November 15, 2022

UM-DAE Centre for Excellence in Basic Sciences (CBS)

Families of Diophantine equations

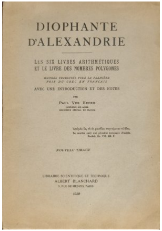
Michel Waldschmidt

Professeur Émérite, Sorbonne Université,
Institut de Mathématiques de Jussieu, Paris
http://www.imj-prg.fr/~michel.waldschmidt/

Abstract

Given a polynomial in several variables with rational integer coefficients, we investigate the set of integer tuples where this polynomial vanishes. The best know example is Fermat’s equation $x^n + y^n = z^n$. Another family is given by the so–called Pell–Fermat equations $x^2 - dy^2 = \pm 1$ already considered by Brahmagupta (598 - 670) and Bhaskaracharya (1114 - 1185). After a short historical survey on this subject starting with Hilbert’s 10th Problem, we describe the state of the art concerning integer points on curves $f(x, y) = k$, including work of Thue, Siegel, Gel’fond, Baker, Schmidt. We conclude with new results on families of such Diophantine equations.

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
INGÉNIEUR DES MINES
DIRECTEUR GÉNÉRAL DU TRAVAIL

Ἀριθμὸς δέ, τὸ ἐκ μονάδων συγκείμενον πλῆθος.
Le nombre (est) une pluralité composée d'unités.
Euclide, liv. VII, déf. 2.

NOUVEAU TIRAGE

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

1959

Pythagoras equation $x^2 + y^2 = z^2$ (ref. : Hardy and Wright)

Diophantine quadruples : $(1, 3, 8, 120)$ $xy + 1$ is a square :
$4 = 2^2$, $9 = 3^2$, $121 = 11^2$, $25 = 5^2$, $361 = 19^2$, $961 = 31^2$.

G. H. Hardy and E. M. Wright, An introduction to the theory of numbers,
Oxford University Press, Oxford, sixth ed., 2008.
Revised by D. R. Heath-Brown and J. H. Silverman.

Brahmagupta (598 – 670)

Brahmasphutasiddhanta : Solve in integers the equation

$$x^2 - 92y^2 = 1$$

The smallest solution is

$$x = 1151, \qquad y = 120.$$

Composition method : *samasa* – Brahmagupta identity

$$(a^2 - db^2)(x^2 - dy^2) = (ax + dby)^2 - d(ay + bx)^2.$$

`http://mathworld.wolfram.com/BrahmaguptasProblem.html`

`http://www-history.mcs.st-andrews.ac.uk/HistTopics/Pell.html`

Bhaskara II or Bhaskaracharya (1114 - 1185)

Lilavati Ujjain (India)

Bijaganita, (1150)

$$x^2 - 61y^2 = 1$$

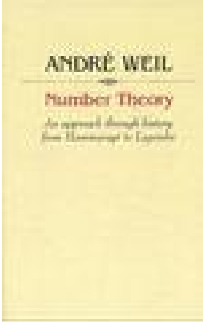
$$x = 1\,766\,319\,049, \qquad y = 226\,153\,980.$$

Cyclic method *Chakravala* : produces a solution to Pell's equation $x^2 - dy^2 = 1$ starting from a solution to $a^2 - db^2 = k$ with a *small* k.

http://www-history.mcs.st-andrews.ac.uk/HistTopics/Pell.html

Reference to Indian mathematics

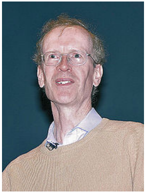
André Weil
Number theory :
An approach through history. From Hammurapi to Legendre.
Birkhäuser Boston, Inc., Boston, Mass., (1984) 375 pp.
`MR 85c:01004`



Pierre de Fermat

Pierre de Fermat

1601–1665



Andrew Wiles

Proof of Fermat's last Theorem by Andrew Wiles (1993) : for $n \geq 3$, there is no positive integer solution (a, b, c) to

$$a^n + b^n = c^n.$$

Ramanujan – Nagell Equation

Srinivasa Ramanujan
1887 – 1920

Trygve Nagell
1895 – 1988

Ramanujan – Nagell Equation

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

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

$x^2 + D = 2^n$

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.

Roger Apéry
1916 – 1994

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.

Frits Beukers

Mike Bennett

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

Diophantine equations : early historical survey

Pierre Fermat (1601 ? – 1665)

Leonhard Euler (1707 – 1783)

Joseph Louis Lagrange (1736 – 1813)

XIXth Century : Adolf Hurwitz, Henri Poincaré

Hilbert's 8th Problem

David Hilbert

1862 – 1943

Second International Congress of Mathematicians in Paris. August 8, 1900

Twin primes,

Goldbach's Conjecture,

Riemann Hypothesis

http://www.maa.org/sites/default/files/pdf/upload$_-$library/22/Ford/Thiele1-24.pdf

Hilbert's tenth problem

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

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

Negative solution to Hilbert's 10th problem

Julia Robinson (1952)

Julia Robinson, Martin Davis, Hilary Putnam (1961)

Yuri Matijasevic (1970)

Remark : the analog for *rational points* of Hilbert's 10th problem is not yet solved :
Does there exist an algorithm in order to decide whether a Diophantine equation has a rational solution or not ?

Diophantine equations : historical survey

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

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

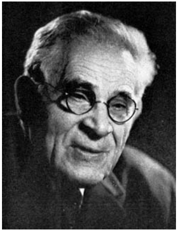
when F is homogeneous irreducible form over $\mathbb{Q}$ of degree ≥ 3.

Mordell's Conjecture (1922) : rational points on algebraic curves

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

Axel Thue

1863 - 1922



Louis Mordell

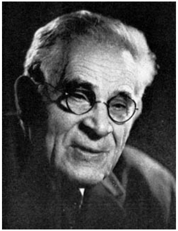
1888 – 1972

Carl Ludwig Siegel

1896 - 1981

Mordell's Conjecture, Faltings's Theorem

Mordell's Conjecture : 1922. Faltings's Theorem (1983).
The set of rational points on a number field of a curve of genus ≥ 2 is finite.



Louis Mordell
1888 – 1972

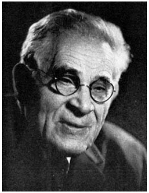
Gerd Faltings

The group of rational points on an elliptic curve

Conjecture (Henri Poincaré, 1901) : finitely many points are sufficient to deduce all rational points by the chord and tangent method.

Henri Poincaré

1854 – 1912



Louis Mordell

1888 – 1972

Theorem (Mordell, 1922). *If E is an elliptic curve over $\mathbb{Q}$, then the abelian group $E(\mathbb{Q})$ is finitely generated : there exists a nonnegative integer r (the Mordell-Weil* rank *of the curve over $\mathbb{Q}$) such that*

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r$$

Mordell–Weil Theorem

André Weil (1928) : generalization to number fields and abelian varieties :

If A is an Abelian variety over a number field K, then the abelian group $A(K)$ is finitely generated :

$$A(K) = A(K)_{\mathrm{tors}} \times \mathbb{Z}^r$$

with $r \geq 0$ while $A(K)_{\mathrm{tors}}$ is a finite group.

Jacques Hadamard

1865 - 1963

André Weil

1906 – 1998

Weil's thesis : 1928. Hadamard's comment.

Reference : ANTOINE CHAMBERT-LOIR. *La conjecture de Mordell : origines, approches, généralisations.* Séminaire Betty B., Septembre 2021 5e année, 2021–2022

Axel Thue

Axel Thue

1863 - 1922

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

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

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

Liouville's inequality (1844)

Liouville's inequality . *Let* α *be an algebraic number of degree* $d \geq 2$. *There exists* $c(\alpha) > 0$ *such that, for any* $p/q \in \mathbb{Q}$ *with* $q > 0$,

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

Joseph Liouville

1809–1882

Liouville's estimate for $\sqrt[3]{2}$:

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

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{6q^3}.$$

Proof.
Since $\sqrt[3]{2}$ is irrational, for p and q rational integers with $q > 0$, we have $p^3 - 2q^3 \neq 0$, hence

$$|p^3 - 2q^3| \geq 1.$$

Write

$$p^3 - 2q^3 = (p - \sqrt[3]{2}q)(p^2 + \sqrt[3]{2}pq + \sqrt[3]{4}q^2).$$

If $p \leq (3/2)q$, then

$$p^2 + \sqrt[3]{2}pq + \sqrt[3]{4}q^2 < 6q^2.$$

Hence

$$1 \leq 6q^2|p - \sqrt[3]{2}q|.$$

Liouville's estimate for $\sqrt[3]{2}$:

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

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{6q^3}.$$

Proof.
We completed the proof in the case $p \le (3/2)q$.
If $p > (3/2)q$, then

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{3}{2} - \sqrt[3]{2} > \frac{1}{6}.$$

Improving Liouville's inequality

If we can improve the lower bound

$$|p^3 - 2q^3| \geq 1,$$

then we can improve Liouville's estimate

$$\left| \sqrt[3]{2} - \frac{p}{q} \right| > \frac{1}{6q^3}.$$

What turns out to be much more interesting is the converse :
If we can improve Liouville's estimate

$$\left| \sqrt[3]{2} - \frac{p}{q} \right| > \frac{1}{6q^3},$$

then we can improve the lower bound

$$|p^3 - 2q^3| \geq 1.$$

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.

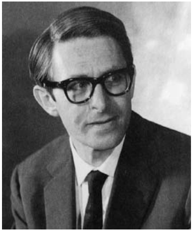
Thue– Siegel– Roth Theorem

Axel Thue

1863 - 1922

Carl Ludwig Siegel

1896 - 1981



Klaus Friedrich Roth

1925 – 2015

For any real algebraic number α, for any $\epsilon > 0$, the set of $p/q \in \mathbb{Q}$ 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 $p/q \in \mathbb{Q}$ with $q \geq q_0$, we have

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

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

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

Mike Bennett http://www.math.ubc.ca/~bennett/

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

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

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

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

Connection between Diophantine approximation and Diophantine equations

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

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

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

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

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

Thue's equation and approximation

Let $f \in \mathbb{Z}[X]$ 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 $(x,y) \in \mathbb{Z}^2$ verifying

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

is finite.

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

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

is finite.

Thue equation

Condition (i) above :

> *For any integer $k \neq 0$, the set of $(x, y) \in \mathbb{Z}^2$ verifying*
>
> $$F(x, y) = k$$
>
> *is finite.*

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

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

is finite.

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

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

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

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

Wolfgang M. Schmidt

Effectivity

The Theorem of Thue–Siegel–Roth–Schmidt is not effective : upper bounds for the number of solutions can be derived, but no upper bound for the solutions themselves.

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

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

Number of solutions

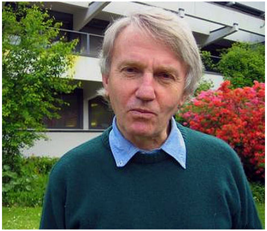
G. Rémond (2000) : explicit upper bound for the number of solutions in Faltings's Theorem.

Gaël Rémond

Effective version of Siegel's Theorem (genus 1)

A. Baker and J. Coates. Integer points on curves of genus 1. Proc. Camb. Philos. Soc. 67, 595–602 (1970).

Alan Baker
1939 – 2018



John Coates
(1945 – 2022)

Gel'fond–Baker method

While Thue's method was based on the non effective Thue–Siegel–Roth Theorem, Baker and Fel'dman followed an effective method introduced by A.O. Gel'fond, involving *lower bounds for linear combinations of logarithms of algebraic numbers with algebraic coefficients.*

Alexandre Ossipovitch Gel'fond

1906–1968

Alan Baker

1939 – 2018

Lower bound for linear combinations of logarithms

A lower bound for a nonvanishing difference

$$ {\alpha_1}^{b_1} \cdots {\alpha_n}^{b_n} - 1 $$

is essentially the same as a lower bound for a nonvanishing number of the form

$$ b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n, $$

since $e^z - 1 \sim z$ for $z \to 0$.
The first nontrivial lower bounds were obtained by A.O. Gel'fond. His estimates were effective only for $n = 2$: for $n \geq 3$, he needed to use estimates related to the Thue–Siegel–Roth Theorem.

Explicit version of Gel'fond's estimates

A. Schinzel (1968) computed explicitly the constants introduced by A.O. Gel'fond. in his lower bound for

$$\left|\alpha_1{}^{b_1}\alpha_2{}^{b_2} - 1\right|.$$

Andrzej Schinzel
1937–1921

He deduced explicit Diophantine results using the approach introduced by A.O. Gel'fond.

Alan Baker (1939 – 2018)

Alan Baker

1939 – 2018

In 1968, A. Baker succeeded to extend to any $n \geq 2$ the transcendence method used by A.O. Gel'fond for $n = 2$. As a consequence, effective upper bounds for the solutions of Thue's equations have been derived.

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 $x^n - dy^n = 1$

B. Delaunay (Delone), 1930 : for d a cubefree integer, the equation $x^3 - dy^3 = 1$ has at most 2 solutions in $\mathbb{Z}$.

W. Ljunggren, 1937 : for d an integer, the equation $x^4 - dy^4 = 1$ has at most one solution in positive integers x, y.

M. A. Bennett, B.M.M. de Weger, 1998, 2001 : for a, b with $ab \neq 0$ and $n \geq 3$, the equation $|ax^n - by^n| = 1$ has at most one solution in positive integers x, y.

Boris Delaunay

1890 – 1980

Wilhelm Ljunggren

1905 – 1973

Mike Bennett

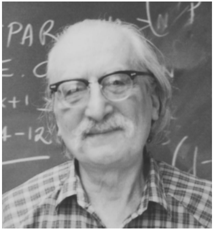
Benne de Weger

Davide Lombardo. A family of quintic Thue equations via Skolem's p-adic method. Riv. Mat. Univ. Parma, Vol. 13, No. 1, 2022, 161–173.
http://www.rivmat.unipr.it/vols/2022-13-1/09-lombardo.html

The simplest cubic fields of D. Shanks

The simplest cubic fields are the cyclic fields, those having square discriminants :

$$D = N^2.$$



Daniel Shanks

1917 – 1996

Like the quadratic fields, but unlike other cubic fields, all roots of the generating polynomial are in the field, all primes q either split completely in the field or do not split at all, and the residue class of $q \pmod{N}$ determines whether q splits or does not.

The simplest cubic fields

The cubic equation

$$x^3 = ax^2 + (a+3)x + 1$$

has the discriminant

$$D = (a^2 + 3a + 9)^2.$$

Daniel Shanks
The Simplest Cubic Fields.
Math. of Computation, **28** 128 (1974) 1137 – 1152.

Marie-Nicole Gras

Marie-Nicole Gras

Marie–Nicole Montouchet.
Sur le Nombre de Classes du Sous-Corps Cubique de $\mathbb{Q}^{(p)}$, ($p \equiv 1 \mod 3$).
Thesis, Grenoble, 1971. Sém. Théorie Nombres 1971-1972, Univ. Bordeaux, No. 2bis, 9 p. (1972).

Marie–Nicole Gras,
Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unités des extensions cubiques cycliques de $\mathbb{Q}$.
J. Reine Angew. Math. **277**, 89 – 116 (1975).

Families of Thue equations (continued)

Emery Thomas
1927 – 2005

E. Thomas in 1990 studied the families of equations $F_n(X,Y) = 1$ associated with D. Shanks' simplest cubic fields, viz.

$$F_n(X,Y) = X^3 - (n-1)X^2Y - (n+2)XY^2 - Y^3.$$

Thomas's family

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

For the same form

$$F_n(X, Y) = X^3 - (n-1)X^2Y - (n+2)XY^2 - Y^3,$$

all solutions of the Thue inequality $|F_n(X, Y)| \leq 2n + 1$ have been found by M. Mignotte A. Pethő and F. Lemmermeyer (1996).

Maurice Mignotte

Attila Pethő

Franz Lemmermeyer

Twisting Thomas's family

Write

$$\begin{aligned} F_n(X,Y) &= X^3-(n-1)X^2Y-(n+2)XY^2-Y^3 \\ &= (X-\lambda_0)(X-\lambda_1)(X-\lambda_2) \end{aligned}$$

with

$$\lambda_0, \quad \lambda_1 = -\frac{1}{\lambda_0+1} \quad \text{and} \quad \lambda_2 = -\frac{\lambda_0+1}{\lambda_0}$$

$$\lambda_0 > 0 > \lambda_1 > -1 > \lambda_2.$$

For $a \in \mathbb{Z} \setminus \{0\}$, the binary cubic form

$$F_{n,a}(X,Y) = (X-\lambda_0^a Y)(X-\lambda_1^a Y)(X-\lambda_2^a Y)$$

is irreducible in $\mathbb{Z}[X,Y]$, the minimal (irreducible) polynomial of λ_0^a being $F_{n,a}(X,1)$.

Twisting Thomas's family

Joint work with Claude Levesque
A family of Thue equations involving powers of units of the simplest cubic fields.
J. Théor. Nombres Bordeaux, **27** (2015), pp. 537–563.

Claude Levesque

Theorem. *If* $|F_{n,a}(x,y)| = \pm 1$ *with* $\max\{|x|,|y|\} \geq 2$, *we have*

$$\max\{|n|,|a|,|x|,|y|\} \leq c$$

where c *is a positive effectively computable positive constant.*

Question : *Is-it true that*

$$n \leq 4, \quad |a| \leq 5, \quad |x| \leq 19, \quad |y| \leq 7 \ ?$$

Open problem

Let $c \in \{+1, -1\}$ and let $n, a \in \mathbb{N}$ with $a \geq 1$. We wonder whether all the solutions $(x, y) \in \mathbb{Z}^2$ of $F_{n,a}(x, y) = c$ are given by

- $(c, 0),\ (0, c)$ for any $n \geq 0$ and $a \geq 1$,
- $(-c, c)$ for any $n \geq 0$ and $a = 1$,
- (c, c) for $n = 0$ and $a = 2$,
- $(-c, -c)$ for $n = 0$ and $a = 1$,
- the exotic solutions

(n, a)	(cx, cy)					
$(0, 1)$	$(-9, 5)$	$(-1, 2)$	$(2, -1)$	$(4, -9)$	$(5, 4)$	
$(0, 2)$	$(-14, -9)$	$(-3, -1)$	$(-2, -1)$	$(1, 5)$	$(3, 2)$	$(13, 4)$
$(0, 3)$	$(2, 1)$					
$(0, 5)$	$(-3, -1)$	$(19, -1)$				
$(1, 1)$	$(-3, 2)$	$(1, -3)$	$(2, 1)$			
$(1, 2)$	$(-7, -2)$	$(-3, -1)$	$(2, 1)$	$(7, 3)$		
$(2, 2)$	$(-7, -1)$	$(-2, -1)$				
$(3, 1)$	$(-7, -2)$	$(-2, 9)$	$(9, -7)$			
$(4, 2)$	$(3, 2)$					

Families of Thue equations (continued)

Family of quartic equations :

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

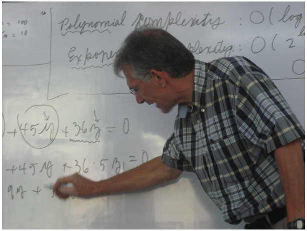
(A. Pethő 1991 , M. Mignotte, A. Pethő and R. Roth, 1996).
The left hand side is $X(X-Y)(X+Y)(X-aY)+Y^4$.
Further work on equations of degrees up to 8 by J.H. Chen, I. Gaál, C. Heuberger, B. Jadrijević, G. Lettl, C. Levesque, M. Mignotte, A. Pethő, R. Roth, R. Tichy, E. Thomas, A. Togbé, P. Voutier, I. Wakabayashi, P. Yuan, V. Ziegler...
Surveys by I. Wakabayashi (2002) and C. Heuberger (2005).

Isao Wakabayashi

Clemens Heuberger

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 joint works with Claude Levesque, for each number field K of degree at least three we produce families of curves related to the units of the number field, having only trivial integral points.
(Also for S–integral points).



Using Schmidt's Subspace Theorem

Let K be a number field, $n \geq 3$ an integer, $\alpha_1, \ldots, \alpha_n$ elements of $K^\times$ and $f \in K[X, Y]$ the binary form

$$f(X,Y) = \bigl(X - \alpha_1 Y\bigr)\bigl(X - \alpha_2 Y\bigr) \cdots \bigl(X - \alpha_n Y\bigr).$$

Denote by $\mathbb{Z}_K$ the ring of integers of K and by $\mathbb{Z}_K^\times$ the group of units. For $\underline{\varepsilon} = (\varepsilon_1, \ldots, \varepsilon_n) \in (\mathbb{Z}_K^\times)^n$, let $f_{\underline{\varepsilon}} \in K[X, Y]$ denote the binary form

$$f_{\underline{\varepsilon}}(X,Y) = (X - \alpha_1\varepsilon_1 Y)(X - \alpha_2\varepsilon_2 Y) \cdots (X - \alpha_n\varepsilon_n Y).$$

Let $\mathcal{E}$ denote the set of elements $\underline{\varepsilon}$ in $(\mathbb{Z}_K^\times)^n$ such that $\varepsilon_1 = 1$ and $\mathrm{Card}\{\alpha_1\varepsilon_1, \alpha_2\varepsilon_2, \ldots, \alpha_n\varepsilon_n\} \geq 3$. Then there exists a finite subset $\mathcal{E}^\star$ de $\mathcal{E}$ such that, for all $\underline{\varepsilon} \in \mathcal{E} \setminus \mathcal{E}^\star$ and for all $(x, y) \in \mathbb{Z}_K \times \mathbb{Z}_K$, the condition

$$f_{\underline{\varepsilon}}(x, y) \in \mathbb{Z}_K^\times$$

implies $xy = 0$.

Example

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

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

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

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

is finite.

A conjecture

The previous result rests on Schmidt's Subspace Theorem and is not effective. Using Baker's method, we proved several cases of the following conjecture.

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

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

Conjecture. *There exists an effectively computable constant $\kappa > 0$, depending only on K, such that, for any $m \geq 2$, any (x,y,ε) in the set*

$$\bigl\{(x,y,\varepsilon) \in \mathbb{Z}^2 \times \mathbb{Z}_K^\times \ \mid \ xy \neq 0,\ \mathbb{Q}(\varepsilon) = K,\ |F_\varepsilon(x,y)| \leq m\bigr\}$$

satisfies

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

A few special cases

- True for a sufficiently large set of units ε.

- Almost totally imaginary number fields (at most one real embedding)

- Cubic fields.

- Rank one subgroup of units.

Sketch of proof

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

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

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

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

Sketch of proof (continued)

For $j = 1, \dots, d$, 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 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 three terms Siegel 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.

Simplest cubic, quartic and sextic fields

Let t be an integer parameter. The infinite parametric families of number fields generated by the roots of the polynomials

$$f_t^{(3)}(x) = x^3 - (t-1)x^2 - (t+2)x - 1, \quad (t \in \mathbb{Z}),$$

$$f_t^{(4)}(x) = x^4 - tx^3 - 6x^2 + tx + 1, \quad (t \in \mathbb{Z} \setminus \{-3, 0, 3\}),$$

$$f_t^{(6)}(x) = x^6 - 2tx^5 - (5t+15)x^4 - 20x^3 + 5tx^2 + (2t+6)x + 1, \\ (t \in \mathbb{Z} \setminus \{-8, -3, 0, 5\}),$$

are called simplest cubic, simplest quartic and simplest sextic fields, respectively.
They are extensively studied in algebraic number theory, starting with D.Shanks in the cubic case.

Simplest quartic and simplest sextic fields

It was shown by G. Lettl, A. Pethő and P. Voutier that these are all parametric families of number fields which are totally real cyclic with Galois group generated by a mapping of type

$$x \mapsto \frac{ax+b}{cx+d}$$

with $a, b, c, d \in \mathbb{Z}$.

István Gaál, Borka Jadrijević, László Remete.
Simplest quartic and simplest sextic Thue equations over imaginary quadratic fields.
Int. J. Number Theory **15**, No. 1, 11 – 27 (2019).

The hypergeometric method

The hypergeometric method has been used for solving the family of Diophantine equations arising from the simplest quartic and sextic fields.

Isao Wakabayashi

Paul Voutier

The associated families of twisted equations have not yet been investigated.

November 15, 2022

UM-DAE Centre for Excellence in Basic Sciences (CBS)

Families of Diophantine equations

Michel Waldschmidt

Professeur Émérite, Sorbonne Université,
Institut de Mathématiques de Jussieu, Paris
http://www.imj-prg.fr/~michel.waldschmidt/