18 Mai 2015

18 - 29 mai 2015 : Oujda (Maroc)
École de recherche CIMPA-Oujda
Théorie des Nombres et ses Applications.

Équations diophantiennes et leurs applications.

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

The pdf file of this talk can be downloaded at URL
http://www.imj-prg.fr/~michel.waldschmidt/

Abstract

The study of Diophantine equations is among the oldest topics investigated by mathematicians. It is known that some problems will never be solved, yet fundamental progress has been achieved recently. We survey some of the main results and some of the main conjectures.

Diophantus of Alexandria

Diophantine equations

A Diophantine equation is an equation of the form

$$f(X_1, \ldots, X_n) = 0$$

where $f(X_1, \ldots, X_n) \in \mathbf{Z}[X_1, \ldots, X_n]$ is a given polynomial and the variables (sometimes called *unknowns*) $X_1, \ldots, X_n$ take their values $x_1, \ldots, x_n$ in $\mathbf{Z}$ (integer points) or in $\mathbf{Q}$ (rational points).

We will mainly consider integral points.

Diophantine equations

A Diophantine equation is an equation of the form

$$f(X_1, \dots, X_n) = 0$$

where $f(X_1, \dots, X_n) \in \mathbf{Z}[X_1, \dots, X_n]$ is a given polynomial and the variables (sometimes called *unknowns*) $X_1, \dots, X_n$ take their values $x_1, \dots, x_n$ in $\mathbf{Z}$ (integer points) or in $\mathbf{Q}$ (rational points).

We will mainly consider integral points.

Pierre Fermat (1601 ? –1665)

Fermat's Last Theorem.

Diophantine equations : 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

August 8, 1900

Second International Congress of Mathematicians in Paris.

David Hilbert (1862 – 1943)

Twin primes,

Goldbach's Conjecture,

Riemann Hypothesis

p://www.maa.org/sites/default/files/pdf/upload_library/22/Ford/Thiele1-24.pdf

Hilbert's 10th problem

http://logic.pdmi.ras.ru/Hilbert10/stat/stat.html

D. Hilbert (1900) —

Entscheidung der Lösbarkeit einer diophantischen Gleichung. Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoefficienten sei vorgelegt : man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

Determination of the solvability of a Diophantine equation. Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients : To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

Hilbert's 10th problem

http://logic.pdmi.ras.ru/Hilbert10/stat/stat.html

D. Hilbert (1900) —

Entscheidung der Lösbarkeit einer diophantischen Gleichung. Eine diophantische Gleichung mit irgendwelchen Unbekannten und mit ganzen rationalen Zahlkoefficienten sei vorgelegt : man soll ein Verfahren angeben, nach welchen sich mittels einer endlichen Anzahl von Operationen entscheiden lässt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.

Determination of the solvability of a Diophantine equation. Given a diophantine equation with any number of unknown quantities and with rational integral numerical coefficients : To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.

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 ?

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 ?

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 ?

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 ?

Axel Thue

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

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

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

Axel Thue

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

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

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

Über Annäherungswerte algebraischer Zahlen.

Von Herrn *Axel Thue* in Kristiania.

Theorem I. Bedeutet ϱ eine positive Wurzel einer ganzen Funktion vom Grade r mit ganzen Koeffizienten, so hat die Relation

$$(1.)\qquad 0 < |q\varrho - p| < \frac{c}{q^{\frac{r}{2}+k}},$$

wo c und k zwei beliebig gegebene positive Größen bezeichnen, nicht unendlich viele Auflösungen in ganzen positiven Zahlen p und q.

Die Richtigkeit hiervon ergibt sich gleich, wenn $r=1$ und wenn $r=2$.

Wir brauchen folglich nur zu zeigen, daß der Satz immer richtig ist, wenn die genannte Funktion irreduktibel ist und $r > 2$.

Um dieses Ziel zu erreichen, wollen wir zuerst zwei Hilfssätze entwickeln.

Erster Hilfssatz. Es sei ϱ eine beliebige Wurzel einer ganzen irreduktiblen Funktion F mit ganzen Koeffizienten und vom Grade $r > 2$.

Es seien ferner θ eine beliebig gewählte positive Größe $> \frac{2}{r}$ und n eine solche beliebige ganze positive Zahl, daß

$$(2.)\qquad \frac{2}{r-2} - \frac{\theta}{n-1} > \omega,$$

wo ω eine beliebig gegebene positive Größe $< \frac{2}{r-2}$ bedeutet.

Über Annäherungswerte algebraischer Zahlen.

Von Herrn *Axel Thue* in Kristiania.

Theorem I. Bedeutet ϱ eine positive Wurzel einer ganzen Funktion vom Grade r mit ganzen Koeffizienten, so hat die Relation

$$(1.)\qquad 0 < |q\varrho - p| < \frac{c}{q^{\frac{r}{2}+k}},$$

wo c und k zwei beliebig gegebene positive Größen bezeichnen, nicht unendlich viele Auflösungen in ganzen positiven Zahlen p und q.

JFM 40.0256.01 [Lampe, Prof. (Berlin)]

Thue, A.
Om en general i store hele tal ulösbar ligning. (Norwegian)
Christiania Vidensk. Selsk. Skr., Nr. 7, 15 S. Published : 1908

Die Gleichung $q^n F(p/q) = c$, wo $F(x)$ eine beliebige ganze irreduzible Funktion r-ten Grades $(r > 2)$ in x mit ganzzahligen Koeffizienten, c eine beliebige ganze Zahl bezeichnet, hat nur eine beschränkte Anzahl von ganzzahligen Lösungen in p und q (Rev. sem. 18_2, 104).

JFM 40.0265.01 [Fueter, Prof. (Basel)]

Thue, A.
Über Annäherungswerte algebraischer Zahlen. (German)
J. für Math. 135, 284-305. Published : (1909)

Bedeutet ϱ eine positive Wurzel einer ganzen Funktion vom Grade r mit ganzen Koeffizienten, so hat die Relation

$$0 < |q\varrho - p| < \frac{c}{q^{\frac{r}{2}+k}},$$

wo c und k zwei beliebige gegebene positive Grössen bezeichnen, nicht unendlich viele Auflösungen in ganzen positiven Zahlen p und q. Nach dem Beweise dieses Satzes wendet der Verf. denselben auf Kettenbrüche und auf die Frage nach der Auflösbarkeit einer in bezug auf p und q homogenen und irreduktiblen Funktion $U(p, q) = c$ in ganzen positiven Zahlen p und q an.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Proof.
We completed the proof in the case $p \leq (3/2)q$.
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

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

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

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

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

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

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

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

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

Consequence of an improvement of Liouville

Assume $(x, y) \in \mathbf{Z}^2$ with $x > 0$ satisfy

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

Since

$$x^3 - 2y^3 = (x - \sqrt[3]{2}y)(x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2),$$

we deduce that x is close to $\sqrt[3]{2}y$. Hence $x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2$ is close to $3x^2$. Being more careful, we deduce

$$x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2 \geq 4x^{0.5}y^{1.5}$$

and therefore

$$\left|\sqrt[3]{2} - \frac{x}{y}\right| \leq \frac{1}{4\ y^{2.5}},$$

a contradiction with Bennett's improvement of Liouville's inequality.

Consequence of an improvement of Liouville

Assume $(x, y) \in \mathbf{Z}^2$ with $x > 0$ satisfy

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

Since

$$x^3 - 2y^3 = (x - \sqrt[3]{2}y)(x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2),$$

we deduce that x is close to $\sqrt[3]{2}y$. Hence $x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2$ is close to $3x^2$. Being more careful, we deduce

$$x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2 \geq 4x^{0.5}y^{1.5}$$

and therefore

$$\left|\sqrt[3]{2} - \frac{x}{y}\right| \leq \frac{1}{4\ y^{2.5}},$$

a contradiction with Bennett's improvement of Liouville's inequality.

Consequence of an improvement of Liouville

Assume $(x, y) \in \mathbf{Z}^2$ with $x > 0$ satisfy

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

Since

$$x^3 - 2y^3 = (x - \sqrt[3]{2}y)(x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2),$$

we deduce that x is close to $\sqrt[3]{2}y$. Hence $x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2$ is close to $3x^2$. Being more careful, we deduce

$$x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2 \geq 4x^{0.5}y^{1.5}$$

and therefore

$$\left|\sqrt[3]{2} - \frac{x}{y}\right| \leq \frac{1}{4\ y^{2.5}},$$

a contradiction with Bennett's improvement of Liouville's inequality.

Consequence of an improvement of Liouville

Assume $(x, y) \in \mathbf{Z}^2$ with $x > 0$ satisfy

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

Since

$$x^3 - 2y^3 = (x - \sqrt[3]{2}y)(x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2),$$

we deduce that x is close to $\sqrt[3]{2}y$. Hence $x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2$ is close to $3x^2$. Being more careful, we deduce

$$x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2 \geq 4x^{0.5}y^{1.5}$$

and therefore

$$\left|\sqrt[3]{2} - \frac{x}{y}\right| \leq \frac{1}{4\ y^{2.5}},$$

a contradiction with Bennett's improvement of Liouville's inequality.

Consequence of an improvement of Liouville

Assume $(x, y) \in \mathbf{Z}^2$ with $x > 0$ satisfy

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

Since

$$x^3 - 2y^3 = (x - \sqrt[3]{2}y)(x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2),$$

we deduce that x is close to $\sqrt[3]{2}y$. Hence $x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2$ is close to $3x^2$. Being more careful, we deduce

$$x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2 \geq 4x^{0.5}y^{1.5}$$

and therefore

$$\left|\sqrt[3]{2} - \frac{x}{y}\right| \leq \frac{1}{4\ y^{2.5}},$$

a contradiction with Bennett's improvement of Liouville's inequality.

Consequence of an improvement of Liouville

Assume $(x, y) \in \mathbf{Z}^2$ with $x > 0$ satisfy

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

Since

$$x^3 - 2y^3 = (x - \sqrt[3]{2}y)(x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2),$$

we deduce that x is close to $\sqrt[3]{2}y$. Hence $x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2$ is close to $3x^2$. Being more careful, we deduce

$$x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2 \geq 4x^{0.5}y^{1.5}$$

and therefore

$$\left|\sqrt[3]{2} - \frac{x}{y}\right| \leq \frac{1}{4\; y^{2.5}},$$

a contradiction with Bennett's improvement of Liouville's inequality.

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*

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

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

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

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

Thue's equation 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 α real algebraic number 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 $\kappa > (d/2) + 1$.

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 $d \geq 2$, 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 equation

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 m 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

$$(X - \alpha_1 Y) \cdots (X - \alpha_n Y) = m$$

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 –)

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.*

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 $\mathbf{Q}$ of degree ≥ 3.

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

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

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 $\mathbf{Q}$ of degree ≥ 3.

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

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

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 $\mathbf{Q}$ of degree ≥ 3.

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

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



Diophantine equations : historical survey

Faltings's Theorem (1983) : finiteness of rational points on an algebraic curve of genus ≥ 2 over a number field.

A. Wiles (1993) : proof of Fermat's last Theorem

$$a^n + b^n = c^n \qquad (n \geq 3)$$

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

Diophantine equations : historical survey

Faltings's Theorem (1983) : finiteness of rational points on an algebraic curve of genus ≥ 2 over a number field.

A. Wiles (1993) : proof of Fermat's last Theorem

$$a^n + b^n = c^n \qquad (n \geq 3)$$

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

Diophantine equations : historical survey

Faltings's Theorem (1983) : finiteness of rational points on an algebraic curve of genus ≥ 2 over a number field.

A. Wiles (1993) : proof of Fermat's last Theorem

$$a^n + b^n = c^n \qquad (n \geq 3)$$

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



Effectivity

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.

Faltings's Theorem is not effective : so far, there is no known effective bound for the solutions $(x, y) \in \mathbf{Q}^2$ of a Diophantine equation $f(x, y) = 0$, where $f \in \mathbf{Z}[X, Y]$ is a polynomial such that the curve $f(x, y) = 0$ has genus ≥ 1.

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

Effectivity

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.

Faltings's Theorem is not effective : so far, there is no known effective bound for the solutions $(x, y) \in \mathbf{Q}^2$ of a Diophantine equation $f(x, y) = 0$, where $f \in \mathbf{Z}[X, Y]$ is a polynomial such that the curve $f(x, y) = 0$ has genus ≥ 1.

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

Effectivity

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.

Faltings's Theorem is not effective : so far, there is no known effective bound for the solutions $(x, y) \in \mathbf{Q}^2$ of a Diophantine equation $f(x, y) = 0$, where $f \in \mathbf{Z}[X, Y]$ is a polynomial such that the curve $f(x, y) = 0$ has genus ≥ 1.

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

Gel'fond–Baker method

A quite different approach to Thue's equation has been 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*

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

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*

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

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.

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. Györy (2006). . .

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. Györy (2006)...

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. Györy (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.

Thue's Fundamentaltheorem

Paul Voutier (2010)
Thue's fundamentaltheorem.
I. *The general case.*
II : *Some New Irrationality Measures*

Back to the Thue–Siegel–Roth Theorem

For any real algebraic irrational number α and for any $\epsilon > 0$, there exists $q_0 > 0$ such that, for $p/q \in \mathbf{Q}$ with $q \geq q_0$, we have

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^{2+\epsilon}}.$$

In other terms, the set of $(q, p) \in \mathbf{Z}^2 \setminus \{(0, 0)\}$ where the two independent linear forms

$$L_0(x_0, x_1) = x_0, \qquad L_1(x_0, x_1) = x_0\alpha - x_1$$

satisfy

$$|L_0(x_0, x_1)L_1(x_0, x_1)| \leq \max\{|x_0|, |x_1|\}^{-\epsilon}$$

is contained in a finite union of lines in $\mathbf{Q}^2$.

Back to the Thue–Siegel–Roth Theorem

For any real algebraic irrational number α and for any $\epsilon > 0$, there exists $q_0 > 0$ such that, for $p/q \in \mathbf{Q}$ with $q \geq q_0$, we have

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^{2+\epsilon}}.$$

In other terms, the set of $(q, p) \in \mathbf{Z}^2 \setminus \{(0,0)\}$ where the two independent linear forms

$$L_0(x_0, x_1) = x_0, \qquad L_1(x_0, x_1) = x_0\alpha - x_1$$

satisfy

$$|L_0(x_0, x_1)L_1(x_0, x_1)| \leq \max\{|x_0|, |x_1|\}^{-\epsilon}$$

is contained in a finite union of lines in $\mathbf{Q}^2$.

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 . . .








Thue–Mahler equation

Let K be a number field, G a finitely generated subgroup of $K^\times$, $\alpha_1, \ldots, \alpha_n$ elements in K with $\mathrm{Card}\{\alpha_1, \ldots, \alpha_n\} \geq 3$. Then there are only finitely many $(x, y) \in \mathbf{Z} \times \mathbf{Z}$ with $\gcd(x, y) = 1$ satisfying the Thue–Mahler equation

$$(x - \alpha_1 y) \cdots (x - \alpha_n y) \in G.$$

(Kurt Mahler 1933)

An exponential Diophantine equation

The only solutions of the equation

$$2^a + 3^b = 5^c$$

where the values of the unknowns a, b, c are nonnegative integers are $(a, b, c) = (1, 1, 1)$, $(2, 0, 1)$, $(4, 2, 2)$:

$$2 + 3 = 5, \quad 4 + 1 = 5, \quad 16 + 9 = 25.$$

The more general exponential Diophantine equation

$$2^{a_1} 3^{a_2} + 3^{b_1} 5^{b_2} = 2^{c_1} 5^{c_2}$$

has only finitely many solutions $(a_1, a_2, b_1, b_2, c_1, c_2)$.

An exponential Diophantine equation

The only solutions of the equation

$$2^a + 3^b = 5^c$$

where the values of the unknowns a, b, c are nonnegative integers are $(a, b, c) = (1, 1, 1)$, $(2, 0, 1)$, $(4, 2, 2)$:

$$2 + 3 = 5, \quad 4 + 1 = 5, \quad 16 + 9 = 25.$$

The more general exponential Diophantine equation

$$2^{a_1} 3^{a_2} + 3^{b_1} 5^{b_2} = 2^{c_1} 5^{c_2}$$

has only finitely many solutions $(a_1, a_2, b_1, b_2, c_1, c_2)$.

S–unit equations – rational case

Let $S = \{p_1, \ldots, p_s\}$ be a finite set of prime numbers. Then the equation

$$u_1 + u_2 = u_3,$$

where the values of the unknowns u_1, u_2, u_3 are relatively prime integers divisible only by the prime numbers in S, has only finitely many solutions.

Notice that for any prime number p, the equation

$$u_1 + u_2 + u_3 = u_4$$

has infinitely many solutions in rational integers u_1, u_2, u_3 divisible only by p and $\gcd(u_1, u_2, u_3, u_4) = 1$: for instance

$$p^a + (-p^a) + 1 = 1 \quad \text{for any} \quad a \geq 0.$$

S–unit equations – rational case

Let $S = \{p_1, \ldots, p_s\}$ be a finite set of prime numbers. Then the equation

$$u_1 + u_2 = u_3,$$

where the values of the unknowns u_1, u_2, u_3 are relatively prime integers divisible only by the prime numbers in S, has only finitely many solutions.

Notice that for any prime number p, the equation

$$u_1 + u_2 + u_3 = u_4$$

has infinitely many solutions in rational integers u_1, u_2, u_3 divisible only by p and $\gcd(u_1, u_2, u_3, u_4) = 1$: for instance

$$p^a + (-p^a) + 1 = 1 \quad \text{for any} \quad a \geq 0.$$

A consequence of Schmidt's Subspace Theorem

Let $S = \{p_1, \ldots, p_s\}$ be a finite set of prime numbers and let $n \geq 2$. Then the equation

$$u_1 + u_2 + \cdots + u_n = 1,$$

where the values of the unknowns $u_1, u_2, \cdots, u_n$ are rational numbers with numerators and denominators divisible only by the prime numbers in S for which no nontrivial subsum

$$\sum_{i \in I} u_i \qquad \emptyset \neq I \subset \{1, \ldots, n\}$$

vanishes, has only finitely many solutions.

Finitely generated subgroup of $\mathbf{Q}^\times = \mathbf{Q} \setminus \{0\}$

If $S = \{p_1, \ldots, p_s\}$ is a finite set of prime numbers, the set of rational numbers with numerators and denominators divisible only by the prime numbers in S is a finitely generated subgroup of $\mathbf{Q}^\times$.

Indeed it is generated by $-1, p_1, \ldots, p_s$.

Conversely, if G is a finitely generated subgroup of $\mathbf{Q}^\times$, then there exists a finite set $S = \{p_1, \ldots, p_s\}$ of prime numbers such that G is contained in the set of rational numbers with numerators and denominators divisible only by the prime numbers in S.

Indeed, if $g_1, \ldots, g_t$ is a set of generators of G, then the set of prime divisors of the numerators and denominators of the g_i is a solution.

Finitely generated subgroup of $\mathbf{Q}^\times = \mathbf{Q} \setminus \{0\}$

If $S = \{p_1, \ldots, p_s\}$ is a finite set of prime numbers, the set of rational numbers with numerators and denominators divisible only by the prime numbers in S is a finitely generated subgroup of $\mathbf{Q}^\times$.

Indeed it is generated by $-1, p_1, \ldots, p_s$.

Conversely, if G is a finitely generated subgroup of $\mathbf{Q}^\times$, then there exists a finite set $S = \{p_1, \ldots, p_s\}$ of prime numbers such that G is contained in the set of rational numbers with numerators and denominators divisible only by the prime numbers in S.

Indeed, if $g_1, \ldots, g_t$ is a set of generators of G, then the set of prime divisors of the numerators and denominators of the g_i is a solution.

Finitely generated subgroup of $\mathbf{Q}^\times = \mathbf{Q} \setminus \{0\}$

If $S = \{p_1, \dots, p_s\}$ is a finite set of prime numbers, the set of rational numbers with numerators and denominators divisible only by the prime numbers in S is a finitely generated subgroup of $\mathbf{Q}^\times$.

Indeed it is generated by $-1, p_1, \dots, p_s$.

Conversely, if G is a finitely generated subgroup of $\mathbf{Q}^\times$, then there exists a finite set $S = \{p_1, \dots, p_s\}$ of prime numbers such that G is contained in the set of rational numbers with numerators and denominators divisible only by the prime numbers in S.

Indeed, if $g_1, \dots, g_t$ is a set of generators of G, then the set of prime divisors of the numerators and denominators of the g_i is a solution.

Finitely generated subgroup of $\mathbf{Q}^\times = \mathbf{Q} \setminus \{0\}$

If $S = \{p_1, \dots, p_s\}$ is a finite set of prime numbers, the set of rational numbers with numerators and denominators divisible only by the prime numbers in S is a finitely generated subgroup of $\mathbf{Q}^\times$.

Indeed it is generated by $-1, p_1, \dots, p_s$.

Conversely, if G is a finitely generated subgroup of $\mathbf{Q}^\times$, then there exists a finite set $S = \{p_1, \dots, p_s\}$ of prime numbers such that G is contained in the set of rational numbers with numerators and denominators divisible only by the prime numbers in S.

Indeed, if $g_1, \dots, g_t$ is a set of generators of G, then the set of prime divisors of the numerators and denominators of the g_i is a solution.

The generalized S–unit equation

Let K be a field of characteristic zero, let G be a finitely multiplicative subgroup of the multiplicative group $K^\times = K \setminus \{0\}$ and let $n \geq 2$. Then the equation

$$u_1 + u_2 + \cdots + u_n = 1,$$

where the values of the unknowns $u_1, u_2, \cdots, u_n$ are in G for which no nontrivial subsum

$$\sum_{i \in I} u_i \qquad \emptyset \neq I \subset \{1, \ldots, n\}$$

vanishes, has only finitely many solutions.

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.

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

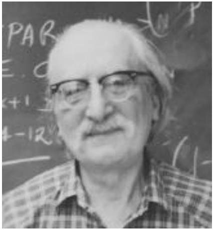
$$F_n(X, Y) = X^3 - (n-1)X^2Y - (n+2)XY^2 - Y^3.$$

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

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

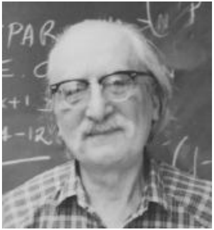
Then

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

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.

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 $F_n(x, y) = 1$.

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 $F_n(x, y) = 1$.

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 $F_3(x,y) = 1$:

$(-7,-2)$, $(-2,9)$, $(9,-7)$

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 $F_3(x, y) = 1$:

$(-7, -2)$, $(-2, 9)$, $(9, -7)$

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.

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 (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.

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.

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) :

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

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) :

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

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) :

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

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

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 $a = 2$

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 ?

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 $m \geq 1$. 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

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

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 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 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.

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.

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

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

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

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

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

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

satisfies

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

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

$$\begin{cases} n + \frac{1}{n} & \leq \lambda_0 \leq & n + \frac{2}{n}, \\ -\frac{1}{n+1} & \leq \lambda_1 \leq & -\frac{1}{n+2}, \\ -1 - \frac{1}{n} & \leq \lambda_2 \leq & -1 - \frac{1}{n+1}. \end{cases}$$

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

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

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

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

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)

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

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

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

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

Sketch of proof (continued)

The Siegel equation

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

leads to the identity

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

and the estimate

$$0 < \left| \frac{\gamma_{i_1,a}(\lambda^a_{i_2} - \lambda^a_{i_0})}{\gamma_{i_2,a}(\lambda^a_{i_1} - \lambda^a_{i_0})} - 1 \right| \leq \frac{2}{y^3 \lambda^a_0}.$$

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)

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)

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

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

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

A. Togbé considered the family of equations

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

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

Families of Thue equations (continued)

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

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

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)

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...

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




18 Mai 2015

18 - 29 mai 2015 : Oujda (Maroc)
École de recherche CIMPA-Oujda
Théorie des Nombres et ses Applications.

Équations diophantiennes et leurs applications.

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

The pdf file of this talk can be downloaded at URL
http://www.imj-prg.fr/~michel.waldschmidt/