vendredi 16 juin 2013

Séminaire de Théorie des Nombres
Département de mathématiques et de statistique
Université Laval Québec.

Sur les équations diophantiennes : du vieux et du neuf.

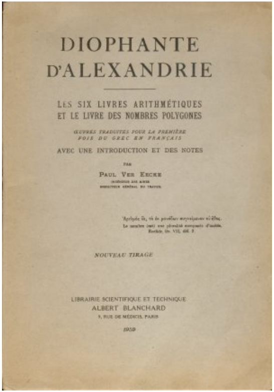
Michel Waldschmidt
Université P. et M. Curie (Paris 6)

Le fichier pdf de cet exposé est téléchargeable sur le site
http://www.math.jussieu.fr/∼miw/

Abstract

The study of Diophantine equations is among the oldest topics investigated by mathematicians. It is known that some problems will never be solved, yet fundamental progress has been achieved recently.
We survey some of the main results and some of the main conjectures.

Diophantus of Alexandria (250 ±50)



DIOPHANTE
D'ALEXANDRIE

LES SIX LIVRES ARITHMÉTIQUES
ET LE LIVRE DES NOMBRES POLYGONES

ŒUVRES TRADUITES POUR LA PREMIÈRE
FOIS DU GREC EN FRANÇAIS

AVEC UNE INTRODUCTION ET DES NOTES

PAR

PAUL VER EECKE

NOUVEAU TIRAGE

LIBRAIRIE SCIENTIFIQUE ET TECHNIQUE
ALBERT BLANCHARD
9, RUE DE MÉDICIS, PARIS

Diophantine equations

A Diophantine equation is an equation of the form

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

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

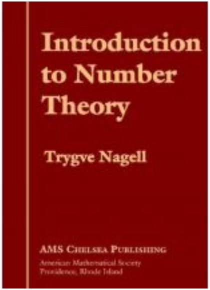
Joseph Louis Lagrange (1736 - 1813)

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 :

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

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

$x^2 + D = 2^n$

F. Beukers (1980) : at most one solution otherwise.

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

Hilbert's 8th Problem

August 8, 1900

David Hilbert (1862 - 1943)

Second International Congress of Mathematicians in Paris.

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

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

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

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

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

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

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

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

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

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 on algebraic curves

Siegel's Theorem (1929) : integral points on algebraic curves

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 on algebraic curves

Siegel's Theorem (1929) : integral points on algebraic curves

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 on algebraic curves

Siegel's Theorem (1929) : integral points on algebraic curves

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 on algebraic curves

Siegel's Theorem (1929) : integral points on algebraic curves

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 on algebraic curves

Siegel's Theorem (1929) : integral points on algebraic curves

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 on algebraic curves

Siegel's Theorem (1929) : integral points on algebraic curves

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.

Open problem : effectivity

Faltings's Theorem is not effective : quantitative versions (upper bounds for the number of solutions) are known (G. Rémond), but so far there is no known effective bound for the solutions $(x, y) \in \mathbf{Q}^2$ of a Diophantine equation $f(x, y) = 0$, where $f \in \mathbf{Z}[X, Y]$ is a polynomial such that the curve $f(x, y) = 0$ has genus ≥ 1.

Even for integral points, there is no effective version of Siegel's Theorem on integral points on a curve of genus ≥ 2.

Open problem : effectivity

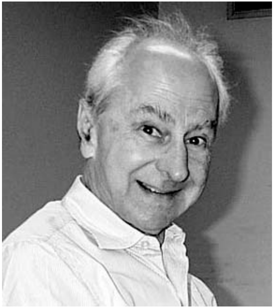
Faltings's Theorem is not effective : quantitative versions (upper bounds for the number of solutions) are known (G. Rémond), but so far there is no known effective bound for the solutions $(x, y) \in \mathbf{Q}^2$ of a Diophantine equation $f(x, y) = 0$, where $f \in \mathbf{Z}[X, Y]$ is a polynomial such that the curve $f(x, y) = 0$ has genus ≥ 1.

Even for integral points, there is no effective version of Siegel's Theorem on integral points on a curve of genus ≥ 2.

Paul Vojta

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

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) :

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

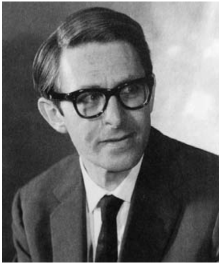
- any $\kappa > (d/2) + 1$ by A. Thue (1909),
- $2\sqrt{d}$ by C.L. Siegel in 1921,
- $\sqrt{2d}$ by F.J. Dyson and A.O. Gel'fond in 1947,
- any $\kappa > 2$ by K.F. Roth in 1955.

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

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

In other terms, the set of $(q, p) \in \mathbf{Z}^2 \setminus \{(0,0)\}$ where the two independent linear forms

$$L_0(x_0, x_1) = x_0, \qquad L_1(x_0, x_1) = x_0\alpha - x_1$$

satisfy

$$|L_0(x_0, x_1)L_1(x_0, x_1)| \leq \max\{|x_0|, |x_1|\}^{-\epsilon}$$

is contained in a finite union of lines in $\mathbf{Q}^2$.

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

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

In other terms, the set of $(q, p) \in \mathbf{Z}^2 \setminus \{(0, 0)\}$ where the two independent linear forms

$$L_0(x_0, x_1) = x_0, \qquad L_1(x_0, x_1) = x_0\alpha - x_1$$

satisfy

$$|L_0(x_0, x_1)L_1(x_0, x_1)| \leq \max\{|x_0|, |x_1|\}^{-\epsilon}$$

is contained in a finite union of lines in $\mathbf{Q}^2$.

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

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

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

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.

Thue equation

For any number field K, for any non–zero element m 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

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

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

Thue–Mahler equation

Let K be a number field, G a finitely generated subgroup of $K^\times$, $\alpha_1, \ldots, \alpha_n$ elements in K with $\mathrm{Card}\{\alpha_1, \ldots, \alpha_n\} \geq 3$. Then there are only finitely many $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ satisfying the Thue–Mahler equation

$$(x - \alpha_1 y) \cdots (x - \alpha_n y) \in G.$$

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 $S = \{p_1, \dots, p_s\}$ 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 $S = \{p_1, \dots, p_s\}$ 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 $-1, p_1, \dots, p_s$.

Conversely, if G is a finitely generated subgroup of $\mathbf{Q}^\times$, then there exists a finite set $S = \{p_1, \dots, p_s\}$ 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 $g_1, \dots, g_t$ 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 $-1, p_1, \ldots, p_s$.

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 $-1, p_1, \ldots, p_s$.

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 $-1, p_1, \ldots, p_s$.

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.

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, 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).

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, 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).

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

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

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

A. Togbé considered the family of equations

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

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) :

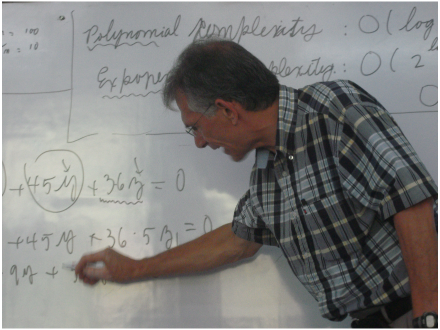
$$\prod_{i=1}^{n}(X - p_i(a)Y) - Y^n = \pm 1,$$

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 finitely generated subgroup of $K^\times$, we produce families of curves related to the units of the number field, having only trivial integral points.



Families of Thue–Mahler equations

Let K be a number field and $d = [K : \mathbf{Q}]$ its degree. Let G a finitely generated subgroup of $K^\times$. For each $\varepsilon \in G$ 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. Then the set

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

is finite.

Families of Thue–Mahler equations

Let K be a number field and $d = [K : \mathbf{Q}]$ its degree. Let G a finitely generated subgroup of $K^\times$. For each $\varepsilon \in G$ 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. Then the set

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

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.

Denote by $\mathbf{Z}_K^\times$ the group of units of K. For $\varepsilon \in \mathbf{Z}_K^\times$, $f_\varepsilon(X)$ 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

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

satisfies

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

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

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

Let $m \geq 1$. The goal is to 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

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

Let $m \geq 1$. The goal is to 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

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

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

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

Let $m \geq 1$. The goal is to 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

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

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

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

Generalized S–unit equation

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.

Generalized S–unit equation

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.

Generalized S–unit equation

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.

vendredi 16 juin 2013

Séminaire de Théorie des Nombres
Département de mathématiques et de statistique
Université Laval Québec.

Sur les équations diophantiennes : du vieux et du neuf.

Michel Waldschmidt
Université P. et M. Curie (Paris 6)

Le fichier pdf de cet exposé est téléchargeable sur le site
http://www.math.jussieu.fr/∼miw/