Carleton University (Ottawa) June 16-20, 2014
13th Conference of the
Canadian Number Theory Association
(CNTA XIII)

A family of Thue equations involving powers of units of the simplest cubic fields

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

The pdf file of this talk can be downloaded at URL
http://www.math.jussieu.fr/∼miw/

Abstract

E. Thomas was one of the first to solve an infinite family of Thue equations, when he considered the forms

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

and the family of equations $F_n(X,Y) = \pm 1$, $n \in \mathbf{N}$.
This family is associated to the family of the simplest cubic fields $\mathbf{Q}(\lambda)$ of D. Shanks, λ being a root of $F_n(X,1)$. We introduce in this family a second parameter by replacing the roots of the minimal polynomial $F_n(X,1)$ of λ by the a-th powers of the roots and we effectively solve the family of Thue equations that we obtain and which depends now on the two parameters n and a.
This is a joint work with Claude Levesque.

Thue Diophantine equations

Let $F \in \mathbf{Z}[X,Y]$ be a homogeneous irreducible form of degree ≥ 3 and let $m \geq 1$.

Thue (1908): there are only finitely many integer solutions $(x,y) \in \mathbf{Z} \times \mathbf{Z}$ of

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

Solving $F(x,y) = m$ by Baker's method

Thue's proof is *ineffective*, it gives only an upper bound for the number of solutions.
Baker's method is *effective*, it gives an upper bound for the solutions:

$$\max\{|x|,|y|\} \leq \max\{m,2\}^{\kappa}$$

where κ is an effectively computable constant depending only on F.

Families of Thue equations

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

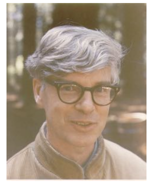
$$(a+1)X^n - aY^n = 1.$$

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

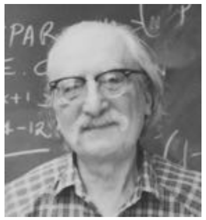
$$F_n(X,Y) = X^3 - (n-1)X^2Y - (n+2)XY^2 - Y^3.$$

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 $F_0(x, y) = 1$:
$(-9, 5)$, $(-1, 2)$, $(2, -1)$, $(4, -9)$, $(5, 4)$

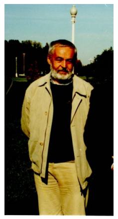
$F_1(X, Y) = X^3 - 3XY^2 - Y^3$
Solutions (x, y) to $F_1(x, y) = 1$:
$(-3, 2)$, $(1, -3)$, $(2, 1)$

$F_3(X, Y) = X^3 - 2X^2Y - 5XY^2 - Y^3$
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.

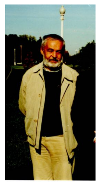


E. Thomas's family of Thue equations

For the same family

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

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



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

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

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

then

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

with an effectively computable absolute constant c.

One would like an upper bound for $\max\{|x|, |y|\}$ depending only on m, 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 m is a given positive integer, there exists an integer n_0 depending upon m such that the inequality $|F_n(x, y)| \leq m$ with $n \geq 0$ and $|y| > \sqrt[3]{m}$ implies $n \leq n_0$.

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

E. Thomas's family of Thue inequations

In 1996, for the family of Thue inequations

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

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?

Suggestion 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 $\mathbf{Q}(\lambda_{0n})$. Twist these equations by introducing 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):

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

Thomas's family with two parameters

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

$$0 \leq n \leq 100, \qquad 2 \leq a \leq 58, \qquad -1000 \leq x, y \leq 1000.$$

Open question: are there further solutions?

Computer search by specialists

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

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

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

then

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

with

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

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

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

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

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

with

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

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

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

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

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

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

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

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

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

We conjecture the upper bound

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

For $m > 1$ 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, m are integers satisfying

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

then

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

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 may also assume n sufficiently large, thanks to the following result which we proved earlier.

Twists of cubic Thue equations

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 $m \geq 2$, any (x, y, a) in the set

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

satisfies

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

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

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

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

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

Sketch of proof (completed)

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

Families of Thue equations (continued)

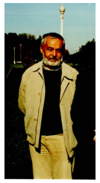
E. Lee and M. Mignotte with N. Tzanakis studied in 1991 and 1992 the family of cubic Thue equations

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

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

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

In 2000, M. Mignotte proved the same result for all $n \geq 3$.



Families of Thue equations (continued)

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

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

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

A. Togbé considered the family of equations

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

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

Families of Thue equations (continued)

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

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

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

Families of Thue equations (continued)

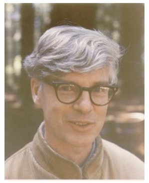
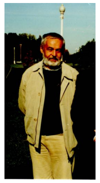
E. Thomas considered some families of Diophantine equations

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

for restricted values of b and c.
Family of quartic equations:

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

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


Families of Thue equations (continued)

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 $\mathbf{Z}[a]$.

Further results by J.H. Chen, B. Jadrijević, R. Roth, P. Voutier, P. Yuan, V. Ziegler...

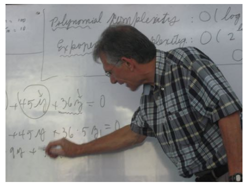
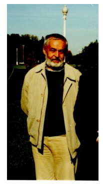
Surveys

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


Families of Thue equations (continued)

Further contributors are :
Istvan Gaál, Günter Lettl, Claude Levesque, Maurice Mignotte,



Attila Pethő, Robert Tichy, Nikos Tzanakis, AlainTogbé




Carleton University (Ottawa) June 16-20, 2014
13th Conference of the
Canadian Number Theory Association
(CNTA XIII)

A family of Thue equations involving powers of units of the simplest cubic fields

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

The pdf file of this talk can be downloaded at URL
http://www.math.jussieu.fr/~miw/