–Mahler equations (continued)

For any finite set S of places of K containing all the archimedean places, for every $m \in K^\times$ 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

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

has but a finite number of classes of solutions
$(x, y, \varepsilon) \in \mathcal{O}_S^2 \times \mathcal{O}_S^\times$
(namely : the set of solutions $(x, y, \varepsilon) \in \mathcal{O}_S^2 \times \mathcal{O}_S^\times$ can be written as the union of a finite number of equivalence classes modulo $\mathcal{O}_S^\times$).

A "special" case

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 $(x, y, \varepsilon) \in \mathcal{O}_S^2 \times \mathcal{O}_S^\times$.

Fact : *this special case is equivalent to the general case !*

A "special" case

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 $(x, y, \varepsilon) \in \mathcal{O}_S^2 \times \mathcal{O}_S^\times$.

Fact : *this special case is equivalent to the general case !*

Siegel S–unit equation

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 $\mathcal{O}_S^\times \times \mathcal{O}_S^\times$.

Fact : *this statement is also equivalent to the finiteness of the number of classes of solutions of the Thue–Mahler equation* $XY(X-Y) = E$.

$$X = E_0, \quad Y = E_2, \quad X - Y = E_1,$$

$$E_1 + E_2 = E_0, \quad E_0 E_1 E_2 = E.$$

Siegel S–unit equation

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 $\mathcal{O}_S^\times \times \mathcal{O}_S^\times$.

Fact : *this statement is also equivalent to the finiteness of the number of classes of solutions of the Thue–Mahler equation* $XY(X-Y) = E$.

$$X = E_0, \quad Y = E_2, \quad X - Y = E_1,$$

$$E_1 + E_2 = E_0, \quad E_0 E_1 E_2 = E.$$

Siegel S–unit equation

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 $\mathcal{O}_S^\times \times \mathcal{O}_S^\times$.

Fact : *this statement is also equivalent to the finiteness of the number of classes of solutions of the Thue–Mahler equation* $XY(X-Y) = E$.

$$X = E_0, \quad Y = E_2, \quad X - Y = E_1,$$

$$E_1 + E_2 = E_0, \quad E_0 E_1 E_2 = E.$$

Siegel S–unit equation

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 $\mathcal{O}_S^\times \times \mathcal{O}_S^\times$.

Fact : *this statement is also equivalent to the finiteness of the number of classes of solutions of the Thue–Mahler equation* $XY(X-Y) = E$.

$$X = E_0, \quad Y = E_2, \quad X - Y = E_1,$$

$$E_1 + E_2 = E_0, \quad E_0 E_1 E_2 = E.$$

Families of Thue equations

The first families of Thue equations having only trivial solutions were introduced by A. Thue himself.

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

He proved that the only solution in positive integers x, y is $x = y = 1$ for n prime and a sufficiently large in terms of n. For $n = 3$ this equation has only this solution for $a \geq 386$.

M. Bennett (2001) proved that this is true for all a and n with $n \geq 3$ and $a \geq 1$.

Families of Thue equations

The first families of Thue equations having only trivial solutions were introduced by A. Thue himself.

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

He proved that the only solution in positive integers x, y is $x = y = 1$ for n prime and a sufficiently large in terms of n. For $n = 3$ this equation has only this solution for $a \geq 386$.

M. Bennett (2001) proved that this is true for all a and n with $n \geq 3$ and $a \geq 1$.

Families of Thue equations (continued)

E. Thomas in 1990 studied the families of equations $F_a(X, Y) = 1$ associated with D. Shanks' simplest cubic fields (cf. John Friedlander's lecture), viz.

$$F_a(X, Y) = X^3 - (a-1)X^2Y - (a+2)XY^2 - Y^3.$$

According to E. Thomas (1990) and M. Mignotte (1993), for $a \geq 4$ the only solutions are $(0, -1)$, $(1, 0)$ and $(-1, +1)$, while for the cases $a = 0, 1, 3$, there exist some nontrivial solutions, too, which are given explicitly by Thomas.

For the same form $F_a(X, Y)$, all solutions of the Thue inequality $|F_a(X, Y)| \leq 2a + 1$ have been found by M. Mignote A. Pethő and F. Lemmermeyer (1996).

The family of Thue's equations attached to some quintic fields by E. Lehmer do not seem to have been investigated from this point of view so far.

Families of Thue equations (continued)

E. Thomas in 1990 studied the families of equations $F_a(X, Y) = 1$ associated with D. Shanks' simplest cubic fields (cf. John Friedlander's lecture), viz.

$$F_a(X, Y) = X^3 - (a-1)X^2Y - (a+2)XY^2 - Y^3.$$

According to E. Thomas (1990) and M. Mignotte (1993), for $a \geq 4$ the only solutions are $(0, -1)$, $(1, 0)$ and $(-1, +1)$, while for the cases $a = 0, 1, 3$, there exist some nontrivial solutions, too, which are given explicitly by Thomas.

For the same form $F_a(X, Y)$, all solutions of the Thue inequality $|F_a(X, Y)| \leq 2a + 1$ have been found by M. Mignote A. Pethő and F. Lemmermeyer (1996).

The family of Thue's equations attached to some quintic fields by E. Lehmer do not seem to have been investigated from this point of view so far.

Families of Thue equations (continued)

E. Thomas in 1990 studied the families of equations $F_a(X, Y) = 1$ associated with D. Shanks' simplest cubic fields (cf. John Friedlander's lecture), viz.

$$F_a(X, Y) = X^3 - (a-1)X^2Y - (a+2)XY^2 - Y^3.$$

According to E. Thomas (1990) and M. Mignotte (1993), for $a \geq 4$ the only solutions are $(0, -1)$, $(1, 0)$ and $(-1, +1)$, while for the cases $a = 0, 1, 3$, there exist some nontrivial solutions, too, which are given explicitly by Thomas.

For the same form $F_a(X, Y)$, all solutions of the Thue inequality $|F_a(X, Y)| \leq 2a + 1$ have been found by M. Mignote A. Pethő and F. Lemmermeyer (1996).

The family of Thue's equations attached to some quintic fields by E. Lehmer do not seem to have been investigated from this point of view so far.

Families of Thue equations (continued)

E. Lee and M. Mignotte with N. Tzanakis studied in 1991 and 1992 the family of cubic Thue equations

$$X^3 - aX^2Y - (a+1)XY^2 - Y^3 = 1.$$

The left hand side is $X(X+Y)(X-(a+1)Y) - Y^3$.

For $a \geq 3.33 \cdot 10^{23}$, there are only the solutions $(1,0)$, $(0,-1)$, $(1,-1)$, $(-a-1,-1)$, $(1,-a)$.

In 2000, M. Mignotte could prove the same result for all $a \geq 3$.

Families of Thue equations (continued)

E. Lee and M. Mignotte with N. Tzanakis studied in 1991 and 1992 the family of cubic Thue equations

$$X^3 - aX^2Y - (a+1)XY^2 - Y^3 = 1.$$

The left hand side is $X(X+Y)(X-(a+1)Y) - Y^3$.

For $a \geq 3.33 \cdot 10^{23}$, there are only the solutions $(1,0)$, $(0,-1)$, $(1,-1)$, $(-a-1,-1)$, $(1,-a)$.

In 2000, M. Mignotte could prove the same result for all $a \geq 3$.

Families of Thue equations (continued)

E. Lee and M. Mignotte with N. Tzanakis studied in 1991 and 1992 the family of cubic Thue equations

$$X^3 - aX^2Y - (a+1)XY^2 - Y^3 = 1.$$

The left hand side is $X(X+Y)(X-(a+1)Y) - Y^3$.

For $a \geq 3.33 \cdot 10^{23}$, there are only the solutions $(1,0)$, $(0,-1)$, $(1,-1)$, $(-a-1,-1)$, $(1,-a)$.

In 2000, M. Mignotte could prove the same result for all $a \geq 3$.

Families of Thue equations (continued)

I. Wakabayashi proved in 2003 that for $a \geq 1.35 \cdot 10^{14}$, the equation

$$X^3 - a^2XY^2 + Y^3 = 1$$

has exactly the five solutions $(0, 1)$, $(1, 0)$, $(1, a^2)$, $(\pm a, 1)$.

A. Togbé considered the family of equations

$$X^3 - (n^3 - 2n^2 + 3n - 3)X^2Y - n^2XY^2 - Y^3 = \pm 1$$

in 2004. For $n \geq 1$, the only solutions are $(\pm 1, 0)$ and $(0, \pm 1)$.

Families of Thue equations (continued)

I. Wakabayashi proved in 2003 that for $a \geq 1.35 \cdot 10^{14}$, the equation

$$X^3 - a^2XY^2 + Y^3 = 1$$

has exactly the five solutions $(0, 1)$, $(1, 0)$, $(1, a^2)$, $(\pm a, 1)$.

A. Togbé considered the family of equations

$$X^3 - (n^3 - 2n^2 + 3n - 3)X^2Y - n^2XY^2 - Y^3 = \pm 1$$

in 2004. For $n \geq 1$, the only solutions are $(\pm 1, 0)$ and $(0, \pm 1)$.

Families of Thue equations (continued)

I. Wakabayashi in 2002 used Padé approximation for solving the Diophantine inequality

$$|X^3 + aXY^2 + bY^3| \leq a + |b| + 1$$

for arbitrary b and $a \geq 360b^4$ as well as for $b \in \{1, 2\}$ and $a \geq 1$.

Families of Thue equations (continued)

E. Thomas considered some families of Diophantine equations

$$X^3 - bX^2Y + cXY^2 - Y^3 = 1$$

for restricted values of b and c.

Family of quartic equations :

$$X^4 - aX^3Y - X^2Y^2 + aXY^3 + Y^4 = \pm 1$$

(A. Pethő 1991 , M. Mignotte, A. Pethő and R. Roth, 1996).
The left hand side is $X(X-Y)(X+Y)(X-aY) + Y^4$.

Families of Thue equations (continued)

E. Thomas considered some families of Diophantine equations

$$X^3 - bX^2Y + cXY^2 - Y^3 = 1$$

for restricted values of b and c.

Family of quartic equations :

$$X^4 - aX^3Y - X^2Y^2 + aXY^3 + Y^4 = \pm 1$$

(A. Pethő 1991 , M. Mignotte, A. Pethő and R. Roth, 1996).
The left hand side is $X(X-Y)(X+Y)(X-aY) + Y^4$.

Families of Thue equations (continued)

Further work on equations of degrees up to 8 by J.H. Chen, I. Gaál, C. Heuberger, B. Jadrijević, G. Lettl, C. Levesque, M. Mignotte, A. Pethő, R. Roth, R. Tichy, E. Thomas, A. Togbé, P. Voutier, I. Wakabayashi, P. Yuan, V. Ziegler...

Families of Thue equations (continued)

Split families of E. Thomas (1993) :

$$\prod_{i=1}^{n}(X - p_i(a)Y) - Y^n = \pm 1,$$

where $p_1, \ldots, p_n$ are polynomials in $\mathbf{Z}[a]$.

Surveys by I. Wakabayashi (2002) and C. Heuberger (2005).

Families of Thue equations (continued)

Split families of E. Thomas (1993) :

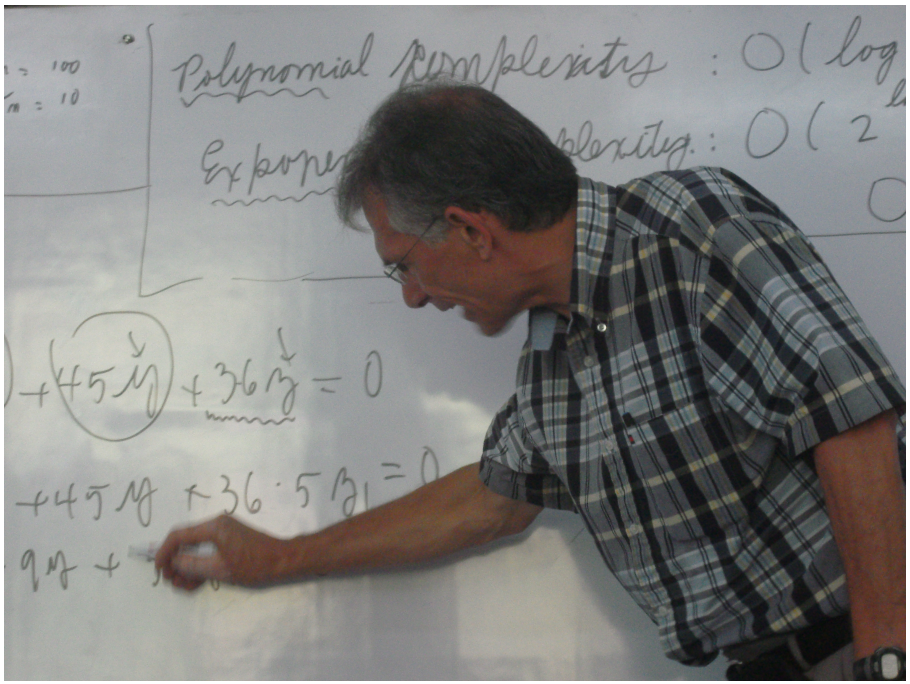
$$\prod_{i=1}^{n}(X - p_i(a)Y) - Y^n = \pm 1,$$

where $p_1, \ldots, p_n$ are polynomials in $\mathbf{Z}[a]$.

Surveys by I. Wakabayashi (2002) and C. Heuberger (2005).

New families of Diophantine equations

So far, a rather small number of families of Thue curves having only trivial integral points have been exhibited. In a joint work with Claude Levesque, for each number field K of degree at least three and for each finite set S of places of K containing the infinite places, we produce families of curves related to the units of the number field, having only trivial S–integral points.



Families of Thue equations

Let K be a number field and $d = [K : \mathbf{Q}]$ its degree. For each $\varepsilon \in \mathbf{Z}_K^\times$ for which $\mathbf{Q}(\varepsilon) = K$, let $f_\varepsilon(X) \in \mathbf{Z}[X]$ be the irreducible polynomial of ε over $\mathbf{Q}$.

Set $F_\varepsilon(X, Y) = Y^d f_\varepsilon(X/Y)$. Hence $F_\varepsilon(X, Y) \in \mathbf{Z}[X, Y]$ is an irreducible binary form of degree d with integer coefficients.

A special case of the main result of a joint work with Claude Levesque is the following :

Theorem

Let K be a number field and let $m \in \mathbf{Z}$, $m \neq 0$. Then the set

$$\left\{(x, y, \varepsilon) \in \mathbf{Z}^2 \times \mathbf{Z}_K^\times \mid xy \neq 0,\ \mathbf{Q}(\varepsilon) = K,\ F_\varepsilon(x, y) = m\right\}$$

is finite.

Families of Thue equations

Let K be a number field and $d = [K : \mathbf{Q}]$ its degree. For each $\varepsilon \in \mathbf{Z}_K^\times$ for which $\mathbf{Q}(\varepsilon) = K$, let $f_\varepsilon(X) \in \mathbf{Z}[X]$ be the irreducible polynomial of ε over $\mathbf{Q}$.

Set $F_\varepsilon(X, Y) = Y^d f_\varepsilon(X/Y)$. Hence $F_\varepsilon(X, Y) \in \mathbf{Z}[X, Y]$ is an irreducible binary form of degree d with integer coefficients.

A special case of the main result of a joint work with Claude Levesque is the following :

Theorem

Let K be a number field and let $m \in \mathbf{Z}$, $m \neq 0$. Then the set

$$\left\{(x, y, \varepsilon) \in \mathbf{Z}^2 \times \mathbf{Z}_K^\times \mid xy \neq 0,\ \mathbf{Q}(\varepsilon) = K,\ F_\varepsilon(x, y) = m\right\}$$

is finite.

Effective results

In some cases, for instance when the number field K has at most one real embedding, we are able to produce an effective result.

Recall that $\varepsilon \in \mathbf{Z}_K^\times$, $f_\varepsilon(X)$ is the irreducible polynomial of ε and

$$F_\varepsilon(X, Y) = Y^d f_\varepsilon(X/Y).$$

Theorem

Under these assumptions, there exists a constant $\kappa > 0$, depending only on K, such that, for any $m \geq 2$, any (x, y, ε) in the set

$$\left\{(x, y, \varepsilon) \in \mathbf{Z}^2 \times \mathbf{Z}_K^\times \;\mid\; xy \neq 0,\ \mathbf{Q}(\varepsilon) = K,\ |F_\varepsilon(x, y)| \leq m\right\}$$

satisfies

$$\max\left\{\left(|x|, |y|, e^{\mathrm{h}(\varepsilon)}\right)\right\} \leq m^\kappa.$$

References :

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

Familles d'équations de Thue–Mahler n'ayant que des solutions triviales ;
Acta Arithmetica, **155** (2012), 117–138.

http://www.math.jussieu.fr/~miw/articles/pdf/CLMWFamillesThueMahler2011.pdf

Sketch of proof

Let $\sigma_1, \ldots, \sigma_d$ be the complex embeddings from the number field K into $\mathbf{C}$, where $d = [K : \mathbf{Q}]$. . Any $\varepsilon \in \mathbf{Z}_K^\times$ with $\mathbf{Q}(\varepsilon) = K$ is root of the irreducible polynomial

$$f_\varepsilon(X) = (X - \sigma_1(\varepsilon)) \cdots (X - \sigma_d(\varepsilon)) \in \mathbf{Z}[X].$$

Let $m \geq 1$. The goal is tho prove that there are only finitely many $(x, y, \varepsilon) \in \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}_K^\times$ with $xy > 1$ and $\mathbf{Q}(\varepsilon) = K$ satisfying

$$(x - \sigma_1(\varepsilon)y) \cdots (x - \sigma_d(\varepsilon)y) = m.$$

Sketch of proof

Let $\sigma_1, \ldots, \sigma_d$ be the complex embeddings from the number field K into $\mathbf{C}$, where $d = [K : \mathbf{Q}]$. . Any $\varepsilon \in \mathbf{Z}_K^\times$ with $\mathbf{Q}(\varepsilon) = K$ is root of the irreducible polynomial

$$f_\varepsilon(X) = \big(X - \sigma_1(\varepsilon)\big) \cdots \big(X - \sigma_d(\varepsilon)\big) \in \mathbf{Z}[X].$$

Let $m \geq 1$. The goal is tho prove that there are only finitely many $(x, y, \varepsilon) \in \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}_K^\times$ with $xy > 1$ and $\mathbf{Q}(\varepsilon) = K$ satisfying

$$\big(x - \sigma_1(\varepsilon)y\big) \cdots \big(x - \sigma_d(\varepsilon)y\big) = m.$$

Sketch of proof

Let $\sigma_1, \ldots, \sigma_d$ be the complex embeddings from the number field K into $\mathbf{C}$, where $d = [K : \mathbf{Q}]$. . Any $\varepsilon \in \mathbf{Z}_K^\times$ with $\mathbf{Q}(\varepsilon) = K$ is root of the irreducible polynomial

$$f_\varepsilon(X) = \big(X - \sigma_1(\varepsilon)\big) \cdots \big(X - \sigma_d(\varepsilon)\big) \in \mathbf{Z}[X].$$

Let $m \geq 1$. The goal is tho prove that there are only finitely many $(x, y, \varepsilon) \in \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}_K^\times$ with $xy > 1$ and $\mathbf{Q}(\varepsilon) = K$ satisfying

$$\big(x - \sigma_1(\varepsilon)y\big) \cdots \big(x - \sigma_d(\varepsilon)y\big) = m.$$

Sketch of proof (continued)

For $j = 1, \ldots, d$, define $\beta_j = x - \varepsilon_j y$, so that

$$\beta_1 \cdots \beta_d = m.$$

Hence β_j is product of an element, which belongs to a finite set depending on K and m only, with a unit. Eliminate x and y among the three equations

$$\beta_1 = x - \varepsilon_1 y, \qquad \beta_2 = x - \varepsilon_2 y, \qquad \beta_3 = x - \varepsilon_3 y.$$

We get

$$\varepsilon_1\beta_2 - \varepsilon_1\beta_3 + \varepsilon_2\beta_3 - \varepsilon_2\beta_1 + \varepsilon_3\beta_1 - \varepsilon_3\beta_2 = 0.$$

Sketch of proof (continued)

For $j = 1, \ldots, d$, define $\beta_j = x - \varepsilon_j y$, so that

$$\beta_1 \cdots \beta_d = m.$$

Hence β_j is product of an element, which belongs to a finite set depending on K and m only, with a unit. Eliminate x and y among the three equations

$$\beta_1 = x - \varepsilon_1 y, \qquad \beta_2 = x - \varepsilon_2 y, \qquad \beta_3 = x - \varepsilon_3 y.$$

We get

$$\varepsilon_1\beta_2 - \varepsilon_1\beta_3 + \varepsilon_2\beta_3 - \varepsilon_2\beta_1 + \varepsilon_3\beta_1 - \varepsilon_3\beta_2 = 0.$$

Sketch of proof (continued)

For $j = 1, \ldots, d$, define $\beta_j = x - \varepsilon_j y$, so that

$$\beta_1 \cdots \beta_d = m.$$

Hence β_j is product of an element, which belongs to a finite set depending on K and m only, with a unit. Eliminate x and y among the three equations

$$\beta_1 = x - \varepsilon_1 y, \qquad \beta_2 = x - \varepsilon_2 y, \qquad \beta_3 = x - \varepsilon_3 y.$$

We get

$$\varepsilon_1\beta_2 - \varepsilon_1\beta_3 + \varepsilon_2\beta_3 - \varepsilon_2\beta_1 + \varepsilon_3\beta_1 - \varepsilon_3\beta_2 = 0.$$

Effectivity

The equation

$$\varepsilon_1\beta_2 - \varepsilon_1\beta_3 + \varepsilon_2\beta_3 - \varepsilon_2\beta_1 + \varepsilon_3\beta_1 - \varepsilon_3\beta_2 = 0$$

is a S–unit equation. Schmidt's subspace Theorem states that there are only finitely many solutions with non–vanishing subsums of the left hand side.
One needs to check what happens when a subsum in the left hand side vanishes.

Effectivity

The equation

$$\varepsilon_1\beta_2 - \varepsilon_1\beta_3 + \varepsilon_2\beta_3 - \varepsilon_2\beta_1 + \varepsilon_3\beta_1 - \varepsilon_3\beta_2 = 0$$

is a S–unit equation. Schmidt's subspace Theorem states that there are only finitely many solutions with non–vanishing subsums of the left hand side.

One needs to check what happens when a subsum in the left hand side vanishes.

Effectivity

The equation

$$\varepsilon_1\beta_2 - \varepsilon_1\beta_3 + \varepsilon_2\beta_3 - \varepsilon_2\beta_1 + \varepsilon_3\beta_1 - \varepsilon_3\beta_2 = 0$$

is a S–unit equation. Schmidt's subspace Theorem states that there are only finitely many solutions with non–vanishing subsums of the left hand side.
One needs to check what happens when a subsum in the left hand side vanishes.

Baker's method involving linear forms in logarithms

One main concern is that Schmidt's subspace Theorem (as well as the Theorem of Thue– Siegel– Roth) is non–effective : upper bounds for the number of solutions can be derived, but no upper bound for the solutions themselves.

Only the case of a S–unit equation

$$\epsilon_1 + \epsilon_2 + \epsilon_3 = 0$$

can be solved effectively by means of Baker's method.

Work of A.O. Gel'fond, A. Baker, K. Győry, M. Mignotte, R. Tijdeman, M. Bennett, P. Voutier, Y. Bugeaud, T.N. Shorey, S. Laishram.

Baker's method involving linear forms in logarithms

One main concern is that Schmidt's subspace Theorem (as well as the Theorem of Thue– Siegel– Roth) is non–effective : upper bounds for the number of solutions can be derived, but no upper bound for the solutions themselves.
Only the case of a S–unit equation

$$\epsilon_1 + \epsilon_2 + \epsilon_3 = 0$$

can be solved effectively by means of Baker's method.

Work of A.O. Gel'fond, A. Baker, K. Győry, M. Mignotte, R. Tijdeman, M. Bennett, P. Voutier, Y. Bugeaud, T.N. Shorey, S. Laishram.

Baker's method involving linear forms in logarithms

One main concern is that Schmidt's subspace Theorem (as well as the Theorem of Thue– Siegel– Roth) is non–effective : upper bounds for the number of solutions can be derived, but no upper bound for the solutions themselves.
Only the case of a S–unit equation

$$\epsilon_1 + \epsilon_2 + \epsilon_3 = 0$$

can be solved effectively by means of Baker's method.

Work of A.O. Gel'fond, A. Baker, K. Győry, M. Mignotte, R. Tijdeman, M. Bennett, P. Voutier, Y. Bugeaud, T.N. Shorey, S. Laishram.

COMSATS IIT, Lahore Campus March 12, 2013

Diophantine approximation and Diophantine equations : old and new

Michel Waldschmidt

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