Thue equations with composite fields

by
Yuri Bilu* (Zürich)
and
Guillaume Hanrot† (Talence)

April 16, 1997

Abstract

We consider the Thue equation $F(x, y) = a$, where F is an irreducible form of degree $n \geq 3$. We describe a method of resolution which takes advantage of the fact that the number field generated by a root of $F(1, y)$ has small subfields. We illustrate this method by solving several real cyclotomic equations of degrees as large as 2505.

Résumé

Considérons l'équation de Thue $F(x, y) = a$, avec F une forme irréductible homogène de degré $n \geq 3$. Nous décrivons une méthode de résolution permettant de tirer profit de l'existence de petits sous-corps du corps de nombres engendré par une racine de $F(1, y)$. À titre d'illustration, nous résolvons l'équation cyclotomique réels en des degrés allant jusqu'à 2505.

1 Introduction

The history of numerical solution of Diophantine equations begun in 1969, when Baker and Davenport [1] solved completely a system of two Pell equations. They used the well-known fact that every "large" solution gives rise to a "very small" value of a linear form $\Lambda(b_1, b_2) = \log \alpha_0 + b_1 \log \alpha_1 + b_2 \log \alpha_2$ (where α_0, α_1 and α_2 are explicitly given algebraic numbers) at an integral point (b_1, b_2). Using Baker's theory of logarithmic forms, they obtained a huge (around 10^{400}) upper bound for $\max(|b_1|, |b_2|)$. After this, expanding $\log \alpha_2 / \log \alpha_1$ into continued fraction, they showed that $|\Lambda(b_1, b_2)|$ cannot be too small when b_1 and b_2 run the integers below the huge bound. Therefore the system cannot have "large" solutions, while "small" solutions can be easily enumerated.

This idea was developed in various directions by Pethö, Tzanakis, de Weger, and many other authors. The subject became especially popular when Lenstra, Lenstra and

*Partially supported by SFB 343 "Diskrete Strukturen in der Mathematik", Bielefeld
†Partially supported by CNRS GDR AMI
1991 *Mathematics Subject Classification* Primary: 11Y50, Secondary: 11B37.

Lovasz [9] suggested a polynomially quick algorithm for finding an almost shortest vector in a lattice (referred to as LLL-algorithm in the sequel). The LLL-algorithm made it possible to extend the idea of Baker and Davenport to logarithmic forms in three or more variables, when continued fractions are not efficient anymore. See [16, 10] for a detailed description of the methods, history of the subject and extensive bibliography up to 1989.

In [4] we showed that one can solve Diophantine equations of Thue using only continued fractions (as Baker and Davenport did), and without involving the LLL-algorithm. This allowed us to solve completely Thue equations of rather high degree. In [5] we extended our method to superelliptic Diophantine equations (see also [3]).

In this paper we show that the method of [4] becomes especially efficient if the number field related to the Thue equation contains a small subfield of degree at least 3 over $\mathbb{Q}$. We shall see that in this case one has to deal mainly with the subfield rather than with the whole field. We were motivated by the fact that such equations often occur in practice, for instance in the classical problem of primitive divisors [15, 18].

Using our method we managed to solve many totally real Thue equations of extremely high degree (up to 2505). See Section 7 for the details.

Acknowledgments. We would like to thank Benne de Weger for useful discussions and suggestions.

2 Notations

We consider the Thue equation

$$F(x,y) = \mathcal{N}_{\mathbb{L}/\mathbb{Q}}(y - \alpha x) = a, \tag{1}$$

where $a = a_1/a_2$ is a rational number, α an algebraic number of degree $n \geq 3$, and $\mathbb{L} = \mathbb{Q}(\alpha)$. We put

$$f(y) = F(1,y) = \mathcal{N}_{\mathbb{L}/\mathbb{Q}}(y - \alpha).$$

We shall assume that the field $\mathbb{L}$ has a "small" subfield $\mathbb{K}$, of degree $m \geq 3$.

Let $\mathbb{K}$ have s real and $2t$ complex conjugate embeddings, where $s + 2t = m$. We number the embeddings $\sigma_1, \ldots, \sigma_m$ so that $\sigma_1, \ldots, \sigma_s$ are the real embeddings, and

$$\sigma_{s+i} = (\text{complex conjugation}) \circ \sigma_{s+i+t} \quad (1 \leq i \leq t). \tag{2}$$

We write $\mathbb{K}_i = \sigma_i(\mathbb{K})$. We shall assume that $s \geq 1$; in particular, $\mathbb{K}$ has no roots of unity distinct from ± 1 (in the case $s = 0$ the equation is trivial; see [4, Section 2], for instance).

Put $l = n/m$ and fix an ordering $\alpha_{11} = \alpha, \alpha_{12}, \alpha_{13}, \ldots, \alpha_{ml}$ of the conjugates of α over $\mathbb{Q}$ so that for a fixed i the numbers $\alpha_{i1}, \ldots, \alpha_{il}$ are conjugate over $\mathbb{K}_i$.

We use $O_1(\ldots)$ as a quantitative version of the usual $O(\ldots)$:

$$A = O_1(B)$$

means $|A| \leq B$.

For practical implementation of the method, one should be able to perform the following operations in the number field $\mathbb{K}$: