COLLOQUIA MATHEMATICA SOCIETATIS JÁNOS BOLYAI
51. NUMBER THEORY, BUDAPEST (HUNGARY), 1987

ON THE PRACTICAL SOLUTION OF THUE-MAHLER EQUATIONS, AN OUTLINE

B.M.M. de WEGER

This paper was presented at the Colloquium on Number Theory, July 20-25, 1987, in Budapest. It reports on work that was done in close cooperation with N. Tzanakis. The author was supported by the Netherlands Foundations for Mathematics (SMC) with financial aid from the Netherlands Organization for the Advancement of Pure Research (ZWO). He also thanks Shell Nederland B.V. for financial support.

Dedicated to Alda, with love.

1. INTRODUCTION

Let $F(X,Y)$ be a binary form with at least three distinct linear factors over $\mathbb{C}$. Let $p_1, \ldots, p_s$ be fixed distinct prime numbers. The diophantine equation

$$F(X,Y) = \pm \prod_{i=1}^{s} p_i^{n_i}$$

in the variables $X, Y \in \mathbb{Z}$, $n_1, \ldots, n_s \in \mathbb{N}_0$, with $(X,Y) = 1$, is known as a Thue-Mahler equation. It was proved by Mahler [1933] that this equation has only finitely many solutions, and by Sprindžuk and Vinogradov [1968] and Coates [1969], [1970] that all the solution can, at least in principle, be determined effectively, since an effectively computable upper bound for the variables can be derived from the p-adic theory of linear forms in logarithms. For the history of this equation we refer to Shorey and Tijdeman [1986], Chapter 7.

It is the purpose of this paper to show that it is possible to solve Thue-Mahler equations, not only in principle, but in practice, by reducing the above mentioned upper bounds considerably. This is done by a combination of real and p-adic computational diophantine approximation techniques, based on the L^3-algorithm for reducing bases of lattices (cf. Lenstra, Lenstra and

Lovász [1982], and for an integral version de Weger [1987[a]]). The method can be considered as a p-adic analogue of the method for solving Thue equations, on which Tzanakis [1987] reports. For a more general treatment of the application of the L^3-algorithm to solving diophantine equations, see de Weger [1987[b]], especially Chapter 3.

A similar idea, but without using the L^3-algorithm, was used by Agrawal, Coates, Hunt and van der Poorten [1980], who determined all solutions of the equation

$$X^3 - X^2 \cdot Y + X \cdot Y^2 + Y^3 = \pm 11^n \ .$$

This is, to the author's knowledge, one of the only two examples in the literature where a Thue-Mahler equation has been solved completely, the other one being

$$X^3 + 3 \cdot Y^3 = 2^n \ ,$$

which was solved by Tzanakis [1984] by a different method. It is an example of the simplest kind, in view of the fact that the cubic field $Q(\theta)$, where θ is a root of $F(x,1) = 0$, has only one fundamental unit, and there occurs only one prime. Therefore it was sufficient to use two-dimensional real continued fractions and one-dimensional p-adic continued fractions, in stead of the

more complicated L^3-algorithm (which was not yet available at the time). We now extend the method to the situation where there are more than one fundamental units, and more than one primes, thus to the general situation. Then the L^3-algorithm becomes very useful. (However, a more or less technical problem will show up for forms of large degree, that has not yet been solved). In this paper we only give an outline of the method. In a paper to be published. Tzanakis and the present author have used the method of this paper to solve the Thue-Mahler equation

$$X^3 - 3 \cdot X \cdot Y^2 - Y^3 = \pm 3^{n_1} \cdot 17^{n_2} \cdot 19^{n_3}.$$

Here, two fundamental units and three primes are involved. Note that if (X_0, Y_0) is a solution, then so is $(-Y_0, X_0+Y_0)$. Thus solutions come in six-tuples, of which exactly one satisfies $X > 0$ and $Y \geq 0$. It turns out that there are 26 such solutions, all satisfying $X \leq 896$, $Y \leq 379$, $n_1 \leq 1$, $n_2 \leq 3$, $n_3 \leq 5$.

2. UPPER BOUNDS

In this section we give a short account of the classical arguments for deriving upper bounds for the solutions of a Thue-Mahler equation. Any Thue-Mahler

equation reduces in a routine manner to a finite number of equations of the type

$$(1) \qquad \delta_1 \cdot \beta_1 - 1 = \delta_2 \cdot \beta_2 ,$$

where δ_1, δ_2 are algebraic constants, and β_1, β_2 are of the form

$$\frac{X - Y \cdot \theta'}{X - Y \cdot \theta''} ,$$

where θ', θ'' are conjugates of the root θ of $F(x,1) = 0$. From the Thue-Mahler equation it follows that there exist algebraic units $\varepsilon_1, \ldots, \varepsilon_r$ and algebraic constants $\alpha, \pi_1, \ldots, \pi_t$, and rational integers $\nu_1, \ldots, \nu_t$ closely related to $n_1, \ldots, n_s$, such that β_1, β_2 are of the type

$$\alpha' \cdot \prod_{i=1}^{r} \varepsilon_i'^{a_i} \cdot \prod_{j=1}^{t} \pi_j'^{\nu_j} ,$$

the prime sign indicating a proper conjugate, and the a_i being rational integers. For a given solution $(X,Y,n_1,\ldots,\ldots,n_s)$ of the Thue-Mahler equation and for a given index $i \in \{1,\ldots,s\}$ these conjugates can be taken in such a way that (supposing that n_i is large enough)

$$\operatorname{ord}_{p_i}(\beta_1) = c_1, \ \operatorname{ord}_{p_i}(\beta_2) = c_2 + c_3 \cdot n_i ,$$

where c_1, c_2, c_3 are small constants. Put

$$A = \max|a_i|, \ N = \max(n_i), \ H = \max(A, N).$$

The theory of p-adic linear forms in logarithms (see e.g. Yu [1987]) provides an explicit constant C_1 such that

$$\operatorname{ord}_{p_i}(\delta_1 \cdot \beta_1 - 1) < C_1 \cdot \log H .$$

It follows that a constant C_2 such that

$$N < C_2 \cdot \log H$$

can be computed explicitly. It will be very large in practice (even for a Thue-Mahler equation of low degree it may be as large as 10^{50}). Put

$$\mu = \prod_{j=1}^{t} \pi_j^{\nu_j} .$$

Then $|\log|\mu|| < c_4 \cdot N < C_3 \cdot \log H$. Suppose that A is large enough. Then, since β_1, β_2 have the form

$$\alpha' \cdot \mu' \cdot \prod_{i=1}^{r} \varepsilon_i'^{a_i} ,$$

the conjugates can be taken such that β_2 is close to 0, namely

$$|\beta_2| < c_5 \cdot |\mu'| \cdot \exp(-c_6 \cdot A)$$

for small constants c_5, c_6. The theory of real linear forms in logarithms (see e.g. Waldschmidt [1980]) provides an explicit (large) constant C_4 such that

$$|\delta_1 \cdot \beta_1 - 1| > \exp(-C_4 \cdot \log A).$$

Combining all the estimates it follows that H is bounded by an explicit constant C_0.

3. REDUCING UPPER BOUNDS

Above we derived an upper bound C_0 for H, using an interplay between p-adic and real arguments. We now show, again combining p-adic and real arguments, and using a computer, how this upper bound C_0 can be reduced to an upper bound for H of the size of log C_0. See also de Weger [1987^b], Chapter 3.

Our computational tool is the L^3-algorithm, that is capable of finding good lower bounds for the length of the shortest nonzero vector in a given lattice Γ, and for the distance of a given point to the nearest lattice point. These lower bounds are expected to be of the size

$$\det(\Gamma)^{1/\dim(\Gamma)} .$$

Write

$$\beta_1 = \delta \cdot \prod_{i=1}^{r} \varepsilon_i^{a_i} \cdot \prod_{j=1}^{t} \pi_j^{\nu_j} .$$

We assume that we know the numbers δ, ε_i, π_j explicitly, and that we can compute their complex and p-adic values

to arbitrary (but finite) precision.

First we make a p-adic step. Put for a fixed prime $p \in \{p_1,\ldots,p_s\}$

$$\eta_i = -\log_p(\varepsilon_i)/\log_p(\pi_t) \text{ for } i = 1,\ldots,r,$$

$$\tau_j = -\log_p(\pi_j)/\log_p(\pi_t) \text{ for } j = 1,\ldots,t-1,$$

$$\varphi = \log_p(\delta)/\log_p(\pi_t) .$$

We assume that these numbers η_i, τ_j, φ are in $\mathbb{Q}_p$, and not in some algebraic extension. This is in general not obvious, but it can be proved in the cases where the degree of the binary form $F(X,Y)$ is not larger than 4. (This is the unsolved problem announced in the introduction)*). Further, we may assume without further loss of generality that they are even in $\mathbb{Z}_p$. For any p-adic integer γ and for any $m \in \mathbb{N}_0$ we denote by $\gamma^{(m)}$ the unique rational integer such that

$$\gamma \equiv \gamma^{(m)} \pmod{p^m},\ 0 \le \gamma^{(m)} \le p^m - 1.$$

We now define the lattice Γ_m by the matrix

*) Note added in proof: This problem is solved now, due to J.-H. Evertse.

$$\begin{bmatrix} 1 & & & & & & \\ & \ddots & & 0 & & & \\ & & 1 & & & & \\ & 0 & & 1 & & & \\ & & & & \ddots & & \\ & & & & & 1 & \\ \eta_1^{(m)} & \cdots & \eta_r^{(m)} & \tau_1^{(m)} & \cdots & \tau_{t-1}^{(m)} & p^m \end{bmatrix},$$

where the column vectors of the matrix are the basis vectors of Γ_m. Here we take m large enough, such that p^m is of the size C_o^{r+t}. Then the distance of the point

$$\underline{x} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \varphi^{(m)} \end{bmatrix}$$

to the nearest lattice point can be bounded from below, from the result of the L^3-algorithm (cf. de Weger [1987^b], Section 3.4). It will, in a typical situation, be at least $c_7 \cdot C_o$ for a suitable constant c_7 (small compared to C_o). If c_7 is not large enough, one should try with a larger value of m. For a solution $a_1, \ldots, a_r, \nu_1, \ldots, \nu_t$ of (1) it follows easily that if $\mathrm{ord}_p(\delta_1 \cdot \beta_1 - 1) \geq \geq m + \mathrm{ord}_p(\log_p(\pi_t))$ then

$$\underline{x} + \begin{bmatrix} a_1 \\ \vdots \\ a_r \\ \nu_1 \\ \vdots \\ \nu_t \end{bmatrix} \in \Gamma_m \quad .$$

Now $\mathrm{ord}_p(\delta_1 \cdot \beta_1 - 1) = c_2 + c_3 \cdot n_i$, where i is the index such that $p = p_i$. This contradicts the upper bound C_o. Hence

$$n_i < m/c_3 + (\mathrm{ord}_p(\log_p(\pi_t)) - c_2)/c_3 \ ,$$

which is only of size log C_o. We repeat this procedure for all $p = p_1, \ldots, p_s$, and find a reduced upper bound N_o for N, of size log C_o.

Next we make a real step. Choose a constant C of size $C_o^r \cdot N_o^t$, large enough. Put

$$\eta_i = [C \cdot \log|\varepsilon_i|] \quad \text{for } i = 1, \ldots, r \ ,$$

$$\tau_j = [C \cdot \log|\pi_j|] \quad \text{for } j = 1, \ldots, t \ ,$$

$$\varphi = - [C \cdot \log|\delta|] \ .$$

Define the lattice Γ by the matrix

$$\begin{bmatrix} C_0/N_0 & & & & & \\ & \ddots & & 0 & & \\ & & \ddots & & & \\ 0 & & C_0/N_0 & & & \\ & & & 1 & \ddots & \\ & & & & \ddots & 1 \\ \tau_1 & \cdots & \tau_t & \eta_1 & \cdots & \eta_{r-1} & \eta_r \end{bmatrix},$$

and suppose that C is so large that the distance from the fixed point

$$\underline{x} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \varphi \end{bmatrix}$$

to the nearest lattice point is at least $c_8 \cdot C_0$ for a small constant c_8, following from the L^3-algorithm. It follows that $|\delta_1 \cdot \beta_1 - 1| > c_9 \cdot C_0/C$ for a small constant c_9. By the upper bounds for $|\beta_2|$ and $|\log|\mu||$ a reduced bound for A follows, which is of size $\log C_0$.

We now may repeat the whole procedure, with the bound C_0 replaced by the new, reduced upper bound for H, that is of size C_0, until no further improvement is reached. Then we can check all remaining possibilities, for example by

using the fact that for a solution of the Thue-Mahler equation, the quotient X/Y must be near to one of the conjugates of the root θ (in the p-adic sense). We also may use some more subtle techniques using approximation lattices, such as the Fincke and Pohst algorithm (cf. de Weger [1987^a], [1987^b]).

We expect that it is possible in this way to solve completely any Thue-Mahler equation of small degree within a few minutes of computer rime.

REFERENCES

AGRAWAL, M.K., COATES, J.H., HUNT, D.C. and van der POORTEN, A.J. [1980], Elliptic curves of conductor 11, *Math. Comp.* 35, 991-1002.

COATES, J. [1969], An effective p-adic analogue of a theorem of Thue, *Acta Arith.* 15, 279-305.

COATES, J. [1970], An effective p-adic analogue of a theorem of Thue II: The greatest prime factor of a binary form, *Acta Arith.* 16, 399-412.

LENSTRA, A.K., LENSTRA jr., H.W. and LOVÁSZ, L. [1982], Factoring polynomials with rational coefficients, *Math. Ann.* 261, 515-534.

SHOREY, T.N. and TIJDEMAN, R. [1986], *Exponential diophantine equations*, Cambridge University Press.

SPRINDŽUK, V.G. and VINOGRADOV, A.I. [1968], The representation of numbers by binary forms (Russian), *Mat. Zametki 3*, 369-376.

TZANAKIS, N. [1984], The complete solution in integers of $x^3 + 3 \cdot y^3 = 2^n$, *J. Number Th.* 19, 203-208.

TZANAKIS, N. [1987], On the practical solution of the Thue equations; an outline, these Proceedings.

TZANAKIS, N. and de WEGER, B.M.M. [1987], On the practical solution of the Thue equation, *Memorandum* 668, Faculty of Applied Mathematics, University of Twente, to appear in *J. Number Th.*

WALDSCHMIDT, M. [1980], A lower bound for linear forms in logarithms, *Acta Arith.* 37, 257-283.

de WEGER, B.M.M. [1987^a], Solving exponential diophantine equations using lattice basis reduction algorithms, *J. Number Th.* 26, 325-367.

de WEGER, B.M.M. [1987^b], *Algorithms for diophantine equations*, PhD Thesis, University of Leiden, to appear as *CWI-Tract*.

YU, K.R. [1987], Linear forms in the p-adic logarithms,
Report MPI/87-20, Max Planck Institut für
Mathematik, Bonn, to appear in *Acta Arith.*

de WEGER, B.M.M.
Faculty of Applied Mathematics,
University of Twente,
P.O. Box 217,
7500 AE ENSCHEDE,
The Netherlands