ICCGNFRT-2017 Proceedings, HRI Allahabad

Thue Diophantine Equations

A survey

Michel Waldschmidt

Abstract This text includes an extended abstract of a keynote talk under the title *Families of Thue equations associated with a rank one subgroup of the unit group of a number field* given on September 4, 2017 at the Harish-Chandra Research Institute (HRI), Allahabad (India), for the International Conference on Class Groups of Number Fields and Related Topics (ICCGNFRT-2017) based on notes by Kristýna Zemková. Some more information is added, including references, especially to joint works with Claude Levesque.

Keywords Thue equations · Diophantine equations · Baker's method · Linear forms in logarithms, Diophantine approximation

Mathematics Subject Classification (2000) MSC 11D59

1 Thue equations

1.1 Introduction

A *Thue equation* is a Diophantine equation of the form $F(x,y) = m$, where $F \in \mathbb{Z}[X,Y]$ is a given homogeneous polynomial in two variables (i.e. a binary form) of degree d with integer coefficients, m is a given non zero integer while the unknowns x,y take their values in $\mathbb{Z}$. Is the set of such (x,y) finite or infinite? If it is finite, can we get an upper bound for the number of its elements? (Such an upper bound is a qualitative statement). Can we get an upper bound for the height of its elements? (Such an upper bound is a quantitative statement).

A *Thue–Mahler equation* is an exponential Diophantine equation of the form $F(x,y) = p_1^{z_1} \cdots p_s^{z_s}$ where F is a given binary form, $p_1, \ldots, p_s$ are given prime num-

Michel WALDSCHMIDT
Sorbonne Université, CNRS, Institut de Mathématiques de Jussieu – Paris Rive Gauche, IMJ–PRG, F – 75005 Paris, France
E-mail: michel.waldschmidt@imj-prg.fr
http://www.imj-prg.fr/~michel.waldschmidt

bers, the unknowns are $x, y, z_1, \dots, z_s$ where x, y take their values in $\mathbb{Z}$ and $z_1, \dots, z_s$ in $\mathbb{Z}_{\ge 0}$.

We denote by $f \in \mathbb{Z}[T]$ the polynomial defined by $f(T) = F(T,1)$:

$$f(T) = a_0 T^d + a_1 T^{d-1} + \cdots + a_{d-1} T + a_d,$$
$$F(X,Y) = a_0 X^d + a_1 X^{d-1} Y + \cdots + a_{d-1} X Y^{d-1} + a_d Y^d,$$

Notice that $a_0 = 0$ is equivalent to saying that $F(X,0)$ is the zero polynomial. We assume $a_0 > 0$, so that f has degree d.

For $m = 0$, the set of $(x,y) \neq (0,0)$ in $\mathbb{Z}^2$ such that $F(x,y) = 0$ is empty if f has no rational root, while, if f has rational roots, then this set is the set of (x,y) with $y \neq 0$ such that x/y is a root of f.

From now on we assume $m \neq 0$.

When $d = 1$, we have $F(X,Y) = a_0 X + a_1 Y$; the solution of a linear equation $a_0 x + a_1 y = m$ is given by Bézout's Theorem. The computation of the gcd of a_0 and a_1 is done efficiently via the Euclidean algorithm, which is nothing else than the continued fraction expansion algorithm applied to a_1/a_0.

Assume $d = 2$. The quadratic equation $a_0 x^2 + a_1 xy + a_2 y^2 = m$ may have no solution or finitely many solutions: one among many examples is for $(a_0, a_1, a_2) = (1,0,1)$ with the equation $x^2 + y^2 = m$. It may have infinitely many solutions; this is the case for $(a_0, a_1, a_2) = (1,0,-D)$ and $m = 1$, where D is a positive integer which is not a square, with the Brahmagupta–Fermat–Pell equation $x^2 - Dy^2 = 1$. The general solution of the quadratic equation (not necessarily a Thue equation) is due to Lagrange [Mo 1969,F 1991].

Assume now $d > 2$. If f is a reducible polynomial in $\mathbb{Z}[X]$, then solving the equation $F(x,y) = m$, where the unknowns x, y take their values in the set of rational integers, amounts to solving finitely many equations $F_i(x,y) = m_i$ with m_i a divisor of m and $F_i(X,Y)$ an irreducible factor of $F(X,Y)$ in $\mathbb{Z}[X,Y]$. For this reason we assume now that f is irreducible in $\mathbb{Z}[X]$.

1.2 Positive definite binary forms

Assume first that the polynomial f has no real root (hence its degree d is even). Then for each $m \in \mathbb{Z}$, $m \neq 0$, the set of (x,y) in $\mathbb{Z}^2$ such that $F(x,y) = m$ is finite. To study the Diophantine equation $F(x,y) = m$ means to study the representation of integers by the definite form F. Let us quote the following elementary lemma 2.1 from [FLW 2018].

Lemma 1 *Let $f \in \mathbb{Z}[T]$ be a nonzero polynomial of degree d which has no real root. Let $g(T) = T^d f(1/T)$. Assume that the leading coefficient of $f(T)$ is positive, so that the real number, defined by*

$$\gamma = \min\left\{ \inf_{-1 \le t \le 1} f(t), \quad \inf_{-1 \le t \le 1} g(t) \right\}$$

is > 0. *Let* $F(X,Y)$ *be the binary form* $Y^d f(X/Y)$ *associated with* f. *Then for each* $(x,y) \in \mathbb{Z}^2$, *we have*

$$F(x,y) \geq \gamma \max\{|x|^d, |y|^d\}.$$

Moreover, for any real number c *with* $c > \gamma$, *there exist infinitely many couples* (x,y) *in* $\mathbb{Z}^2$ *satisfying*

$$F(x,y) < c \max\{|x|^d, |y|^d\}.$$

A class of definite forms F (namely, forms which are associated with a polynomial f without real root) is given by the norm over $\mathbb{Q}$ of a CM field. Recall that a subfield K of $\mathbb{C}$ is a CM field if it is a number field which satisfies the following equivalent conditions:
(i) K is totally imaginary and is a quadratic extension of a totally real field.
(ii) There exists $\gamma \in K$ such that $K = \mathbb{Q}(\gamma)$ and γ^2 is totally real with all conjugates negative.
(iii) K is not real and the complex conjugation $z \to \overline{z}$ commutes with every embedding of K into $\mathbb{C}$: for $\sigma : K \to \mathbb{C}$ and $\alpha \in K$,

$$\overline{\sigma(\alpha)} = \sigma(\overline{\alpha}).$$

Theorem 1 (K. Győry, [G 1977]) *Let* K *be a CM field of degree* d *over* $\mathbb{Q}$. *Let* $\alpha \in K$ *be such that* $K = \mathbb{Q}(\alpha)$; *let* f *be the irreducible polynomial of* α *over* $\mathbb{Q}$ *and let* $F(X,Y) = Y^d f(X/Y)$ *the associated homogeneous binary form. Set* $a_0 = F(1,0)$, $a_d = F(0,1)$. *For* $(x,y) \in \mathbb{Z}^2$ *we have*

$$x^d \leq 2^d a_d^{d-1} F(x,y) \quad \textit{and} \quad y^d \leq 2^d a_0^{d-1} F(x,y).$$

Recall that the leading coefficient a_0 of the irreducible polynomial of α is positive. The assumption implies that α is totally imaginary, hence $a_d > 0$ and $F(x,y) > 0$ for $(x,y) \neq (0,0)$.

Proof Let $\alpha_1, \ldots, \alpha_d$ be the roots of f in $\mathbb{C}$, so that

$$F(X,Y) = a_0(X - \alpha_1 Y) \cdots (X - \alpha_d Y).$$

For $1 \leq j \leq d$, the number α_j is not real (since K is totally imaginary) and we have

$$|x - \alpha_j y| \geq |\Im\mathrm{m}(\alpha_j) y|.$$

Since K is a CM field, $\overline{\alpha}$ is in K and $2i\Im\mathrm{m}(\alpha) = \alpha - \overline{\alpha}$ is a nonzero element in K; its conjugates in $\mathbb{C}$ are $\alpha_j - \overline{\alpha_j}$. Moreover, $a_0(\alpha - \overline{\alpha})$ being a nonzero algebraic integer, its norm is a nonzero rational integer, of absolute value ≥ 1. Therefore

$$2^d a_0^{d-1} F(x,y) = y^d \mathrm{N}_{K/\mathbb{Q}}(2ia_0 \Im\mathrm{m}(\alpha)) \geq y^d.$$

The same argument gives the upper bound for x^d. □

In the special case where α is a unit in K, we have $a_0 = a_d = 1$ and the conclusion can be written

$$\max\{|x|,|y|\} \le 2F(x,y)^{1/d}. \tag{1}$$

Examples of binary forms satisfying the assumptions of Theorem 1 with $a_0 = a_d = 1$ are given by the cyclotomic binary forms, which we define as follows.

For $n \ge 1$, denote by $\phi_n(T)$ the cyclotomic polynomial of index n and degree $\varphi(n)$ (Euler's totient function). The *cyclotomic binary form* $\Phi_n(X,Y)$ is defined by $\Phi_n(X,Y) = Y^{\varphi(n)}\phi_n(X/Y)$. In particular, we have $\Phi_n(x,y) > 0$ for $n \ge 3$ and $(x,y) \ne (0,0)$.

An example showing that the estimate (1) is optimal is given by the form $F(X,Y) = \Phi_n(X-Y,Y)$ of degree $d = \varphi(n)$, where $n \ge 3$ is not of the form p^r nor $2p^r$ with p prime. This condition on n implies $\phi_n(1) = \phi_n(-1) = 1$, hence for $y \in \mathbb{Z}$ we have

$$F(2y,y) = y^d F(2,1) = y^d \phi_n(1) = y^d.$$

The irreducible polynomial of the unit $\alpha = 1+\zeta_n$ is $\phi_n(t-1)$ and the field $\mathbb{Q}(\alpha)$ is the CM field $\mathbb{Q}(\zeta_n)$.

In the special case of cyclotomic binary forms, Theorem 1 gives

$$\max\{|x|,|y|\} \le 2|m|^{1/\varphi(n)}$$

for the integral solutions (n,x,y) of $\Phi_n(x,y) = m$. An upper bound for n can be deduced only if $\max\{|x|,|y|\} \ge 3$.

In [FLW 2018], the refined estimate

$$\max\{|x|,|y|\} \le \frac{2}{\sqrt{3}}|m|^{1/\varphi(n)}$$

has been proved for the integral solutions (n,x,y) of $\Phi_n(x,y) = m$ satisfying $n \ge 3$ and $\max\{|x|,|y|\} \ge 2$. Therefore

$$\varphi(n) \le \frac{2}{\sqrt{3}}\log m.$$

See [OEIS, A296095, A299214, A293654, A301429 and A301430].

1.3 Thue equation and Diophantine approximation

We now come back to the general case where $f \in \mathbb{Z}[T]$ is irreducible over $\mathbb{Q}$ of degree $d \ge 3$ and may have real zeroes. Write

$$f(T) = a_0(T-\alpha_1)(T-\alpha_2)\cdots(T-\alpha_d).$$

Recall our assumption $a_0 > 0$. Assume $m \ne 0$ is fixed while x,y are rational integers with $F(x,y) = m$. Let us show that, as soon as $\max\{|x|,|y|\}$ is sufficiently large, x/y is close to one of the roots α_i of f and is not close to any other root (since f is

irreducible, the roots α_i are distinct). For $i = 1, \ldots, d$, define $\beta_i = x - \alpha_i y$. Label the roots of f so that

$$|\beta_1| = \min_{1 \le i \le d} |\beta_i|.$$

From $a_0 \beta_1 \cdots \beta_d = m$ we deduce

$$|\beta_1|^d \le \frac{|m|}{a_0},$$

which means

$$\left| \alpha_1 - \frac{x}{y} \right| \le \frac{|m|^{1/d}}{a_0^{1/d} |y|}. \tag{2}$$

We may notice that if α_1 is not real, then we get immediately a sharp upper bound for $|y|$:

$$|y| \le \frac{|m|^{1/d}}{a_0^{1/d} |\Im\mathrm{m}(\alpha_1)|}.$$

We now sharpen the upper bound (2). If

$$|y| \le \frac{2|m|^{1/d}}{a_0^{1/d} \min\limits_{2 \le i \le d} |\alpha_i - \alpha_1|},$$

then the relation $x = \alpha_1 y + \beta_1$ implies the upper bound

$$|x| \le \left(\frac{2|\alpha_1|}{\min\limits_{2 \le i \le d} |\alpha_i - \alpha_1|} + 1 \right) \frac{|m|^{1/d}}{a_0^{1/d}},$$

which shows that $|x|$ and $|y|$ are bounded. Assume now

$$|y| > \frac{2|m|^{1/d}}{a_0^{1/d} \min\limits_{2 \le i \le d} |\alpha_i - \alpha_1|}.$$

For $i = 2, \ldots, d$, we have $\beta_i = (\alpha_1 - \alpha_i) y + \beta_1$, hence

$$|\beta_i| = |x - \alpha_i y| \ge |(\alpha_i - \alpha_1) y| - \frac{|m|^{1/d}}{a_0^{1/d}} \ge \frac{1}{2} |(\alpha_i - \alpha_1) y|,$$

which implies

$$|m| = |a_0 \beta_1 \cdots \beta_d| \ge |y|^{d-1} |\beta_1| \frac{1}{2^{d-1}} a_0 \prod_{i=2}^{d} |\alpha_i - \alpha_1|$$

and therefore we deduce the following improvement of the upper bound (2):

$$\left| \alpha_1 - \frac{x}{y} \right| \le \frac{\kappa_1(f) |m|}{|y|^d}$$

with

$$\kappa_1(f) = \frac{2^{d-1}}{a_0 \prod_{i=2}^{d} |\alpha_i - \alpha_1|}.$$

Liouville's estimate is the lower bound

$$\left|\alpha_1 - \frac{x}{y}\right| \geq \frac{\kappa_2(f)}{|y|^d}$$

with some explicit constant $\kappa_2(f)$; this does not give any information on the Thue Diophantine equation, but any non trivial improvement of Liouville's estimate gives a non trivial information on the equation $F(x,y) = m$ (see [W 1986, LW 2011]). The work by Thue in 1914 culminated with the proof by Roth in 1955 of the following result:

Theorem 2 (Thue, Siegel, Roth) *If α is an algebraic number of degree $d \geq 2$, for any $\varepsilon > 0$ there exists a positive constant $\kappa(\alpha, \varepsilon)$ such that, for any rational number p/q with $q > 0$, we have*

$$\left|\alpha - \frac{p}{q}\right| > \frac{\kappa(\alpha, \varepsilon)}{q^{2+\varepsilon}}.$$

From the previous argument we deduce

Corollary 1 (A. Thue) *Let $F \in \mathbb{Z}[X,Y]$ be an irreducible binary form of degree $d \geq 3$. Let $m \in \mathbb{Z}$. Then there are only finitely many (x,y) in $\mathbb{Z} \times \mathbb{Z}$ such that $F(x,y) = m$.*

One main drawback of this argument is that the proof following the original approach by Thue does not produce an effective value for the constant $\kappa(\alpha, \varepsilon)$ when ε is less than $d-2$. As a consequence, Corollary 1 is not effective; as a matter of fact, upper bounds for the number of solutions (x,y) to the Diophantine equation $F(x,y) = m$ (qualitative statements) can be derived from the proof, but no upper bound for $\max\{|x|, |y|\}$ can be obtained (quantitative statements). We will discuss below (see §2) another approach which has been suggested by A.O. Gel'fond and worked out by A. Baker, involving lower bounds for linear forms in logarithms - and it is effective.

An illuminating presentation of Thue's method is given by D.W. Masser in [M 2016], Chap. 12, where he starts with $x^3 - 2y^3 = m$ and goes on by explaining some of the main ideas behind Thue's proof, building upon Newton's method.

1.4 An example: $x^3 - 2y^3 = m$

Let us consider the special case of the cubic Thue equation $x^3 - 2y^3 = m$ (see [W 1986]). Let ψ be a positive real function which satisfies

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{\psi(q)}{q^3}$$

for each $q > 0$. Let $m \in \mathbb{Z}$, $m \neq 0$ and let $(x,y) \in \mathbb{Z}^2$ satisfy $x^3 - 2y^3 = m$. Assume x and y are positive (this is no loss of generality). Write

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

and observe that $x^2 + \sqrt[3]{2}xy + \sqrt[3]{4}y^2 > y^2$. We deduce that any solution (x,y) in positive integers of the equation $x^3 - 2y^3 = m$ satisfies

$$\psi(y) \leq |m|. \tag{3}$$

If $\psi(q)$ tends to infinity with q, then we get an upper bound for y, while x is bounded by

$$x \leq \sqrt[3]{2}\max\{\sqrt[3]{|m|}, \sqrt[3]{2}y\}.$$

In the other direction, let ψ be a positive real function such that any solution (x,y) in positive rational integers of $x^3 - 2y^3 = m$ satisfies

$$\psi(y) \leq |m|.$$

We write

$$|p^3 - 2q^3| = \left|\sqrt[3]{2} - \frac{p}{q}\right| (p^2 + \sqrt[3]{2}pq + \sqrt[3]{4}q^2)q.$$

If $p \leq (3/2)q$, we have $p^2 + \sqrt[3]{2}pq + \sqrt[3]{4}q^2 \leq 6q^2$ and we deduce

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| \geq \frac{\psi(q)}{6q^3}.$$

If $p > (3/2)q$, then we have the sharper estimate

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{3}{2} - \sqrt[3]{2} > \frac{1}{5}.$$

Liouville's estimate

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{6q^3} \tag{4}$$

follows by taking for ψ the constant function $\psi(y) = 1$, while any upper bound for the solutions (x,y) of $x^3 - 2y^3 = m$ implies the validity of (3) with a function $\psi(y)$ tending to infinity with y, and this yields an improvement on Liouville's estimate (4).

In this direction, the sharpest known estimates are due to M. Bennett [Be 1997a]:

$$\left|\sqrt[3]{2} - \frac{p}{q}\right| > \frac{1}{4q^{2.5}} \quad \text{and} \quad |x^3 - 2y^3| \geq \sqrt{x}.$$

See also [Be 1997b] for similar results concerning other algebraic numbers than $\sqrt[3]{2}$.

2 Solving Thue equation using Baker's method

2.1 References

Here is a selection of books having a section devoted to Baker's method for solving Thue equations.
• [Ba 1975] Chap. 4 (Diophantine equations) §2 The Thue equation - proof using lower bounds for linear forms in logarithms.
• [SVTS 1977] Main results arising from Baker's method in 1977, with proofs using lower bounds for linear forms in logarithms.
• [ST 1986] Chap. 5 (The Thue equation) proof using lower bounds for linear forms in logarithms. Includes effective estimates.
• [Sp 1982] Chap. IV (The Thue Equation).
• [BW 2007] Chap. 3 (Diophantine problems) §3 The Thue equation - sketch of proof using lower bounds for linear forms in logarithms.
• [G 2002] Survey of some important applications of Baker's theory of linear forms in logarithms to Diophantine equations.
• [EG 2015] Chap. 9 (Decomposable forms equations) §9.6 (Effective results) §9.6.1 (Thue equations) Explicit results.
• [Bu 2018] Chap. 4 §3 (The Thue equation).

2.2 Thue equation and Siegel's unit equation

We explain some of the basic ideas behind the reduction of the Diophantine equation $F(x,y) = m$ to Siegel's unit equation.

Assume for simplicity $a_0 = 1$, $a_d = \pm 1$, $m = 1$, so that the polynomial f can be written

$$f(T) = T^d + a_1 T^{d-1} + \cdots + a_{d-1}T \pm 1 = (T-\alpha_1)\cdots(T-\alpha_d)$$

where $\alpha_1, \ldots, \alpha_d$ are units of degree d. The numbers $\beta_i = x - \alpha_i y$ $(i = 1, \ldots, d)$ are also units of degree d, since they are algebraic integers satisfying $\beta_1 \cdots \beta_d = 1$. If i_1, i_2, i_3 are distinct indices in $\{1, \ldots, d\}$ (recall $d \geq 3$), eliminating x and y among the three relations

$$\beta_{i_1} = x - \alpha_{i_1} y, \quad \beta_{i_2} = x - \alpha_{i_2} y, \quad \beta_{i_3} = x - \alpha_{i_3} y$$

shows that the determinant

$$\begin{vmatrix} 1 & -\alpha_{i_1} & \beta_{i_1} \\ 1 & -\alpha_{i_2} & \beta_{i_2} \\ 1 & -\alpha_{i_3} & \beta_{i_3} \end{vmatrix}$$

is 0. This yields the so–called *Siegel unit equation*

$$\beta_{i_1}(\alpha_{i_2} - \alpha_{i_3}) + \beta_{i_2}(\alpha_{i_3} - \alpha_{i_1}) + \beta_{i_3}(\alpha_{i_1} - \alpha_{i_2}) = 0.$$

The main result on Siegel's unit equation is that given γ_1, γ_2 in $K^\times$, the set of pairs (u_1, u_2) of units in a number field K satisfying $\gamma_1 u_1 + \gamma_2 u_2 = 1$ is finite. In homogeneous form, the result is the following: if $\gamma_1, \gamma_2, \gamma_3$ are in $K^\times$, if we consider the equation $\gamma_1 u_1 + \gamma_2 u_2 + \gamma_3 u_3 = 0$, then the set of $(u_1/u_3, u_2/u_3)$ is finite. Baker's method gives an effective upper bound for the heights of the solutions.

Once we know that the set of numbers

$$\frac{\beta_{i_1}(\alpha_{i_2} - \alpha_{i_3})}{\beta_{i_2}(\alpha_{i_3} - \alpha_{i_1})},$$

for (x, y) solution of $F(x, y) = m$, is finite, we deduce that the set of quotients β_{i_1}/β_{i_2} is finite, hence x/y belongs to a finite set E; if $y = \nu x$ with $\nu \in E$, then $F(x, y) = x^d F(1, \nu)$ and the equation $x^d F(1, \nu) = m$ yields the desired upper bound for $|x|$.

2.3 Lower bounds for linear forms in logarithms and Siegel's unit equation

Let $\alpha_1, \ldots, \alpha_n$ be nonzero algebraic numbers and $b_1, \ldots, b_n$ be rational integers such that

$$\alpha_1^{b_1} \cdots \alpha_n^{b_n} \neq 1.$$

Define $B = \max\{2, |b_1|, \ldots, |b_n|\}$. A "trivial" estimate "à la Liouville" is

$$|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| \geq e^{-C_1 B},$$

where C_1 is an explicit constant depending only on $\alpha_1, \ldots, \alpha_n$. Methods from transcendental number theory involving the quantity $\beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n$ yield the refinement

$$|\alpha_1^{b_1} \cdots \alpha_n^{b_n} - 1| \geq B^{-C_2}, \tag{5}$$

where C_2 is also an explicit constant depending only on $\alpha_1, \ldots, \alpha_n$. This estimate is optimal as far as the dependence on B is concerned (but optimal estimates for C_2 have not yet been achieved).

Let γ_1, γ_2 be non zero elements in a number field K. Let $\varepsilon_1, \ldots, \varepsilon_r$ be a basis of the group of units of K. Let (u_1, u_2) be two units in K such that

$$\gamma_1 u_1 + \gamma_2 u_2 = 1.$$

We write

$$\frac{u_1}{u_2} = \zeta \varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r}$$

where ζ is a root of unity in K and $b_1, \ldots, b_r$ are rational integers. Set

$$\gamma_0 = \frac{-\gamma_1 \zeta}{\gamma_2}.$$

We use the fundamental Diophantine estimate (5) to obtain a lower bound for the modulus of any complex conjugate of the left hand side of

$$\gamma_0 \varepsilon_1^{b_1} \cdots \varepsilon_r^{b_r} - 1 = \frac{-1}{\gamma_2 u_2}$$

An auxiliary lemma (e.g. Lemma 5.1 of [ST 1986] or Lemma 5 of [LW 2016]) shows that one can choose such a complex embedding for which the modulus of the right hand side is small, so that we end up with an upper bound for the heights of u_1 and u_2.

Essentially, the three statements:
• finiteness of the set of solutions to Thue equations
• finiteness of the set of solutions of the unit equation
• non trivial refinement of Liouville's Theorem
are equivalent. An upper bound for the number of exceptional solutions for one of these statements implies such an upper bound for the two others; an effective result on one of them (upper bound for the exceptional solutions) yields an effective result on the two others. See [W 1986, LW 2011].

An effective result on the Thue equation is the following: let $F \in \mathbb{Z}[X,Y]$ be an irreducible binary form of degree ≥ 3; let $(x,y) \in \mathbb{Z}^2$ and let $m = F(x,y)$. Then

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

where κ is a positive effective absolute constant depending only on F; explicit formulae are available (see for instance [EG 2015]). At the early stages of Baker's method, such constants were huge; drastic improvements have been achieved; nowadays these estimates are good enough for solving explicitly Thue equations with coefficients which are not too large. Algorithms using this approach are implemented in computation packages.

3 Families of Thue equations

3.1 Historical survey

Given a family $F_t(X,Y)$, $t \in I$ of binary forms of degree ≥ 3, the first goal is to prove, under suitable assumptions, that for all $m > 0$ there are only finitely many $(t,x,y) \in I \times \mathbb{Z} \times \mathbb{Z}$ satisfying $F_t(x,y) = m$. Sometimes some subsets of (t,x,y), corresponding to "trivial solutions", are excluded. The second goal is to give an upper bound for the exceptional solutions.

A survey on these questions is [H 2004]. Further results can be found in [EG 2015]. See also [AMZ 2017] for another approach (the family $x^3 - (t^3-1)y^3 = 1$ is quoted).

3.2 Idea of the proof

Let $f \in \mathbb{Z}[T]$ be an irreducible polynomial of degree $d \geq 3$ and let

$$F(X,Y) = Y^d f(X/Y) \in \mathbb{Z}[X,Y].$$

Denote by α a root of f, by K the field $\mathbb{Q}(\alpha)$ and by υ a unit in K of infinite order. For $a \in \mathbb{Z}$ we denote by f_a the irreducible polynomial of $\alpha\upsilon^a$. We assume that f_a has

degree d. Let F_a be the binary form $Y^d f_a(X/Y)$, so that $f_0 = f$ and $F_0 = F$. Given $m \in \mathbb{Z}$, $m \neq 0$, we consider the set of triples (x,y,a) in $\mathbb{Z}^3$ such that

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

Let $\sigma_1, \ldots, \sigma_d$ the embeddings of K in $\mathbb{C}$. We define

$$\alpha_i = \sigma_i(\alpha), \quad \upsilon_i = \sigma_i(\upsilon) \qquad (i = 1, \ldots, d),$$

so that

$$f_a(T) = a_0 \prod_{i=1}^{d} (T - \alpha_i \upsilon_i^a),$$

$$F_a(X,Y) = Y^d f_a(X/Y) = a_0 \prod_{i=1}^{d} \big(X - \alpha_i \upsilon_i^a Y\big).$$

Let m be a nonzero integer and (x,y,a) be a solution of $F_a(x,y) = m$ with $\mathbb{Q}(\alpha\upsilon^a) = K$. For $i = 1, \ldots, d$, set $\beta_i = x - \alpha_i \upsilon_i^a y$. We have

$$a_0 \beta_1 \cdots \beta_d = m.$$

Eliminating x and y among three equations $\beta_i = x - \alpha_i \upsilon_i^a y$ for $i = i_1, i_2, i_3$ yields the unit equation

$$\beta_{i_1} \alpha_{i_2} \upsilon_{i_2}^a - \beta_{i_1} \alpha_{i_3} \upsilon_{i_3}^a + \beta_{i_2} \alpha_{i_3} \upsilon_{i_3}^a - \beta_{i_2} \alpha_{i_1} \upsilon_{i_1}^a + \beta_{i_3} \alpha_{i_1} \upsilon_{i_1}^a - \beta_{i_3} \alpha_{i_2} \upsilon_{i_2}^a = 0.$$

A first approach is to use Schmidt's Subspace Theorem and its consequence on the generalized S–unit equations: given a finite set of places S of a number field K and an integer n, the set of nondegenerate solutions $(u_1, \ldots, u_n)$ in S–units of the equation

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

is finite. *Nondegenerate* means that no nontrivial subsum of $u_1 + \cdots + u_n$ vanishes. A technical difficulty is that we need to deal with degenerate solutions. This approach yields strong general but ineffective results [LW 2012].

Another approach, which is effective, is to use Baker's method. This is efficient as soon as two of the six terms on the left hand side have a size which is much larger than the sum of all other four terms (besides, these two terms should not yield a zero subsum). So far, this has been achieved only in special cases [LW 2013b, LW 2013c, LW 2015a, LW 2015b, LW 2016, LW 2017].

3.3 Joint papers with Claude Levesque

We give here a summary of the results in a sequence of joint papers with C. Levesque, which was initiated during our visit to IMPA in Rio de Janeiro in 2010. The initial goal, which was to solve the family of equations obtained from Thomas equations (see [H 2004]) by including powers of units, has been achieved in [LW 2015b].

In [LW 2011], we work out equivalence statements between assertions dealing with several Diophantine questions: Thue–Mahler equations, S–unit equation, integral points on $\mathbb{P}^1(K)$ minus three points.

Our first results [BLW 2011,LW 2012,LW 2013a] were based on Schmidt's subspace Theorem and therefore were not effective - but they were very general. We obtained families of Thue–Mahler equations having only finitely many solutions and we gave upper bounds for the number of solutions; but we were not able to give upper bounds for the solutions themselves, hence we could not solve the equations.

Our first main new results were proved in [LW 2012]. Some consequences on Diophantine approximation were given in [LW 2013a].

Here is a special case of Corollary 3.6 of [LW 2012] which deals with Thue–Mahler equations.

Theorem 3 *Let K be a number field and Γ a finitely generated subgroup of $K^\times$. For $\gamma \in \Gamma$, denote by $f_\gamma \in \mathbb{Z}[X]$ the irreducible polynomial of γ and by $F_\gamma \in \mathbb{Z}[X,Y]$ its homogeneous version. Then the set of $\gamma \in \Gamma$ satisfying $[\mathbb{Q}(\gamma):\mathbb{Q}] \ge 3$ for which there exists $(x,y) \in \mathbb{Z}^2$ with $F_\gamma(x,y) \in \Gamma$ and $xy \ne 0$ is finite.*

Proof Since K has only finitely many subfields, it suffices to prove that the set of $\gamma \in \Gamma$ satisfying $\mathbb{Q}(\gamma) = K$ for which there exists $(x,y) \in \mathbb{Z}^2$ with $F_\gamma(x,y) \in \Gamma$ and $xy \ne 0$ is finite.

Assume $\gamma \in \Gamma$ satisfies $\mathbb{Q}(\gamma) = K$ and assume that there exists $(x,y) \in \mathbb{Z}^2$ with $F_\gamma(x,y) \in \Gamma$ and $xy \ne 0$. Let $\alpha \in K$ with $K = \mathbb{Q}(\alpha)$. Let S be a finite set of places of K such that $\alpha \in O_S^\times$ et $\Gamma \subset O_S^\times$. Corollary 3.6 of [LW 2012] with $t = 0$, $\varepsilon = \gamma/\alpha$ yields the result. □

By taking for Γ the group of units $\mathbb{Z}_K^\times$ in K, we deduce the following result:

Corollary 2 *Let K be a number field. The set of units $\varepsilon \in \mathbb{Z}_K^\times$ of degree ≥ 3 for which there exists $(x,y) \in \mathbb{Z}^2$ with $F_\varepsilon(x,y) = \pm 1$ and $xy \ne 0$ is finite.*

Another result from [LW 2012] is the following. *Let $S = \{p_1, \dots, p_s\}$ be a finite set of prime numbers, $f \in \mathbb{Z}[X]$ an irreducible polynomial of degree $d \ge 3$, α a root of f, K the number field $\mathbb{Q}(\alpha)$, $\sigma_1, \dots, \sigma_d$ the embeddings of K into $\mathbb{C}$. For each S–unit $\varepsilon \in O_S^\times$, define $F_\varepsilon(X,Y) \in \mathbb{Z}[X,Y]$ by*

$$F_\varepsilon(X,Y) = a_0\big(X - \sigma_1(\alpha\varepsilon)Y\big)\big(X - \sigma_2(\alpha\varepsilon)Y\big)\cdots\big(X - \sigma_d(\alpha\varepsilon)Y\big).$$

Let $m \in \mathbb{Z} \setminus \{0\}$. Then the set of $(x,y,\varepsilon,z_1,\dots,z_s)$ in $\mathbb{Z}^2 \times O_S^\times \times \mathbb{N}^s$ satisfying

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

with $xy \ne 0$, $\gcd(xy, p_1 \cdots p_s) = 1$ and $[\mathbb{Q}(\alpha\varepsilon):\mathbb{Q}] \ge 3$, is finite.

Theorem 3 implies finiteness results for families of Thue–Mahler equations. It is not effective: upper bounds for the number of solutions could be deduced, but not upper bounds for the heights of the solutions.

In [BLW 2011], which is a joint paper involving also Yann Bugeaud, we obtained an upper bound for the number of solutions of simultaneous Brahmagupta–Fermat–Pell–Mahler equations: given rational integers $a_1, b_1, c_1, a_2, b_2, c_2$ and prime numbers $p_1, \dots, p_s$, we considered the system of equations

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

where the unknowns $x, y, z, m_1, \dots, m_s, n_1, \dots, n_s$ take their values in the set of rational integers with $m_1, \dots, m_s, n_1, \dots, n_s$non negative.

Our more recent papers provide effective results for families of Thue equations by means of Baker's method. One main goal is to prove the following conjecture.

Conjecture 1 *Let α be an algebraic number of degree $d \geq 3$ over $\mathbb{Q}$. We denote by K the algebraic number field $\mathbb{Q}(\alpha)$, by $f \in \mathbb{Z}[X]$ the irreducible polynomial of α over $\mathbb{Z}$, by $\mathbb{Z}_K^\times$ the group of units of K and by r the rank of the abelian group $\mathbb{Z}_K^\times$. For any unit $\varepsilon \in \mathbb{Z}_K^\times$ such that the degree $\delta = [\mathbb{Q}(\alpha\varepsilon) : \mathbb{Q}]$ is ≥ 3, we denote by $f_\varepsilon(X) \in \mathbb{Z}[X]$ the irreducible polynomial of $\alpha\varepsilon$ over $\mathbb{Z}$ (uniquely defined upon requiring that the leading coefficient be > 0) and by F_ε the irreducible binary form defined by $F_\varepsilon(X,Y) = Y^\delta f_\varepsilon(X/Y) \in \mathbb{Z}[X,Y]$. Then there exists an effectively computable constant $\kappa > 0$, depending only upon α, such that, for any $m \geq 2$, each solution $(x, y, \varepsilon) \in \mathbb{Z}^2 \times \mathbb{Z}_K^\times$ of the inequation $|F_\varepsilon(x,y)| \leq m$ with $xy \neq 0$ and $[\mathbb{Q}(\alpha\varepsilon) : \mathbb{Q}] \geq 3$ satisfies*

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

In [LW 2013b], we prove conjecture 1 when the field K is a non totally real cubic field. In [LW 2016], we prove conjecture 1 in the more general case where the field K has at most one real embedding. In [LW 2013c], we prove conjecture 1 when one requests the unknown ε to belong to a subset of the group of units of K; we show that this subset contains a positive proportion of all units as soon as the degree of K is at least 4.

The papers [LW 2013b, LW 2015a, LW 2015b, LW 2017] deal with the special case where one restricts to a rank one subgroup of the group of units, namely when $\varepsilon = \upsilon^a$ with $a \in \mathbb{Z}$.

The main result of [LW 2013b], which deals only with non totally real cubic equations, is a special case of the main result of [LW 2017]; the "constants" in [LW 2013b] depend on α and υ, while in [LW 2017] they depend only on the degree d. The main result of [LW 2013c] deals with Thue equations twisted by a set of units which is not supposed to be a group of rank 1, but it involves an assumption (namely that at least two of the conjugates of υ have a modulus as large as a positive power of $\lceil\upsilon\rceil$) which we do not need in [LW 2017]. Our Theorem in [LW 2017] also improves the main result of [LW 2015a]: we remove the assumption that the unit is totally real (besides, the result of [LW 2015a] is not explicit in terms of the heights and regulator). We also notice that part (iii) of Theorem 1.1 of [LW 2015b] follows from our Theorem in [LW 2017]. The main result of [LW 2016] does not assume that the twists are done

by a group of units of rank 1, but it needs a strong assumption which does not occur in [LW 2017], namely that the field K has at most one real embedding.

A very recent joint work with E. Fouvry and C. Levesque, already quoted in §1.2, deals with the family of cyclotomic binary forms [FLW 2018]. One motivation came from the fact that in [LW 2017], we needed an assumption that some number was not a root of unity. It was a natural task to study the special case of roots of unity, which gives rise to the sequence of cyclotomic binary forms.

4 A guide to further references

One of the main references is the classical paper of C.L. Siegel in 1929, which has been recently translated into English. The reference [Z 2014] includes the English translation *On some applications of Diophantine approximations* by Clemens Fuchs, of the original text by C.L. Siegel in German *Über einige Anwendungen diophantischer Approximationen*, which is also reproduced in [Z 2014], together with comments by Clemens Fuchs and Umberto Zannier *Integral points on curves: Siegel's theorem after Siegel's proof*.

Another reference is [Z 2009] Chap. 2 (Thue's equations and rational approximations), where full proofs are given with lots of supplements.
There are many references on Diophantine geometry and Schmidt subspace Theorem, including the following ones:
• [L 1983], Chap. 7 (The Thue Siegel – Roth Theorem).
• [Se 1989], Chap. 7 (Siegel's method), Chap. 8 (Baker's method).
• [Sc 1991], Chap. III (The Thue equation); also Chap. V (Diophantine Equations in More Than Two Variables).
• [Z 2003], Chap. 1 (Diophantine Approximation and Diophantine Equations) §1.2 (From Thue to Roth); also Chap. II (Schmidt's Subspace Theorem and S–unit equations) and Chap. III (Integral points on curves and other varieties).
• [Bu 2004], Chap. 2 (Approximation to algebraic numbers), §2.1 (Rational approximation), §2.2 (Effective rational approximation).
• [HY 2008], Chap. 6 (Roth Theorem); also Chap. 7 (Subspace Theorem) and Chap. 8 (Vojta's conjectures)
• [C 2016], Chap. 3 (The theorems of Thue and Siegel); also includes results on Hilbert Irreducibility Theorem and integral points on surfaces.

References

AMZ 2017. F. AMOROSO, D. MASSER & U. ZANNIER, *Bounded height in pencils of finitely generated subgroups*, Duke Math. J., **166** (2017), pp. 2599–2642.
arXiv:1509.04963 [math.NT]

Ba 1975. A. BAKER, *Transcendental number theory*, Cambridge Mathematical Library, Cambridge University Press (1975); second ed., 1990.

BW 2007. A. BAKER & G. WÜSTHOLZ, *Logarithmic forms and Diophantine geometry*, vol. **9** of New Mathematical Monographs, Cambridge University Press (2007).

Be 1997a. M. A. BENNETT, *Effective measures of irrationality for certain algebraic numbers*, J. Austral. Math. Soc. Ser. A, 62 (1997), pp. 329–344.

Be 1997b. — , *Explicit lower bounds for rational approximation to algebraic numbers*, Proc. London Math. Soc. (3), 75 (1997), pp. 63–78.

Bu 2004. Y. BUGEAUD, *Approximation by algebraic numbers*, vol. **160** of Cambridge Tracts in Mathematics, Cambridge University Press (2004).

Bu 2018. — , *Linear Forms in Logarithms and Applications*, IRMA Lectures in Mathematics and Theoretical Physics Vol. **28**, European Mathematical Society (2018).
http://www.ems-ph.org/books/book.php?proj_nr=228

BLW 2011. Y. BUGEAUD, C. LEVESQUE & M. WALDSCHMIDT, *Équations de Fermat-Pell–Mahler simultanées*, Publicationes Mathematicae Debrecen, **79** 3-4 (2011), 357–366.

C 2016. P. CORVAJA, *Integral points on algebraic varieties*, vol. **3** of Institute of Mathematical Sciences Lecture Notes, Hindustan Book Agency, New Delhi, 2016.

EG 2015. J.-H. EVERTSE & K. GYŐRY, *Unit equations in Diophantine number theory*, vol. **146** of Cambridge Studies in Advanced Mathematics, Cambridge University Press (2015).

F 1991. A. FAISANT, *L'équation diophantienne du second degré*, vol. 1430 of Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics], Hermann, Paris, 1991. Collection Formation des Enseignants et Formation Continue. [Collection on Teacher Education and Continuing Education].

FLW 2018. E. FOUVRY, C. LEVESQUE & M. WALDSCHMIDT, *Representation of integers by cyclotomic binary forms*, Acta Arithmetica (2018).
arXiv:1712.09019 [math.NT]

G 1977. K. GYŐRY, *Représentation des nombres entiers par des formes binaires*, Publ. Math. Debrecen **24 (3–4)**, 363–375, (1977).

G 2002. — , *Solving Diophantine equations by Baker's theory*, in A panorama of number theory or the view from Baker's garden (Zürich, 1999), Cambridge Univ. Press (2002), pp. 38–72.

H 2004. C. HEUBERGER, *Parametrized Thue equations – A survey*, In: Proceedings of the RIMS symposium "Analytic Number Theory and Surrounding Areas", Kyoto, Oct. 18–22, 2004, RIMS Kôkyûroku, vol. **1511**, 2006, pp. 82–91.

HY 2008. P.-C. HU & C.-C. YANG, *Distribution theory of algebraic numbers*, vol. **45** of De Gruyter Expositions in Mathematics (2008).

L 1983. S. LANG, *Fundamentals of Diophantine geometry*, Springer-Verlag, New York, 1983.

LW 2011. C. LEVESQUE & M. WALDSCHMIDT, *Some remarks on diophantine equations and diophantine approximation*, Vietnam Journal of Mathematics **39** 3 (2011) 343–368.
arXiv:1312.7200 [math.NT]

LW 2012. — , *Familles d'équations de Thue–Mahler n'ayant que des solutions triviales*, Acta Arith., **155** (2012), 117–138.
arXiv:1312.7202 [math.NT]

LW 2013a. — , *Approximation of an algebraic number by products of rational numbers and units*, Journal of the Australian Mathematical Society, **93** (2013) 1-2, pp. 121–131.
arXiv:1312.7203 [math.NT]

LW 2013b. — , *Families of cubic Thue equations with effective bounds for the solutions*, J.M. Borwein et al. (eds.), Number Theory and Related Fields: In Memory of Alf van der Poorten, Springer Proceedings in Mathematics & Statistics **43** (2013), 229–243.
arXiv:1312.7204 [math.NT]

LW 2013c. — , *Solving effectively some families of Thue Diophantine equations*, Moscow J. of Combinatorics and Number Theory **3**, 3–4 (2013), 118–144.
arXiv:1312.7205 [math.NT]

LW 2015a. — , *Familles d'équations de Thue associées à un sous-groupe de rang* 1 *d'unités totalement réelles d'un corps de nombres*, in SCHOLAR – a Scientific Celebration Highlighting Open Lines of Arithmetic Research, 2013 (volume dedicated to Ram Murty), CRM collection Contemporary Mathematics", AMS, **655** (2015), 117–134.
http://www.ams.org/books/conm/655/
arXiv: 1505.06656 [math.NT]

LW 2015b. — , *A family of Thue equations involving powers of units of the simplest cubic fields*, J. Théor. Nombres Bordx. **27**, No. 2 (2015), 537–563.
arXiv:1505.06708 [math.NT]

LW 2016. — , *Solving simultaneously Thue Diophantine equations: almost totally imaginary case*, Ramanujan Mathematical Society, Lecture Notes Series **23** (2016), 137–156.
arXiv: 1505.06653 [math.NT]

LW 2017. — , *Families of Thue equations associated with a rank one subgroup of the unit group of a number field*, Mathematika, **63** 3 (2017) 1060-1080.
arXiv: 1701.01230 [math.NT].

M 2016. D. MASSER, *Auxiliary polynomials in number theory*, vol. **207** of Cambridge Tracts in Mathematics, Cambridge University Press (2016).

Mo 1969. L. J. MORDELL, *Diophantine equations*, Pure and Applied Mathematics, Vol. 30, Academic Press, London-New York, 1969.

OEIS. N.J. SLOANE, *The On–line Encyclopedia of Integer Sequences*.
https://oeis.org/

Sc 1991. W. M. SCHMIDT, *Diophantine approximations and Diophantine equations*, vol. **1467** of Lecture Notes in Mathematics, Springer-Verlag, Berlin, 1991.

Se 1989. J.-P. SERRE, *Lectures on the Mordell-Weil theorem*, Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, (1989); third ed., 1997.

ST 1986. T. N. SHOREY & R. TIJDEMAN, *Exponential Diophantine equations*, vol. **87** of Cambridge Tracts in Mathematics, Cambridge University Press (1986).

SVTS 1977. T. N. SHOREY, A. J. VAN DER POORTEN, R. TIJDEMAN & A. SCHINZEL, *Applications of the Gel'fond-Baker method to Diophantine equations*, in Transcendence theory: advances and applications, Cambridge (1977), pp. 59–77.

Sp 1982. V. G. SPRINDŽUK, *Classical Diophantine equations*, vol. **1559** of Lecture Notes in Mathematics, Springer-Verlag, Berlin, 1993. Translated from the 1982 Russian original.

W 1986. M. WALDSCHMIDT, *Diophantine equations and transcendental methods* (written by Noriko Hirata). In Transcendental numbers and related topics, RIMS Kôkyûroku, Kyoto, **599** (1986), n°8, 82-94.
http://www.kurims.kyoto-u.ac.jp/∼kyodo/kokyuroku/contents/599.html

Z 2003. U. ZANNIER, *Some applications of Diophantine approximation to Diophantine equations with special emphasis on the Schmidt subspace Theorem*, Forum Editrice Universitaria Udine srl, Udine 2003.

Z 2009. — , *Lecture notes on Diophantine analysis*, vol. **8** of Appunti. Scuola Normale Superiore di Pisa (Nuova Serie), Edizioni della Normale, Pisa, 2009.

Z 2014. — , (Ed.), *On some applications of Diophantine approximations*, vol. **2** of Quaderni/Monographs, Edizioni della Normale, Pisa, 2014. A translation of Carl Ludwig Siegel's "Über einige Anwendungen diophantischer Approximationen" by Clemens Fuchs, With a commentary and the article "Integral points on curves: Siegel's theorem after Siegel's proof" by Fuchs and Umberto Zannier.