Mahidol University International College
Applied Mathematics Program

November 17, 2016

Lecture on Families of Diophantine equations

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

http://www.imj-prg.fr/~michel.waldschmidt/

Abstract

In a series of recent joint papers with Claude Levesque, we produce new families of Diophantine equations for which effective methods can be applied to solve them. We present a survey of this work.

Diophantus of Alexandria

Thue's Theorem (1908)

Let $F \in \mathbf{Z}[X, Y]$ be a homogeneous irreducible form of degree $d \geq 3$:

$$F(X, Y) = a_0X^d + a_1X^{d-1}Y + \cdots + a_{d-1}XY^{d-1} + a_dY^d.$$

Axel Thue
(1863 – 1922)

Let $k \in \mathbf{Z}$, $k \neq 0$. Then there are only finitely many integer solutions $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ to the Diophantine equation

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

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

On Thue's equations and approximation

When $f \in \mathbf{Z}[X]$ is a polynomial of degree d, we let $F(X, Y) = Y^d f(X/Y)$ denote the associated homogeneous binary form of degree d.
Assume f is irreducible. 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 $c > 0$ and for any root $\alpha \in \mathbf{C}$ of f, the set of rational numbers p/q verifying

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

is finite.

Improvements of Liouville's inequality

In the lower bound

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

for a real algebraic number α of degree $d \geq 2$, the exponent d of q in the denominator is best possible for $d = 2$, not for $d \geq 3$.

In 1909, A. Thue succeeded to prove that it can be replaced by κ with any $\kappa > (d/2) + 1$.

Thue's inequality

Let α be an algebraic number of degree $d \geq 3$ and let $\kappa > (d/2) + 1$. Then there exists $c(\alpha, \kappa) > 0$ such that, for any $p/q \in \mathbf{Q}$ with $q > 0$,

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

Thue inequation

Thue's result

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 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 $(x, y) \in \mathbf{Z} \times \mathbf{Z}$.

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

- 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 $p/q \in \mathbf{Q}$ with $|\alpha - p/q| < q^{-2-\epsilon}$ 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

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

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

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

W.M. Schmidt

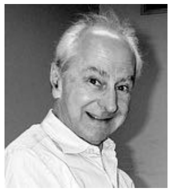
Subspace Theorem

W.M. Schmidt

H.P. Schlickewei

Consequences of the Subspace Theorem

Work of P. Vojta, S. Lang, J-H. Evertse, K. Győry, P. Corvaja, U. Zannier, Y. Bilu, P. Autissier, A. Levin ...





Gel'fond–Baker method

The Thue–Siegel–Roth Theorem is not effective: upper bounds for the number of solutions can be derived, but not upper bounds for the solutions.

Baker and Fel'dman developed an effective method introduced by A.O. Gel'fond, involving *lower bounds for linear combinations of logarithms of algebraic numbers with algebraic coefficients.*


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

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

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

Alan Baker

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.

Thue's equation and Siegel's unit equation

The main idea behind the Gel'fond–Baker approach for solving Thue's equation is to exploit Siegel's unit equation.
Assume $\alpha_1, \alpha_2, \alpha_3$ are algebraic integers and x, y rational integers such that

$$(x - \alpha_1 y)(x - \alpha_2 y)(x - \alpha_3 y) = 1.$$

Then the three numbers

$$u_1 = x - \alpha_1 y, \quad u_2 = x - \alpha_2 y, \quad u_3 = x - \alpha_3 y,$$

are units. Eliminating x and y, one deduces *Siegel's unit equation*

$$u_1(\alpha_2 - \alpha_3) + u_2(\alpha_3 - \alpha_1) + u_3(\alpha_1 - \alpha_2) = 0.$$

Siegel's unit equation

Write Siegel's unit equation

$$u_1(\alpha_2 - \alpha_3) + u_2(\alpha_3 - \alpha_1) + u_3(\alpha_1 - \alpha_2) = 0$$

in the form

$$\frac{u_1(\alpha_2 - \alpha_3)}{u_2(\alpha_1 - \alpha_3)} - 1 = \frac{u_3(\alpha_1 - \alpha_2)}{u_2(\alpha_1 - \alpha_3)}.$$

The quotient

$$\frac{u_1(\alpha_2 - \alpha_3)}{u_2(\alpha_1 - \alpha_3)}$$

is the quantity

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

in Gel'fond–Baker Diophantine inequality.

Work on Baker's method:

A. Baker (1968), N.I. Feldman (1971), V.G. Sprindžuck and H.M. Stark (1973), K. Győry and Z.Z. Papp (1983), E. Bombieri (1993), Y. Bugeaud and K. Győry (1996), Y. Bugeaud (1998)...

Solving Thue equations:
A. Pethő and R. Schulenberg (1987), B. de Weger (1987), N. Tzanakis and B. de Weger (1989), Y. Bilu and G. Hanrot (1996), (1999)...

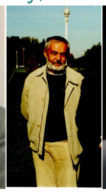
Solving Thue–Mahler equations:
J.H. Coates (1969), S.V. Kotov and V.G. Sprindžuk (1973), A. Bérczes–Yu Kunrui– K. Győry (2006)...

Diophantine equations

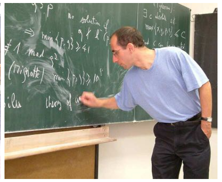
A.O. Gel'fond, A. Baker, V. Sprindžuk, K. Győry, M. Mignotte, R. Tijdeman,
M. Bennett, P. Voutier, Y. Bugeaud, T.N. Shorey, S. Laishram...









N. Saradha, T.N. Shorey, R. Tijdeman



Survey by T.N. Shorey
Diophantine approximations, Diophantine equations, transcendence and applications.

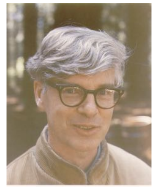
Families of Thue equations

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 $a \geq 1$. He used a lower bound for linear combinations of logarithms of algebraic numbers due to T.N. Shorey.

E. Thomas's family of Thue equations



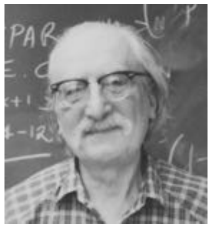
E. Thomas in 1990 studied the families of Thue equations
$x^3 - (n-1)x^2y - (n+2)xy^2 - y^3 = 1$

Set

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

The cubic fields $\mathbf{Q}(\lambda)$ generated by a root λ of $F_n(X,1)$ are called by D. Shanks the *simplest cubic fields*. The roots of the polynomial $F_n(X,1)$ can be described via homographies of degree 3.

D. Shanks's simplest cubic fields $\mathbf{Q}(\lambda)$.



Let λ be one of the three roots of

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

Then $\mathbf{Q}(\lambda)$ is a real Galois cubic field.

Write

$$F_n(X,Y) = (X - \lambda_0 Y)(X - \lambda_1 Y)(X - \lambda_2 Y)$$

with

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

Then

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

Simplest fields.

When the following polynomials are irreducible for $s, t \in \mathbf{Z}$, the fields $\mathbf{Q}(\omega)$ generated by a root ω of respectively

$$\begin{cases} sX^3 - tX^2 - (t+3s)X - s, \\ sX^4 - tX^3 - 6sX^2 + tX + s, \\ sX^6 - 2tX^5 - (5t+15s)X^4 - 20sX^3 + 5tX^2 + (2t+6s)X + s, \end{cases}$$

are cyclic over $\mathbf{Q}$ of degree 3, 4 and 6 respectively.
For $s = 1$, they are called *simplest fields* by many authors.
For $s \geq 1$, I. Wakabayashi call them *simplest fields*.

In each of the three cases, the roots of the polynomials can be described via homographies of $PSL_2(\mathbf{Z})$ of degree 3, 4 and 6 respectively.

E. Thomas's family of Thue equations

In 1990, E. Thomas proved in some effective way that the set of $(n, x, y) \in \mathbf{Z}^3$ with

$$n \geq 0, \quad \max\{|x|, |y|\} \geq 2 \quad \text{and} \quad F_n(x, y) = \pm 1$$

is finite.

In his paper, he completely solved the equation $F_n(x, y) = 1$ for $n \geq 1.365 \cdot 10^7$: the only solutions are $(0, -1)$, $(1, 0)$ and $(-1, +1)$.

Since $F_n(-x, -y) = -F_n(x, y)$, the solutions to $F_n(x, y) = -1$ are given by $(-x, -y)$ where (x, y) are the solutions to $F_n(x, y) = 1$.

Exotic solutions found by E. Thomas in 1990

$F_0(X, Y) = X^3 + X^2Y - 2XY^2 - Y^3$
Solutions (x, y) to $F_0(x, y) = 1$:
$(-9, 5)$, $(-1, 2)$, $(2, -1)$, $(4, -9)$, $(5, 4)$

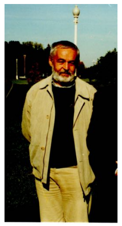
$F_1(X, Y) = X^3 - 3XY^2 - Y^3$
Solutions (x, y) to $F_1(x, y) = 1$:
$(-3, 2)$, $(1, -3)$, $(2, 1)$

$F_3(X, Y) = X^3 - 2X^2Y - 5XY^2 - Y^3$
Solutions (x, y) to $F_3(x, y) = 1$:
$(-7, -2)$, $(-2, 9)$, $(9, -7)$

M. Mignotte's work on E. Thomas's family

In 1993, M. Mignotte completed the work of E. Thomas by solving the problem for each n.

For $n \geq 4$ and for $n = 2$, the only solutions to $F_n(x, y) = 1$ are $(0, -1)$, $(1, 0)$ and $(-1, +1)$, while for the cases $n = 0, 1, 3$, the only nontrivial solutions are the ones found by E. Thomas.

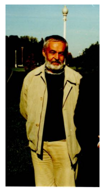


E. Thomas's family of Thue equations

For the same family

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

given $k \neq 0$, M. Mignotte A. Pethő and F. Lemmermeyer (1996) studied the family of Diophantine equations $F_n(X, Y) = k$.



M. Mignotte A. Pethő and F. Lemmermeyer (1996)

For $n \geq 2$, when x, y are rational integers verifying

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

then

$$\log |y| \leq c(\log n)(\log n + \log k)$$

with an effectively computable absolute constant c.

One would like an upper bound for $\max\{|x|, |y|\}$ depending only on k, not on n.

M. Mignotte A. Pethő and F. Lemmermeyer

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

As a consequence, when k is a given positive integer, there exists an integer n_0 depending upon k such that the inequality $|F_n(x, y)| \leq k$ with $n \geq 0$ and $|y| > \sqrt[3]{k}$ implies $n \leq n_0$.

Note that for $0 < |t| \leq \sqrt[3]{m}$, $(-t, t)$ and $(t, -t)$ are solutions. Therefore, the condition $|y| > \sqrt[3]{k}$ cannot be omitted.

E. Thomas's family of Thue inequations

In 1996, for the family of Thue inequations

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

Chen Jian Hua has given a bound for n by using Padé's approximations. This bound was highly improved in 1999 by G. Lettl, A. Pethő and P. Voutier.

Homogeneous variant of E. Thomas family

I. Wakabayashi, using again the approximants of Padé, extended these results to the families of forms, depending upon two parameters,

$sX^3 - tX^2Y - (t + 3s)XY^2 - sY^3$,

which includes the family of Thomas for $s = 1$ (with $t = n - 1$).

May 2010, Rio de Janeiro What were we doing on the beach of Rio?

Question of Claude Levesque

Consider Thomas's family of cubic Thue equations $F_n(X, Y) = \pm 1$ with

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

Write

$$F_n(X, Y) = (X - \lambda_{0n}Y)(X - \lambda_{1n}Y)(X - \lambda_{2n}Y)$$

where λ_{in} are units in the totally real cubic field $\mathbf{Q}(\lambda_{0n})$. According to E. Thomas, there are only finitely many (n, x, y) satisfying

$$n \geq 0, \quad \max\{|x|, |y|\} \geq 2 \quad \text{and} \quad F_n(x, y) = \pm 1.$$

Define

$$F_{n,2}(X, Y) = (X - \lambda_{0n}^2 Y)(X - \lambda_{1n}^2 Y)(X - \lambda_{2n}^2 Y).$$

Question: Are there only finitely many (n, x, y) satisfying

$$n \geq 0, \quad \max\{|x|, |y|\} \geq 2 \quad \text{and} \quad F_{n,2}(x, y) = \pm 1?$$

Expanding the suggestion of Claude Levesque

Given any irreducible binary form $F \in \mathbf{Z}[X, Y]$ and a unit ϵ in the field $\mathbf{Q}(\alpha)$ where α is a root of $F(X, 1)$, one may consider a family of Diophantine equations

$$F_a(X, Y) = k, \quad (a \in \mathbf{Z})$$

where $F_a(X, Y)$ is deduced from $F(X, Y)$ by twisting with ϵ^a: assuming $\mathbf{Q}(\alpha) = \mathbf{Q}(\alpha\epsilon^a)$, we define $F_a(X, 1)$ as the irreducible polynomial of $\alpha\epsilon^a$.

$$F(X, Y) = \prod_{i=1}^{d} (X - \sigma_i(\alpha)Y),$$

$$F_a(X, Y) = \prod_{i=1}^{d} (X - \sigma_i(\alpha\epsilon^a)Y).$$

Non effective results

With Claude Levesque, we started this program by using Schmidt's Subspace Theorem. We obtained general but non effective results for the twists of a given Thue equation. For instance :

Let α be an algebraic number of degree $d \geq 3$ and K be the field $\mathbf{Q}(\alpha)$. When ε is a unit of K such that $\alpha\varepsilon$ has degree d, let $f_\varepsilon(X)$ be the irreducible polynomial of $\alpha\varepsilon$ and let $F_\varepsilon(X, Y)$ be its homogeneous version. Then for all but finitely many of these units, the Thue equation $F_\varepsilon(x, y) = \pm 1$ has only the trivial solutions x, y in $\mathbf{Z}$ where $xy = 0$.

Non effective results on families of Thue–Mahler equations

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

Previous results by

J-H. Evertse, K. Győry, P. Vojta



Twists of a given Thue equation (effective results)

With Claude Levesque we obtained effective partial results in several cases:

- Our first paper (Springer Proceedings in Mathematics & Statistics, 2013) was dealing with non totally real cubic fields.
- Our second one (Ramanujan Math. Soc. Lecture Notes, published in 2016) was dealing with Thue equations attached to a number field having at most one real embedding.
- In the third paper (MJCNT, 2013), for each (irreducible) binary form attached to an algebraic number field, which is not a totally real cubic field, we exhibited an infinite family of equations twisted by units for which Baker's method provides effective bounds for the solutions.
- In a fourth paper (Contemporary Mathematics, 2015), we go one step further by considering twists by a power of a totally real unit.
- In a paper in JTNBx (2015), we solve the problem for the family obtained by twisting Thomas's equations related with the simplest cyclic cubic fields.

Back to Thomas's family

In Thomas's family, introduce a new parameter $a \in \mathbf{Z}$:

$$F_{n,a}(X,Y) = (X - \lambda_{0n}^a Y)(X - \lambda_{1n}^a Y)(X - \lambda_{2n}^a Y) \in \mathbf{Z}[X,Y].$$

Then we get a family of cubic Thue equations depending on two parameters (n,a):

$$F_{n,a}(x,y) = \pm 1.$$

Question: Are there only finitely many (n,a,x,y) satisfying

$$F_{n,a}(x,y) = \pm 1?$$

Thomas's family with two parameters

Joint work with Claude Levesque

Main result (2014): *there is an effectively computable absolute constant* $c > 0$ *such that, if* (x,y,n,a) *are nonzero rational integers with* $\max\{|x|,|y|\} \geq 2$ *and*

$$F_{n,a}(x,y) = \pm 1,$$

then

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

For all $n \geq 0$, trivial solutions with $a \geq 2$:
$(1,0)$, $(0,1)$
$(1,1)$ for $a = 2$

Exotic solutions to $F_{n,a}(x,y) = 1$ with $a \geq 2$

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

No further solution in the range

$$0 \leq n \leq 10, \qquad 2 \leq a \leq 70, \qquad -1000 \leq x, y \leq 1000.$$

Open question: are there further solutions?

Computer search by specialists


Further Diophantine results on the family $F_{n,a}(x,y)$

Let $k \geq 1$. There exists an absolute effectively computable constant κ such that, if there exists $(n,a,k,x,y) \in \mathbf{Z}^5$ with $a \neq 0$ verifying

$$0 < |F_{n,a}(x,y)| \leq k,$$

then

$$\log \max\{|x|,|y|\} \leq \kappa\mu$$

with

$$\mu = \begin{cases} (\log k + |a| \log |n|)(\log |n|)^2 \log\log |n| & \text{for } |n| \geq 3, \\ \log k + |a| & \text{for } n = 0, \pm 1, \pm 2. \end{cases}$$

For $a = 1$, this follows from the above mentioned result of M. Mignotte, A. Pethő and F. Lemmermeyer.

Further Diophantine results on the family $F_{n,a}(x,y)$

Let $k \geq 1$. There exists an absolute effectively computable constant κ such that, if there exists $(n,a,k,x,y) \in \mathbf{Z}^5$ with $a \neq 0$ verifying

$$0 < |F_{n,a}(x,y)| \leq k,$$

with $n \geq 0$, $a \geq 1$ and $|y| \geq 2\sqrt[3]{k}$, then

$$a \leq \kappa\mu'$$

with

$$\mu' = \begin{cases} (\log k + \log n)(\log n) \log\log n & \text{for } n \geq 3, \\ 1 + \log k & \text{for } n = 0, 1, 2. \end{cases}$$

Further Diophantine results on the family $F_{n,a}(x,y)$

Let $k \geq 1$. There exists an absolute effectively computable constant κ such that, if there exists $(n, a, k, x, y) \in \mathbf{Z}^5$ with $a \neq 0$ verifying

$$0 < |F_{n,a}(x,y)| \leq k,$$

with $xy \neq 0$, $n \geq 0$ and $a \geq 1$, then

$$a \leq \kappa \max\left\{1,\ (1+\log|x|)\log\log(n+3),\ \log|y|,\ \frac{\log k}{\log(n+2)}\right\}.$$

Conjecture on the family $F_{n,a}(x,y)$

Assume that there exists $(n, a, k, x, y) \in \mathbf{Z}^5$ with $xy \neq 0$ and $|a| \geq 2$ verifying

$$0 < |F_{n,a}(x,y)| \leq k.$$

We conjecture the upper bound

$$\max\{\log|n|, |a|, \log|x|, \log|y|\} \leq \kappa(1+\log k).$$

For $k > 1$ we cannot give an upper bound for $|n|$.

Since the rank of the units of $\mathbf{Q}(\lambda_0)$ is 2, one may expect a more general result as follows:

Conjecture on a family $F_{n,s,t}(x,y)$

Conjecture. For s, t and n in $\mathbf{Z}$, define

$$F_{n,s,t}(X,Y) = (X - \lambda_{0n}^s\lambda_{1n}^t Y)(X - \lambda_{1n}^s\lambda_{2n}^t Y)(X - \lambda_{2n}^s\lambda_{0n}^t Y).$$

There exists an effectively computable positive absolute constant κ with the following property: If n, s, t, x, y, k are integers satisfying

$$\max\{|x|,|y|\} \geq 2, \quad (s,t) \neq (0,0) \quad \text{and} \quad 0 < |F_{n,s,t}(x,y)| \leq k,$$

then

$$\max\{\log|n|, |s|, |t|, \log|x|, \log|y|\} \leq \kappa(1+\log k).$$

Sketch of proof

We want to prove the **Main result**: *there is an effectively computable absolute constant $c > 0$ such that, if (x, y, n, a) are nonzero rational integers with $\max\{|x|,|y|\} \geq 2$ and*

$$F_{n,a}(x,y) = \pm 1,$$

then

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

We may assume $a \geq 2$ and $y \geq 1$.

We first consider the case where n is sufficiently large.

Sketch of proof (continued)

Write λ_i for λ_{in}, $(i = 0, 1, 2)$:

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

We have

$$\begin{cases} n + \dfrac{1}{n} & \le \lambda_0 \le \quad n + \dfrac{2}{n}, \\ -\dfrac{1}{n+1} & \le \lambda_1 \le \quad -\dfrac{1}{n+2}, \\ -1 - \dfrac{1}{n} & \le \lambda_2 \le \quad -1 - \dfrac{1}{n+1}. \end{cases}$$

Sketch of proof (continued)

Define

$$\gamma_i = x - \lambda_i^a y, \quad (i = 0, 1, 2)$$

so that $F_{n,a}(x,y) = \pm 1$ becomes $\gamma_0\gamma_1\gamma_2 = \pm 1$.

One γ_i, say γ_{i_0}, has a small absolute value, namely

$$|\gamma_{i_0}| \le \frac{1}{y^2 \lambda_0^a},$$

the two others, say $\gamma_{i_1}, \gamma_{i_2}$, have large absolute values:

$$\min\{|\gamma_{i_1}|, |\gamma_{i_2}|\} > y|\lambda_2|^a.$$

Sketch of proof (continued)

Use λ_0, λ_2 as a basis of the group of units of $\mathbf{Q}(\lambda_0)$: there exist $\delta = \pm 1$ and rational integers A and B such that

$$\begin{cases} \gamma_{0,a} &= \delta \lambda_0^A \lambda_2^B, \\ \gamma_{1,a} &= \delta \lambda_1^A \lambda_0^B = \delta \lambda_0^{-A+B} \lambda_2^{-A}, \\ \gamma_{2,a} &= \delta \lambda_2^A \lambda_1^B = \delta \lambda_0^{-B} \lambda_2^{A-B}. \end{cases}$$

We can prove

$$|A| + |B| \le \kappa \left(\frac{\log y}{\log \lambda_0} + a \right).$$

Sketch of proof (continued)

The Siegel equation

$$\gamma_{i_0,a}(\lambda_{i_1}^a - \lambda_{i_2}^a) + \gamma_{i_1,a}(\lambda_{i_2}^a - \lambda_{i_0}^a) + \gamma_{i_2,a}(\lambda_{i_0}^a - \lambda_{i_1}^a) = 0$$

leads to the identity

$$\frac{\gamma_{i_1,a}(\lambda_{i_2}^a - \lambda_{i_0}^a)}{\gamma_{i_2,a}(\lambda_{i_1}^a - \lambda_{i_0}^a)} - 1 = -\frac{\gamma_{i_0,a}(\lambda_{i_1}^a - \lambda_{i_2}^a)}{\gamma_{i_2,a}(\lambda_{i_1}^a - \lambda_{i_0}^a)}$$

and the estimate

$$0 < \left| \frac{\gamma_{i_1,a}(\lambda_{i_2}^a - \lambda_{i_0}^a)}{\gamma_{i_2,a}(\lambda_{i_1}^a - \lambda_{i_0}^a)} - 1 \right| \le \frac{2}{y^3 \lambda_0^a}.$$

End of the proof when n is large

We complete the proof when n is large by means of a lower bound for a linear form in logarithms of algebraic numbers (Baker's method).

Next we need to consider the case where n is bounded. We have results which are valid not only for the Thue equations of the family of Thomas. The next result completes the proof of our main theorem.

Twists of a given cubic Thue equation

Consider a monic irreducible cubic polynomial $f(X) \in \mathbf{Z}[X]$ with $f(0) = \pm 1$ and write

$$F(X, Y) = Y^3 f(X/Y) = (X - \epsilon_1 Y)(X - \epsilon_2 Y)(X - \epsilon_3 Y).$$

For $a \in \mathbf{Z}$, $a \neq 0$, define

$$F_a(X, Y) = (X - \epsilon_1^a Y)(X - \epsilon_2^a Y)(X - \epsilon_3^a Y).$$

Then there exists an effectively computable constant $\kappa > 0$, depending only on f, such that, for any $k \geq 2$, any (x, y, a) in the set

$$\{(x, y, a) \in \mathbf{Z}^2 \times \mathbf{Z} \mid xya \neq 0,\ \max\{|x|, |y|\} \geq 2,\ |F_a(x, y)| \leq k\}$$

satisfies

$$\max\{|x|, |y|, e^{|a|}\} \leq k^\kappa.$$

A conjecture

One of our goals is to prove the following:

Conjecture. *There exists a constant $\kappa > 0$, depending only on α, such that, for any $k \geq 2$, all solutions (x, y, ε) in $\mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}_K^\times$ of the inequality*

$$|F_\varepsilon(x, y)| \leq k, \text{ with } xy \neq 0 \text{ and } [\mathbf{Q}(\alpha\varepsilon) : \mathbf{Q}] \geq 3,$$

satisfy

$$\max\{|x|,\ |y|,\ e^{\mathrm{h}(\alpha\varepsilon)}\} \leq k^\kappa.$$

Mahidol University International College *November 17, 2016*

Applied Mathematics Program

Lecture on Families of Diophantine equations

Michel Waldschmidt

Université P. et M. Curie (Paris 6)

http://www.imj-prg.fr/~michel.waldschmidt/