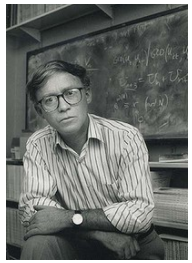
March 15, 2012 CARMA
International Number Theory
Conference



Some families of curves with only trivial S–integral points

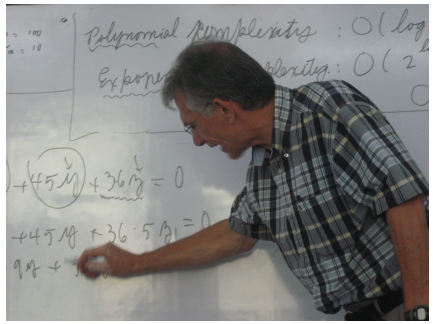
(joint work with Claude Levesque)

Michel Waldschmidt

Institut de Mathématiques de Jussieu (Univ. Paris VI)
http://www.math.jussieu.fr/∼miw/

Abstract

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



Joint papers with Alf

Loxton, John H. ; Mignotte, Maurice ; van der Poorten, Alfred J. ; Waldschmidt, Michel
A lower bound for linear forms in the logarithms of algebraic numbers.
C. R. Math. Rep. Acad. Sci. Canada 9 (1987), no. 2, 119–124.
MR0880603 (88j:11041) (Reviewer : P. L. Cijsouw)

Brindza, Béla ; Pintér, Ákos ; van der Poorten, Alfred J. ; Waldschmidt, Michel
On the distribution of solutions of Thue's equation.
Number theory in progress, Vol. 1 (Zakopane-Kościelisko, 1997), 35–46, de Gruyter, Berlin, 1999.
MR1689497 (2000c:11048) (Reviewer : Yann Bugeaud)

Number of solutions of Thue equations

Brindza, B. ; Pintér, Á. ; van der Poorten, A. J. ; W.M. (1997)

Let $F \in \mathbf{Z}[X, Y]$ be an irreducible binary form of degree $n \geq 3$ and let m be a positive integer having s distinct prime factors. Then the equation

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

has at most $2n^2(s+1) + 13n$ solutions with

$$\max(|x|, |y|) \geq 21 n^2 M^5 m^\theta,$$

where

$$\theta = \frac{1}{n-2} + \frac{1}{(n-1)^2}.$$

Thue equations

Axel Thue

(1863 - 1922)

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

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

has only finitely many solutions $(x, y) \in \mathbf{Z} \times \mathbf{Z}$.

Liouville's inequality

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

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

Joseph Liouville, 1844

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

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

Mike Bennett

http://www.math.ubc.ca/∼bennett/

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

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

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

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

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

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

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

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

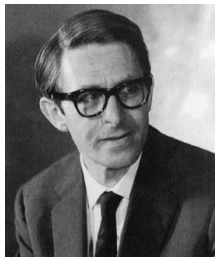
- any $\kappa > (d/2) + 1$ by A. Thue (1909),
- $2\sqrt{d}$ by C.L. Siegel in 1921,
- $\sqrt{2d}$ by F. Dyson and A.O. Gel'fond in 1947,
- any $\kappa > 2$ by K.F. Roth in 1955.

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.

Families of Thue equations

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

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

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

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

Families of Thue equations (continued)

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

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

According to E. Thomas (1990) and M. Mignotte (1993), for $a \geq 4$ the only solutions are $(0, -1)$, $(1, 0)$ and $(-1, +1)$, while for the cases $a = 0, 1, 3$, there exist some nontrivial solutions, too, which are given explicitly by Thomas.
For the same form $F_a(X, Y)$, all solutions of the Thue inequality $|F_a(X, Y)| \leq 2a + 1$ have been found by M. Mignote A. Pethő and F. Lemmermeyer (1996).
The family of Thue's equations attached to some quintic fields by E. Lehmer do not seem to have been investigated from this point of view so far.

Families of Thue equations (continued)

E. 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 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)

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).

New families of Thue equations

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

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 with integer coefficients.

A corollary of our main result is the following :

Corollary

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

$$\left\{(x,y,\varepsilon) \in \mathbf{Z}^2 \times \mathbf{Z}_K^\times \mid xy \neq 0,\ [\mathbf{Q}(\varepsilon) : \mathbf{Q}] \geq 3,\ F_\varepsilon(x,y) = m\right\}$$

is finite.

Thue–Mahler equations

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

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

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

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

S–integers, S–units

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

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

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

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

Two special cases

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

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

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

and

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

Hence

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

Thue–Mahler equations over a number field

We will consider the Thue–Mahler equations

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

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

If (x, y, ε) is a solution, namely

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

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

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

Equivalence classes

Definition. Two solutions (x, y, ε) and (x', y', ε') in $\mathcal{O}_S^2 \times \mathcal{O}_S^\times$ of the equation $F(X, Y) = E$ are said to be *equivalent modulo* $\mathcal{O}_S^\times$ if the points of $\mathbf{P}^1(K)$ with projective coordinates $(x : y)$ and $(x' : y')$ are the same.

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

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

where d is the degree of F.

Thue–Mahler equations (continued)

For any finite set S of places of K containing all the archimedean places, for every $m \in K^\times$ and for any binary homogeneous form $F(X, Y)$ with the property that the polynomial $F(X, 1) \in K[X]$ has at least three linear factors involving three distinct roots in K, the Thue-Mahler equation

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

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

A "special" case

For any finite set S of places of K containing all the archimedean places, the Thue-Mahler equation

$$XY(X - Y) = E$$

has but a finite number of classes of solutions $(x, y, \varepsilon) \in \mathcal{O}_S^2 \times \mathcal{O}_S^\times$.

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

Siegel S–unit equation

For any finite set S of places of K containing all the archimedean places, the S–unit equation

$$E_1 + E_2 = 1$$

has but a finite number of solutions $(\varepsilon_1, \varepsilon_2)$ in $\mathcal{O}_S^\times \times \mathcal{O}_S^\times$.

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

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

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

Integral points on $\mathbf{P}^1$ minus three points

A further equivalent statement is the following one :

For any finite set S of places of K containing all the archimedean places, every set of S–integral points of $\mathbf{P}^1(K)$ minus three points is finite.

Families of Thue–Mahler equations

A more general corollary of our main result is the following :

Corollary

Further, let $p_1, \dots, p_s$ be finitely many primes. Then the set of $(x, y, z_1, \dots, z_s, \varepsilon) \in \mathbf{Z}^{2+s} \times \mathbf{Z}_K^\times$ with $z_j \geq 0$ for $j = 1, \dots, s$, $xy \neq 0$ and $\gcd(xy, p_1 \cdots p_s) = 1$ such that $[\mathbf{Q}(\varepsilon) : \mathbf{Q}] \geq 3$ and

$$F_\varepsilon(x, y) = m p_1^{z_1} \cdots p_s^{z_s}$$

is finite.

The general equation

Let K be a number field, S a finite set of places of K containing the infinite places, μ, $\alpha_1, \alpha_2, \alpha_3$ nonzero elements in K. Consider the equation

$$(X - \alpha_1 E_1 Y)(X - \alpha_2 E_2 Y)(X - \alpha_3 E_3 Y)Z = \mu E,$$

where the variables take for values

$$(x, y, z, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon) \in \mathcal{O}_S^3 \times (\mathcal{O}_S^\times)^4.$$

Trivial solutions are solutions with $xy = 0$.
Two nontrivial solutions $(x, y, z, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon)$ and $(x', y', z', \varepsilon_1', \varepsilon_2', \varepsilon_3', \varepsilon')$ are called *S^3–dependent* if there exist S–units η_1, η_2 and η_3 in $\mathcal{O}_S^\times$ such that

$$x' = x\eta_1,\ y' = y\eta_1\eta_3^{-1},\ z' = z\eta_2,\ \varepsilon_i' = \varepsilon_i\eta_3,\ \varepsilon' = \varepsilon\eta_1^3\eta_2.$$

The main result

Theorem

The set of classes of S^3–dependence of the nontrivial solutions

$$(x, y, z, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon) \in \mathcal{O}_S^3 \times (\mathcal{O}_S^\times)^4$$

of the equation

$$(X - \alpha_1 E_1 Y)(X - \alpha_2 E_2 Y)(X - \alpha_3 E_3 Y)Z = \mu E$$

satisfying $\mathrm{Card}\{\alpha_1\varepsilon_1, \alpha_2\varepsilon_2, \alpha_3\varepsilon_3\} = 3$ is finite.

The number of these classes is bounded by an explicit constant depending only on K, μ, $\alpha_1, \alpha_2, \alpha_3$ and the rank s of the group $\mathcal{O}_S^\times$.

A "special" case

It turns out that the special case of the equation

$$(X - Y)(X - E_1 Y)(X - E_2 Y) = E$$

is equivalent to the general case.

Two solutions $(x, y, \varepsilon_1, \varepsilon_2, \varepsilon)$ and $(x', y', \varepsilon_1', \varepsilon_2', \varepsilon')$ in $\mathcal{O}_S^2 \times (\mathcal{O}_S^\times)^3$ of this equation are called *S–dependent* if there exists $\eta \in \mathcal{O}_S^\times$ such that

$$x' = x\eta,\ y' = y\eta,\ \varepsilon_1' = \varepsilon_1,\ \varepsilon_2' = \varepsilon_2,\ \varepsilon' = \varepsilon\eta^3.$$

Theorem

The number of classes of S–dependence of the solutions $(x, y, \varepsilon_1, \varepsilon_2, \varepsilon)$ with $\varepsilon_1 \neq 1$, $\varepsilon_2 \neq 1$, $\varepsilon_1 \neq \varepsilon_2$ of the equation $(X - Y)(X - E_1 Y)(X - E_2 Y) = E$ is finite.

Connection with a result of P. Vojta

Let D be a divisor of $\mathbf{P}^n$ with at least $n + 2$ distinct components. Then any set of D–integral points on $\mathbf{P}^n$ is degenerate (namely : is contained in a proper Zarisky closed set).

With $n = 4$, with projective coordinates $(X : Y : Z : E_1 : E_2)$ and with the divisor

$$Z\, E_1\, E_2\, (X - Y)(XZ - E_1 Y)(XZ - E_2 Y) = 0$$

on $\mathbf{P}^4$, one deduces that the set of solutions of the equation

$$(X - Y)(X - E_1 Y)(X - E_2 Y) = E$$

is degenerate.

Generalized S–unit equation

Let $n \geq 1$ be an integer and let S a finite set of places of K including the archimedean places. Then the equation

$$E_0 + \cdots + E_n = 0$$

has but finitely many classes modulo $\mathcal{O}_S^\times$ of solutions $(\varepsilon_0, \ldots, \varepsilon_n) \in (\mathcal{O}_S^\times)^{n+1}$ for which no proper subsum $\sum_{i \in I} \varepsilon_i$ vanishes, with I being a subset of $\{0, \ldots, n\}$, with at least two elements and at most n.

Integral points on $\mathbf{P}^n$ minus $n + 2$ hyperplanes

Let $n \geq 1$ be an integer and let S a finite set of places of K including the archimedean places. Then for any set of $n + 2$ distinct hyperplanes $H_0, \ldots, H_{n+1}$ in $\mathbf{P}^n(K)$, the set of S–integral points of $\mathbf{P}^n(K) \setminus (H_0 \cup \cdots \cup H_{n+1})$ is contained in a finite union of hyperplanes of $\mathbf{P}^n(K)$.

Work of P. Vojta.

Generalized Siegel unit equation and integral points

The finiteness of non degenerate solutions of the generalized S–unit equation is equivalent to the statement on integral points on $\mathbf{P}^n$ minus $n+2$ hyperplanes, and both statements depend on Schmidt's Subspace Theorem.

The statement on the generalized S–unit equation is our main tool for the proof of our finiteness results on families of Thue–Mahler Diophantine equations.

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 $\mathbf{Q}^m$.

Wolfgang M. Schmidt

Schmidt's Subspace Theorem

For $\mathbf{x} = (x_0, \ldots, x_{m-1}) \in \mathbf{Z}^m$, define $|\mathbf{x}| = \max\{|x_0|, \ldots, |x_{m-1}|\}$.

W.M. Schmidt (1970) : *For $m \geq 2$ let $L_0, \ldots, L_{m-1}$ be m independent linear forms in m variables with algebraic coefficients. Let $\epsilon > 0$. Then the set*

$$\{\mathbf{x} = (x_0, \ldots, x_{m-1}) \in \mathbf{Z}^m \; ; \; |L_0(\mathbf{x}) \cdots L_{m-1}(\mathbf{x})| \leq |\mathbf{x}|^{-\epsilon}\}$$

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

Example : $m = 2$, $L_0(x_0, x_1) = x_0$, $L_1(x_0, x_1) = \alpha x_0 - x_1$.
Roth's Theorem : *for any real algebraic irrational number α, for any $\epsilon > 0$, the set of $p/q \in \mathbf{Q}$ with $|\alpha - p/q| < q^{-2-\epsilon}$ is finite.*

Schmidt's subspace Theorem – Several places

Let $m \geq 2$ be a positive integer, S a finite set of places of $\mathbf{Q}$ containing the infinite place. For each $v \in S$ let $L_{0,v}, \ldots, L_{m-1,v}$ be m independent linear forms in m variables with algebraic coefficients in the completion of $\mathbf{Q}$ at v. Let $\epsilon > 0$. Then the set of $\mathbf{x} = (x_0, \ldots, x_{m-1}) \in \mathbf{Z}^m$ such that

$$\prod_{v \in S} |L_{0,v}(\mathbf{x}) \cdots L_{m-1,v}(\mathbf{x})|_v \leq |\mathbf{x}|^{-\epsilon}$$

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

Sketch of proof of the main theorem

Let α_1, α_2, α_3, μ be nonzero elements of the number field K. Consider a solution $(x, y, z, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon)$ in $\mathcal{O}_S^3 \times (\mathcal{O}_S^\times)^4$ of the equation

$$(X - \alpha_1 E_1 Y)(X - \alpha_2 E_2 Y)(X - \alpha_3 E_3 Y)Z = \mu E$$

satisfying $xy \neq 0$ and $\mathrm{Card}\{\alpha_1\varepsilon_1, \alpha_2\varepsilon_2, \alpha_3\varepsilon_3\} = 3$:

$$(x - \alpha_1\varepsilon_1 y)(x - \alpha_2\varepsilon_2 y)(x - \alpha_3\varepsilon_3 y)z = \mu\varepsilon.$$

Sketch of proof of the main theorem (continued)

Set $\beta_j = x - \alpha_j\varepsilon_j y$ ($j = 1, 2, 3$), so that $\beta_1\beta_2\beta_3 z = \mu\varepsilon$.
À la Siegel, eliminate x and y among the three equations

$$\beta_1 = x - \alpha_1\varepsilon_1 y,\ \beta_2 = x - \alpha_2\varepsilon_2 y,\ \beta_3 = x - \alpha_3\varepsilon_3 y.$$

We deduce

$$u_{12} - u_{13} + u_{23} - u_{21} + u_{31} - u_{32} = 0,$$

where

$$u_{ij} = \alpha_i\epsilon_i\beta_j, \quad (i, j = 1, 2, 3,\ i \neq j).$$

This is a generalized S–unit equation with six terms. But nontrivial subsums may vanish. . .

Thue's equations 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.

A variant of Liouville's inequality

Claude Levesque and M.W.,
Approximation of an algebraic number by products of rational numbers and units,
Journal of the Australian Mathematical Society, Special Issue dedicated to Alf van der Poorten, to appear.

Let $\alpha \in \mathbf{C}$ be an algebraic number of degree d. There exists a constant c_1 such that, for any $p/q \in \mathbf{Q}$ and for any unit ε of $\mathbf{Q}(\alpha)$ such that $\varepsilon\alpha \neq p/q$, we have

$$\left|\varepsilon\alpha - \frac{p}{q}\right| \geq \frac{c_1}{q^d \lceil\varepsilon\rceil^{d-1}}.$$

Quadratic case

Let ϵ_0 be the fundamental unit > 1 of the real quadratic field $\mathbf{Q}(\alpha)$. For any $n \geq 0$ with at most one exception, there exists a constant c_2 and infinitely many rational numbers p/q such that

$$\left|\epsilon_0^n \alpha - \frac{p}{q}\right| \leq \frac{c_2}{q^2 \epsilon_0^n}$$

and infinitely many rational numbers p/q such that

$$\left|\epsilon_0^{-n} \alpha - \frac{p}{q}\right| \leq \frac{c_2}{q^2 \epsilon_0^n}.$$

Refinement in degree ≥ 3

Consequence of the finiteness result of S–integral points on Thue's curves :

Let α be an algebraic number of degree d. For any constant $\kappa > 0$, the set of pairs $(p/q, \varepsilon) \in \mathbf{Q} \times \mathbf{Z}_K^\times$ such that $[\mathbf{Q}(\varepsilon\alpha) : \mathbf{Q}] \geq 3$ and

$$\left|\varepsilon\alpha - \frac{p}{q}\right| \leq \frac{\kappa}{q^d \, |\varepsilon|^{d-1}}$$

is finite.

Corvaja–Zannier

Denote by $\| \cdot \|$ the distance to the nearest integer : for $x \in \mathbf{R}$,

$$\|x\| := \min_{n \in \mathbf{Z}} |x - n|.$$

Let $\overline{\mathbf{Q}}$ denote the field of complex numbers which are algebraic over $\mathbf{Q}$. Following P. Corvaja and U. Zannier (2004), call a (complex) algebraic number ξ a *pseudo–Pisot* number if
(i) $|\xi| > 1$ and all its conjugates have (complex) absolute value strictly less than 1 ;
(ii) ξ has integral trace : $\mathrm{Tr}_{\mathbf{Q}(\xi)/\mathbf{Q}}(\xi) \in \mathbf{Z}$.

Corvaja–Zannier

The main Theorem of Corvaja and Zannier, whose proof also rests on Schmidt's Subspace Theorem, can be stated as follows.

Let $\Gamma \subset \overline{\mathbf{Q}}^\times$ be a finitely generated multiplicative group of algebraic numbers, let $\alpha \in \overline{\mathbf{Q}}^\times$ be a non–zero algebraic number and let $\eta > 0$ be fixed. Then there are only finitely many pairs $(q, \varepsilon) \in \mathbf{Z} \times \Gamma$ with $\delta = [\mathbf{Q}(\varepsilon) : \mathbf{Q}]$ such that $|\alpha q \varepsilon| > 1$, $\alpha q \varepsilon$ is not a pseudo–Pisot number and

$$0 < \|\alpha q \varepsilon\| < \frac{1}{e^{\eta \mathrm{h}(\varepsilon)} q^{\delta + \eta}}.$$

Effectivity (work in progess)

Explicit upper bounds for the number of solutions or for the number of classes of solutions are obtained by means of quantitative versions of the Subspace Theorem of W.M. Schmidt, but effective bounds for the solutions or for the heights of the solutions are not available in general.

In a few special cases we are able to produce effective results.

An effective refinement of Liouville's estimate

Let K be a number field and let $\alpha \in K$. There exists an effectively computable constant $c_3 > 0$ such that, for any unit $\varepsilon \in \mathbf{Z}_K^\times$ and any rational number p/q with $\varepsilon\alpha \neq p/q$,

$$\left|\varepsilon\alpha - \frac{p}{q}\right| \geq \left(\log(|\overline{\varepsilon}|+2)\right)^{-c_3 \log \max\{|p|,\, q,\, 2\}}.$$

On the Brahmagupta–Fermat–Pell equations

The equation $x^2 - dy^2 = \pm 1$, where the unknowns x and y are positive integers while d is a fixed positive integer which is not a square, has been mistakenly called with the name of Pell by Euler. It was investigated by Indian mathematicians since Brahmagupta (628) who solved the case $d = 92$, next by Bhaskara II (1150) for $d = 61$ and Narayana (during the 14-th Century) for $d = 103$.

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*) : produce 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

Narayana Pandit $\sim 1340 - \sim 1400$

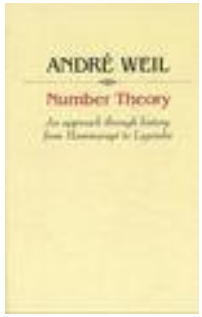
$$x^2 - 103y^2 = 1$$

$$x = 227\,528, \qquad y = 22\,419.$$

$$227\,528^2 - 103 \cdot 22\,419^2 = 1.$$

References 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



Brahmagupta–Fermat–Pell equations

Connection with
- Continued fractions
- Linear recurrence sequences

(cf. the lecture by Hugh Williams)

Simultaneous Brahmagupta–Fermat–Pell equations

Let a and b be two nonzero distinct rational integers.
M.A. Bennett, M. Cipu, M. Mignotte and R. Okazaki (2006) : the system of two equations

$$X^2 - aZ^2 = 1, \quad Y^2 - bZ^2 = 1,$$

where the unknowns (X, Y, Z) take positive integer values, has at most two solutions .

An infinite family of couples (a, b) for which this system has exactly two solutions is known explicitly.

A result due to M. Bennett

Let a and b be two rational integers which are not square. Let u and v be nonzero rational integers with $av \neq bu$.
M. Bennett (1998) : the system of two equations

$$X^2 - aZ^2 = u, \quad Y^2 - bZ^2 = v,$$

where the unknowns (X, Y, Z) take positive integer values has at most

$$c\, 2^{\min\{\omega(u),\omega(v)\}} \log(|u| + |v|)$$

solutions, with an absolute positive constant c, where $\omega(n)$ is the number of distinct prime factors of n.

D.W. Masser and J.H. Rickert (1996)

For any N, there exist two rational integers u and v such that the system of two equations

$$X^2 - 2Z^2 = u, \quad Y^2 - 3Z^2 = v$$

has at least N solutions (x, y, z) in positive integers.

Bugeaud–Levesque–W.

Équations de Fermat-Pell-Mahler simultanées,
Publicationes Mathematicae Debrecen, 79 3-4 (2011), 357–366.

Let a and b be two rational integers which are not square and such that ab is not a square. Let $\{p_1, \ldots, p_s\}$ be a finite set of prime numbers. Then the system of two simultaneous equations :

$$\begin{cases} X^2 - aZ^2 &= \pm p_1^{m_1} \cdots p_s^{m_s}, \\ Y^2 - bZ^2 &= \pm p_1^{n_1} \cdots p_s^{n_s}, \end{cases}$$

has only finitely many solutions in integers $(x, y, z, m_1, \ldots, m_s, n_1, \ldots, n_s)$, with $x, y, z > 0$ and $\gcd(x, y, z, p_1 \cdots p_s) = 1$.

Brahmagupta–Fermat–Pell–Mahler equations

Let b_1, b_2 be rational integers, a_1, a_2, c_1, c_2 be nonzero rational integers, $S = \{p_1, \ldots, p_s\}$ a finite set of prime numbers.

Set $\Delta_1 = b_1^2 - 4a_1c_1$, $\Delta_2 = b_2^2 - 4a_2c_2$ and assume that the product $\Delta_1\Delta_2$ is not a square.

Consider the equation

$$(a_1X^2 + b_1XZ + c_1Z^2)(a_2Y^2 + b_2YZ + c_2Z^2) = W,$$

where the unknowns (X, Y, Z, W) take their values (x, y, z, w) in $\mathbf{Z}_S^3 \times \mathbf{Z}_S^\times$ with $xyz \neq 0$.

Equivalence classes

Two solutions (x, y, z, w) and (x', y', z', w') of the equation

$$(a_1X^2 + b_1XZ + c_1Z^2)(a_2Y^2 + b_2YZ + c_2Z^2) = W,$$

are called *S–equivalent* if there exists a S-unit u such that

$$x' = ux,\ y' = uy,\ z' = uz,\ w' = u^4w.$$

Bugeaud–Levesque–W.

Équations de Fermat-Pell-Mahler simultanées,
Publicationes Mathematicae Debrecen, 79 3-4 (2011), 357–366.

The set of S–equivalence classes of solutions $(x, y, z, w) \in \mathbf{Z}_S^3 \times \mathbf{Z}_S^\times$ of the equation

$$(a_1X^2 + b_1XZ + c_1Z^2)(a_2Y^2 + b_2YZ + c_2Z^2) = W,$$

with $xyz \neq 0$, is finite, and this set has at most κ_1 elements, where

$$\kappa_1 = 2 + 2^{962t} \quad \textit{with} \quad t = 4(\omega(a_1a_2p_1 \cdots p_s) + 1).$$

Consequence

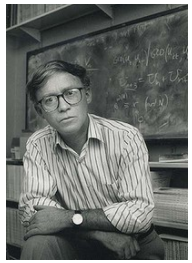
Let $p_1, \ldots, p_s$ be distinct prime numbers. The set of $(2s + 3)$ tuples of rational integers $(x, y, z, m_1, \ldots, m_s, n_1, \ldots, n_s)$, with $x, y, z > 0$ and $\gcd(x, y, z, p_1 \cdots p_s) = 1$, satisfying

$$\begin{cases} a_1X^2 + b_1XZ + c_1Z^2 &= \pm p_1^{m_1} \cdots p_s^{m_s}, \\ a_2Y^2 + b_2YZ + c_2Z^2 &= \pm p_1^{n_1} \cdots p_s^{n_s}, \end{cases}$$

is finite, and this set has at most κ_2 elements, where

$$\kappa_2 = 2 + 2^{3848(\omega(a_1a_2p_1\cdots p_s)+1)}.$$

March 15, 2012 CARMA
International Number Theory
Conference



Some families of curves with only trivial S–integral points

(joint work with Claude Levesque)

Michel Waldschmidt

Institut de Mathématiques de Jussieu (Univ. Paris VI)
http://www.math.jussieu.fr/∼miw/