On Thue equations

(Joint results with Michel Waldschmidt)

Claude Levesque (U. Laval)

1. Introduction

Some infinite families of diophantine Thue equations having only trivial solutions (or a finite number of integral solutions) have been exhibited by a few mathematicians:

Thomas, Győry, Schlickewei, Pethő, Evertse, Gaál, Tichy, Heuberger, de Weger, Fuchs, Lettl, Voutier, Chen, Mignotte, Tzanakis, Wakabayashi, Togbé, Ziegler, Berczes, Walsh, Halter-Koch, Dujella, etc. ... and of course Michel Waldschmidt.

2. The first family of Thomas

In 1990 Thomas studied the families of diophantine equations

$$F_n(X, Y) = c$$

where

$$F_n(X, Y) = X^3 - (n-1)X^2Y - (n+2)XY^2 - Y^3 \quad \textit{and} \quad c = \pm 1.$$

The polynomial $F_n(X, Y)$ *is the homogenized form of the minimal polynomial* $f_n(X)$ *of Shanks's simplest cubic fields, namely*

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

Theorem (Thomas). *Let*

$$F_n(X,Y) = X^3 - (n-1)X^2Y - (n+2)XY^2 - Y^3 \quad \textit{with} \quad c = \pm 1.$$

(i) *For* $n \geq 1.365 \times 10^7$*, there are only the trivial solutions:*

$$(c,0), \quad (0,c), \quad (c,-c).$$

(ii) *For* $0 \leq n \leq 1000$*, the other solutions are:*

$$\begin{array}{lcllll} n=0 & : & (-9c,5c), & (-c,2c), & (2c-c), \\ & & (4c,-9c), & (5c,4c), & (-c,-c) \\ n=1 & : & (-3c,2c), & (c,-3c), & (2c,c); \\ n=3 & : & (-7c,-2c), & (-2c,9c), & (9c,-7c). \end{array}$$

Theorem (Mignotte). *For* $n \geq 0$*, the only solutions are the above ones.*

3. Our main theorem

Theorem (Waldschmidt-L).
Let K be an algebraic number field of degree $d \geq 3$. For every unit ε of degree at least 3, except for a finite number of them, the following holds true: Let $f_\varepsilon(X)$ be the minimal polynomial of ε and let $F_\varepsilon(X, Y)$ be the homogenized binary form associated to $f_\varepsilon(X)$. Then the solutions of the Thue equation

$$F_\varepsilon(X, Y) = 1$$

are given by $xy = 0$.

4. A general result involving powers of units

Let $d \geq 3$ be a given integer. Let $F(X, Y)$ be a monic irreducible binary form in $\mathbf{Z}[X, Y]$ satisfying $F(0, 1) = \pm 1$ and that we write as

$$F(X, Y) = \prod_{j=1}^{d} (X - \alpha_j Y)$$

with $|\alpha_1| \leq |\alpha_2| \leq \cdots \leq |\alpha_d|$. Denote by R the regulator of the number field $\mathbf{Q}(\alpha_1)$. Further, let $\lambda = |\alpha_d|$. For $a \geq 0$, consider the polynomial of $\mathbf{Z}[X, Y]$ defined by

$$F_a(X, Y) = \prod_{j=1}^{d} (X - \alpha_j^a Y).$$

Theorem (Waldschmidt-L). *Assume that α_1 is not a root of unity. There exists an effectively computable constant κ, depending only on d, with the following property. Let $(x, y, a) \in \mathbf{Z}^3$ satisfy*

$$xy \neq 0, \quad [\mathbf{Q}(\alpha_1^a) : \mathbf{Q}] = d, \quad F_a(x, y) = \pm 1.$$

Then,

$$|a| \leq \kappa \lambda^{d^4} R \log R.$$

Moreover, there exists another effectively computable constant κ such that

$$\max\{\log|x|,\ \log|y|\} < \kappa R \log(R)\big(R + |a| \log(\lambda)\big).$$

Our proof actually gives a much stronger estimate which depends on the following parameter $\mu > 1$ defined by

$$\mu = \begin{cases} \max\{2, \lambda\} & \text{if } |\alpha_1| = |\alpha_{d-1}| \text{ or } |\alpha_2| = |\alpha_d|, \\ \min\left\{ \dfrac{|\alpha_{d-1}|}{|\alpha_1|}, \dfrac{|\alpha_d|}{|\alpha_2|} \right\} & \text{if } |\alpha_1| < |\alpha_2| = |\alpha_{d-1}| < |\alpha_d|, \\ \dfrac{|\alpha_{d-1}|}{|\alpha_2|} & \text{if } |\alpha_2| < |\alpha_{d-1}|. \end{cases}$$

Theorem. *There exists an effectively computable constant κ such that*

$$|a| \le \kappa R \, \frac{\log \lambda}{\log \mu} \, (R + \log \lambda) \log(R + \log \lambda).$$

Thank you very much!

Introduction

When $f(X) \in \mathbf{Z}[X]$ *is a polynomial of degree* d*, we define the associated homogenous binary form* $F(X, Y)$ *of degree* d *by*

$$F(X, Y) = Y^d f(X/Y).$$

A **Thue equation** *is a diophantine equation of the form*

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

for some fixed integer k*, for which we look for all integral solutions.*

A **Thue-Mahler equation** *is a diophantine equation for which we look for solutions which are* S*-integers, where* S *is a finite set of primes.*

1. A family of A.Thue

The first family of Thue equations having only some trivial (positive) solutions was introduced by Thue:

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

Theorem *(Thue)*. *When n is a prime, if a is sufficiently large, then $x = y = 1$.*

Theorem *(Bennett)*. *When $n \geq 3$, we have $x = y = 1$ for each $a \geq 1$.*

Some Thue equations experts

Some infinite families of diophantine Thue equations having only trivial solutions (or a finite number of integral solutions) have been exhibited by a few mathematicians:

Thomas, Győry, Schlickewei, Pethő, Evertse, Gaál, Tichy, Heuberger, de Weger, Fuchs, Lettl, Voutier, Chen, Mignotte, Tzanakis, Wakabayashi, Togbé, Ziegler, Berczes, Halter-Koch, Dujella, etc. ... and of course Michel Waldschmidt.

3. Notations

K	:	*algebraic number field*
$\mathcal{O}_K$	:	*ring of integers of* K
$\mathcal{O}_K^\times$	:	*group of units of* K
$\mathcal{O}_S$	:	*ring of* S*-integers of* K *for a finite set* S *of places*
$\mathcal{O}_S^\times$	:	*group of* S*-units of* K

4. The first family of Thomas

In 1990 Thomas studied the families of diophantine equations

$$F_n(X, Y) = c$$

where

$$F_n(X, Y) = X^3 - (n-1)X^2Y - (n+2)XY^2 - Y^3 \quad \textit{and} \quad c = \pm 1.$$

The polynomial $F_n(X, Y)$ *is the homogenized form of the minimal polynomial* $f_n(X)$ *of Shanks's simplest cubic fields, namely*

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

Theorem (Thomas). *Let*

$$F_n(X,Y) = X^3 - (n-1)X^2Y - (n+2)XY^2 - Y^3 \quad \textit{with} \quad c = \pm 1.$$

(i) *For $n \geq 1.365 \times 10^7$, there are only the trivial solutions:*

$$(c,0), \quad (0,c), \quad (c,-c).$$

(ii) *For $0 \leq n \leq 1000$, the other solutions are:*

$$\begin{array}{lcllll} n=0 & : & (-9c,5c), & (-c,2c), & (2c-c), \\ & & (4c,-9c), & (5c,4c), & (-c,-c) \\ n=1 & : & (-3c,2c), & (c,-3c), & (2c,c); \\ n=3 & : & (-7c,-2c), & (-2c,9c), & (9c,-7c). \end{array}$$

Theorem (Mignotte). *For $n \geq 0$, the only solutions are the above ones.*

2. A general result on Thue-Mahler equations

Theorem (Waldschmidt-L). *Let K be a number field, S a finite set of places of K containing the archimedean places, n an integer ≥ 3, $\alpha_1, \ldots, \alpha_n$ some nonzero elements of K and $f(X,Y) \in K[X,Y]$ the binary form*

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

For $\underline{\varepsilon} \in (\mathcal{O}_S)^n$ defined by $\underline{\varepsilon} = (\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$, let

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

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

$$f_{\underline{\varepsilon}}(x,y) \in \mathcal{O}_S^\times$$

implies $xy = 0$.

3. A corollary of the last theorem

Theorem (Waldschmidt-L).
Let K be an algebraic number field of degree $d \geq 3$. For every unit ε of degree at least 3, except for a finite number of them, the following holds true: Let $f_\varepsilon(X)$ be the minimal polynomial of ε and let $F_\varepsilon(X, Y)$ be the homogenized binary form associated to $f_\varepsilon(X)$. Then the solutions of the Thue equation

$$F_\varepsilon(X, Y) = 1$$

are given by $xy = 0$.

4. Schmidt's subspace theorem

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

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

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

Note. *The subspace theorem is not effective.*

5. Unit equations.

Theorem *(Evertse, Beukers, Sdshlickwei)*. *Let K be an algebraic number field. Let $\delta_1, \ldots, \delta_\ell$ be nonzero elements of K and let S be a finite set of places of K of cardinality s. Then there are finitely many solutions $(x_1, \ldots, x_\ell) \in (O_S^\times)^\ell$ of the equation*

$$\delta_1 X_1 + \delta_2 X_2 + \cdots + \delta_\ell X_\ell = 1$$

for which no strict subsum

$$\sum_{i \in I} \delta_i x_i \qquad (\emptyset \neq I \subset \{1, \ldots, \ell\})$$

vanishes.

Make
everything
effective!

6. A family involving the simplest cubic fields

Write

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

where

$$\varepsilon_{1n}=\lambda_n, \quad \varepsilon_{2n}=\frac{1}{\lambda_n+1}, \quad \varepsilon_{3n}=\frac{\lambda_n+1}{\lambda_n}$$

are units of Shanks's simplest cubic fields $\mathbf{Q}(\varepsilon_{1n})$. Twist these equations by considering

$$F_{na}(X,Y)=(X-\varepsilon_{1n}^aY)(X-\varepsilon_{2n}^aY)(X-\varepsilon_{3n}^aY)$$

(a polynomial of $\mathbf{Z}[X,Y]$) and solve

$$F_{na}(X,Y)=\pm 1.$$

7. Linear forms in logarithms

Theorem (Baker).
Suppose that $\alpha_1, \ldots, \alpha_n$ *are nonzero algebraic numbers and that* $log(\alpha_1), \ldots, log(\alpha_n)$ *are linearly independent over the rational numbers. Then for all algebraic numbers* $\beta_0, \ldots, \beta_n$*, which are not all zero, we have*

$$|\beta_0 + \beta_1 log(\alpha_1) + \cdots + \beta_n log(\alpha_n)| > H^{-C}.$$

Here H *is the maximum of the heights of the elements* β_i *and* C *is an effectively computable number depending on* n*, on the elements* $log(\alpha_i)$*, and on the maximum* d *of the degrees of the elements* β_i*.*

Note. If β_0 is nonzero, then we may drop the assumption that the elements $\log \alpha_i$ are linearly independent.

8. Siegel's unit equation

Assume that $\alpha_1, \alpha_2, \alpha_3$ are algebraic integers and that x, y are 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**:

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

namely

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

which can also be written in the form

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

9. A diophantine tool.

Proposition *(Waldschmidt)*. *Let s and D be two positive integers. There exists an effectively computable positive constant κ, depending only upon s and D, with the following property. Let $\gamma_1, \ldots, \gamma_s$ be nonzero algebraic numbers generating a number field of degree $\leq D$. Let $c_1, \ldots, c_s$ be rational integers and let $H_1, \ldots, H_s$ be real numbers ≥ 1 satisfying*

$$\begin{cases} H_j \leq H_s & \textit{for} \quad 1 \leq j \leq s, \\ H_i \geq \mathrm{h}(\gamma_i) & \textit{for} \quad 1 \leq i \leq s. \end{cases}$$

Let C be a real number subject to

$$C \geq 2, \quad C \geq \max_{1 \leq j \leq s} \left\{ \frac{H_j}{H_s} |c_j| \right\} \cdot$$

Suppose also $\gamma_1^{c_1} \cdots \gamma_s^{c_s} \neq 1$. Then

$$|\gamma_1^{c_1} \cdots \gamma_s^{c_s} - 1| > \exp\{-\kappa H_1 \cdots H_s \log C\} \cdot$$

10. A family involving the simplest cubic fields (bis)

Write

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

where

$$\varepsilon_{1n}, \quad \varepsilon_{2n}, \quad \varepsilon_{3n}$$

are units of $\mathbf{Q}(\varepsilon_{1n})$. Twist these equations by considering

$$F_{na}(X,Y) = (X-\varepsilon_{1n}^a Y)(X-\varepsilon_{2n}^a Y)(X-\varepsilon_{3n}^a Y)$$

(a polynomial of $\mathbf{Z}[X,Y]$) and solve

$$F_{na}(X,Y) = \pm 1.$$

Theorem (Waldschmidt-L). *Let $m \geq 1$. There exist some absolute effectively computable constants $\kappa_1, \kappa_2, \kappa_3, \kappa_4$ and κ_5 such that if there exists $(n, a, m, x, y) \in \mathbf{Z}^5$ with $a \neq 0$ verifying*

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

then the following properties hold true:
(i) *When $m = 1$ and $max\{|x|, |y|\} \geq 2$, we have*

$$max\{|n|, |a|, |x], |y|\} \leq \kappa_2.$$

(ii) *We have*

$$\log max\{|x|, |y]\} \leq \kappa_3\mu$$

where

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

Let $c \in \{1, -1\}$ and let $n, a \in \mathbf{N}$ with $a \geq 1$. We wonder whether all the solutions $(x, y) \in \mathbf{Z}^2$ of $F_{na}(x, y) = c$ 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)					
$(0, 1)$	$(-9, 5)$	$(-1, 2)$	$(2, -1)$	$(4, -9)$	$(5, 4)$	$-$
$(0, 2)$	$(-14, 9)$	$(-3, -1)$	$(-2, -1)$	$(1, 5)$	$(3, 2)$	$(13, 4)$
$(0, 3)$	$(2, 1)$	$-$	$-$	$-$	$-$	$-$
$(0, 5)$	$(-3, -1)$	$(19, -1)$	$-$	$-$	$-$	$-$
$(1, 1)$	$(-3, 2)$	$(1, -3)$	$(2, 1)$	$-$	$-$	$-$
$(1, 2)$	$(-7, -2)$	$(-3, -1)$	$(2, 1)$	$(7, 3)$	$-$	$-$
$(2, 2)$	$(-7, -1)$	$(-2, -1)$	$-$	$-$	$-$	$-$
$(3, 1)$	$(-7, -2)$	$(-2, 9)$	$(9, -7)$	$-$	$-$	$-$
$(4, 2)$	$(3, 2)$	$-$	$-$	$-$	$-$	$-$

11. A familiy of cubic Thue equations

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

$$F(X, Y) = (X - \varepsilon_1 Y)(X - \varepsilon_2 Y)(X - \varepsilon_3 Y).$$

Twist with $a \in \mathbf{Z}, a \neq 0$, to obtain the polynomial of $\mathbf{Z}[X, Y]$:

$$F_a(X, Y) = (X - \varepsilon_1^a Y)(X - \varepsilon_2^a Y)(X - \varepsilon_3^a Y).$$

Theorem (Waldschmidt-L). *There exists a constant $\kappa > 0$, depending only on F, such that for any $m \geq 2$, each (x, y, a) in the set*

$$\left\{(x, y, a) \in \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z} \ : \ xya \neq 0, \ |F_a(x, y)| \leq m\right\}$$

satisfies

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

12. Involving a field with at most one real embedding.

Suppose that K is an algebraic number field of degree at least 3 which has at most one real embedding and that for any unit ε of K, $f_\varepsilon(X)$ is the minimal polynomial of ε. Let

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

Theorem (Waldschmidt-L). *There exists a constant $\kappa > 0$, depending only on K, such that for any $m \geq 2$, each triple (x, y, ε) in the set*

$$\Big\{(x, y, \varepsilon) \in \mathbf{Z} \times \mathbf{Z} \times \mathcal{O}_K^\times \,:\, xy \neq 0,\ \mathbf{Q}(\varepsilon) = K,\ |F_\varepsilon(x, y)| \leq m\Big\}$$

satisfies

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

13. A general result involving powers of units

Let $d \geq 3$ be a given integer. Let $F(X, Y)$ be a monic irreducible binary form in $\mathbf{Z}[X, Y]$ satisfying $F(0, 1) = \pm 1$ and that we write as

$$F(X, Y) = \prod_{j=1}^{d} (X - \alpha_j Y)$$

with $|\alpha_1| \leq |\alpha_2| \leq \cdots \leq |\alpha_d|$. Denote by R the regulator of the number field $\mathbf{Q}(\alpha_1)$. Further, let $\lambda = |\alpha_d|$. For $a \geq 0$, consider the polynomial of $\mathbf{Z}[X, Y]$ defined by

$$F_a(X, Y) = \prod_{j=1}^{d} (X - \alpha_j^a Y).$$

Theorem (Waldschmidt-L). *Assume that* α_1 *is not a root of unity. There exists an effectively computable constant* κ*, depending only on* d*, with the following property. Let* $(x, y, a) \in \mathbf{Z}^3$ *satisfy*

$$xy \neq 0, \quad [\mathbf{Q}(\alpha_1^a) : \mathbf{Q}] = d, \quad F_a(x, y) = \pm 1.$$

Then,

$$|a| \leq \kappa \lambda^{d^4} R \log R.$$

Moreover, there exists another effectively computable constant κ *such that*

$$max\{\log |x|, \log |y|\} < \kappa R \log(R)\big(R + |a| \log(\lambda)\big).$$

Our proof actually gives a much stronger estimate which depends on the following parameter $\mu > 1$ defined by

$$\mu = \begin{cases} \max\{2, \lambda\} & \text{if } |\alpha_1| = |\alpha_{d-1}| \text{ or } |\alpha_2| = |\alpha_d|, \\ \min\left\{ \dfrac{|\alpha_{d-1}|}{|\alpha_1|}, \dfrac{|\alpha_d|}{|\alpha_2|} \right\} & \text{if } |\alpha_1| < |\alpha_2| = |\alpha_{d-1}| < |\alpha_d|, \\ \dfrac{|\alpha_{d-1}|}{|\alpha_2|} & \text{if } |\alpha_2| < |\alpha_{d-1}|. \end{cases}$$

Theorem. *There exists an effectively computable constant κ such that*

$$|a| \le \kappa R \frac{\log \lambda}{\log \mu} (R + \log \lambda) \log(R + \log \lambda).$$

Thank you very much!
Merci beaucoup!
Dziękuję bardzo!
Mahalo nui loa!
Gracias! Gràcies!
Grazie!
Děkuji!
Ďakujem!
Obrigado!
Doumo arigatou gozaimasu!
Xièiè!
Gomabseubnida!
Dhanyavaad!