On the practical solution of the Thue-Mahler equation *

N. Tzanakis and B.M.M. de Weger

1 Introduction

We are interested in the following problem: Given any Thue-Mahler equation, to find *explicitly* all its solutions. Although there is an effective way to solve any Thue-Mahler equation (see, for example, Chapter 7 of [5]), in practice one faces a variety of computational problems. To the best of our knowledge, only one or two Thue-Mahler equations have been solved so far (see [1] and [7]) and in these, only one prime power and one fundamental unit (thus, two unknown exponents) are involved.

We have developed a general method, which we now want to illustrate by solving a specific equation. In this example four unknown exponents are involved.

A famous Thue equation is Ljunggren's $x^3 - 3xy^2 - y^3 = 1$ (see [2]; Chapter 23 of Mordell's book [4] and [6]). We decided to solve

$$x^3 - 3xy^2 - y^3 = \pm 3^{n_0} 17^{n_1} 19^{n_2}, \tag{1}$$

which "includes" Ljunggren's equation. The primes 3, 17, 19 have not been arbitrarily chosen; in fact, these are the only primes $p < 20$ for which $x^3 - 3xy^2 - y^3 \equiv 0 \pmod{p}$ is solvable.

2 Solution of (1)

We worked in $\mathbb{Q}(\theta)$, where $\theta^3 - 3\theta - 1 = 0$. This is a Galois field. This fact is not essential in our method, but surely simplified our computations and clarified our exposition.

To every solution (x, y), a class of six solutions is associated:

$$\{\pm(x, y), \pm(y, -x - y), \pm(-x - y, x)\}.$$

*Lecture given by N.Tzanakis

Computational Number Theory

Using this observation, it was easy to show that, in order to solve (1), it suffices to solve

$$\beta := x - y\theta = \pm\psi^{n_0}\pi^{n_1}\rho^{n_2}\theta^{a_1}\eta^{a_2}. \tag{2}$$

Here

$$\psi = -1 + \theta \text{ is the prime divisor of } 3,$$

$$\pi = 3 - \theta \text{ is a prime divisor of } 17,$$

$$\rho \in \{3 + \theta, 5 - \theta^2, 1 - \theta + \theta^2\}, \text{ the set of prime divisors of } 19,$$

$$\theta, \eta = 1 + \theta \text{ is a pair of fundamental units},$$

$$n_0 \in \{0, 1\} \text{ (an obvious fact)},$$

$$n_1, n_2 \text{ are unknown nonnegative integers},$$

$$a_1, a_2 \text{ are unknown integers}.$$

Of course, solving (2) means to find all $(n_0, n_1, n_2, a_1, a_2)$ for which the coefficient of θ^2 is zero when the right-hand side of (2) is expressed in terms of the basis $1, \theta, \theta^2$.

Using (2) and its other two conjugate relations we eliminated x, y and got the relation

$$(-1)^{a_2}\xi^{n_1}\chi^{n_2}\theta^{a_1'}\eta^{a_2'} - 1 = (-1)^{a_1+a_2+n_0}\xi^{*n_1}\chi^{*n_2}\theta^{2a_1+a_2-1}\eta^{-a_1+a_2-n_0}, \tag{3}$$

where ξ, χ, ξ^*, χ^* are explicitly known elements of $\mathbb{Q}(\theta)$ and $a_1' = a_1 + 2a_2 - n_0 - 1$, $a_2' = -2a_1 - a_2 + 1$.

In the right-hand side of (3) all elements apart from ξ^* have π-adic order zero, while $\mathrm{ord}_\pi(\xi^*) = 1$. Then (3) implies that

$$\mathrm{ord}_\pi\left((-1)^{a_2}\xi^{n_1}\chi^{n_2}\theta^{a_1'}\eta^{a_2'} - 1\right) = n_1. \tag{4}$$

Put $N = \max\{n_1, n_2\}$, $A = \max\{|a_1'|, |a_2'|\}$, $H = \max\{N, A\}$. Since ξ, χ, θ, η are explicitly known, we could apply the p-adic theory of linear forms in logarithms of algebraic numbers to the left-hand side of (4), in order to find an upper bound of n_1 in terms of H. This was accomplished thanks to a recent theorem of Kunrui Yu ([12]). Analogously, working ρ-adically, we found an upper bound of n_2. Thus we have an upper bound of N, which, by Yu's theorem, is of the form

$$N \le C_{13}(\log H + C_{14}). \tag{5}$$

In our case we computed $C_{13} = 6.190047 \cdot 10^{24}$ and $C_{14} = 4.28$.

Our next task was to find an upper bound of A similar to that of N. Using elementary arguments we did so, under the assumption that

$$\min_{1 \le i \le 3} |\beta^{(i)}| > e^{-C_{16}A}, \tag{6}$$

for a suitable C_{16}. Then A is at most const. + const. $\log H$, which in combination with (5) gives

$$H < C_{19} + C_{20} \log H.$$

In our case we derived in this way

$$H < 4.38 \cdot 10^{27}, \tag{7}$$

under the restriction (6), where $C_{16} = 0.085$.

The case opposite to (6) remained. Here the philosophy is to work as in the case of a Thue equation, where also one of the conjugates of $\beta = x - y\theta$ is necessarily "very small" (see e.g. [8]). We proved by elementary arguments

$$0 < |\Lambda_0| < \text{const.} e^{-C_{16}H}, \tag{8}$$

where

$$\Lambda_0 = n_1 \log |\xi^{(i_0)}| + n_2 \log |\chi^{(i_0)}| + a_1' \log |\theta^{(i_0)}| + a_2' \log |\eta^{(i_0)}|$$

($i_0 \in \{1, 2, 3\}$, so we had to consider three cases), and the constant in (8) is explicitly calculable. On the other hand, we applied the (real-complex) theory of linear forms in logarithms of algebraic numbers (in our case we applied Waldschmidt's theorem [10]) to conclude that

$$|\Lambda_0| > e^{-C_7(\log H + C_8)},$$

where $C_7 = 2.6467 \cdot 10^{29}$ and $C_8 = 2.442325$. This relation, combined with (8), leads to a relation of the form

$$H < \text{const.} + \text{const.} \log H,$$

from which we have found

$$H < K_0 := 5.76 \cdot 10^{32}. \tag{9}$$

Compare this with (7) to see that in all cases (9) is true. In view of (9), the solution of (2) and, hence, of (1), is effective (by enumeration), but clearly such a task is thoroughly unrealistic.

3 Reduction of H

We found a reduced upper bound of n_1 as follows: By some elementary arguments (4) can be written as

$$n_1 = \text{ord}_{17}(\Lambda_1),$$

where Λ_1 is a linear form in 17-adic logarithms:

$$\Lambda_1 = n_1\lambda_1 + n_2\lambda_2 + a_1'\mu_1 + a_2'\mu_2.$$

Here, $\lambda_1, \lambda_2, \mu_1, \mu_2$ are explicitly known 17-adic logarithms of algebraic numbers. Next, put

$$\beta_1 = -\frac{\lambda_1}{\lambda_2}, \quad \alpha_1 = -\frac{\mu_1}{\lambda_2}, \quad \alpha_2 = -\frac{\mu_2}{\lambda_2} \quad \text{(17-adic integers)}.$$

For a positive integer m, to be specified later, we computed rational approximations $\beta_1^{(m)}$, $\alpha_1^{(m)}$, $\alpha_2^{(m)}$ of β_1, α_1, α_2 respectively, and considered the lattice Γ_m with basis vectors the columns of the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \alpha_1^{(m)} & \alpha_2^{(m)} & \beta_1^{(m)} & 17^m \end{pmatrix}.$$

This lattice is just the set of vectors $(n_1, n_2, a_1', a_2')^t \in \mathbb{Z}^4$ for which $\mathrm{ord}_{17}(\Lambda_1) \geq 17^{m-1}$ (this shows the meaning of m).

By the L^3-algorithm ([3], see also [11] for various applications of this algorithm to diophantine problems) we computed a reduced basis $\mathbf{b}_1, \ldots, \mathbf{b}_4$ of Γ_m. We proved that

$$\text{if} \quad |\mathbf{b}_1| > 2^{5/2} K_0 \quad \text{then} \quad n_1 \leq m.$$

In practice, the condition $|\mathbf{b}_1| > 2^{5/2} K_0$ was satisfied, when we took m "somewhat larger" than $4 \log K_0 / \log 17$. To give an idea, in our example $4 \log K_0 / \log 17 \simeq 106.5$ and it turned out that $m = 110$ was sufficient; hence $n_1 \leq 110$. Working analogously with n_2 we came to the conclusion that $n_2 \leq 111$. This completes the *p-adic reduction step.*

Then we proceeded with the *real reduction step*: From (9) we have $A < K_0$, while from the p-adic reduction step we know that $N \leq 111$. We chose an integer C of the size of $K_0^2 \cdot 111^2$ (in our case $C = 10^{75}$ was good) and we put

$$\beta_1 = [C \log |\xi^{(i_0)}|], \quad \beta_2 = [C \log |\chi^{(i_0)}|],$$
$$\alpha_1 = [C \log |\theta^{(i_0)}|], \quad \alpha_2 = [C \log |\eta^{(i_0)}|].$$

Then we considered the lattice Γ with basis vectors the columns of the matrix

$$\begin{pmatrix} [K_0/111] & 0 & 0 & 0 \\ 0 & [K_0/111] & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \beta_1 & \beta_2 & \alpha_1 & \alpha_2 \end{pmatrix},$$

and we calculated a reduced basis $\mathbf{b}_1, \ldots, \mathbf{b}_4$ of Γ by the L^3-algorithm. We have proved (using a.o. the fact that $N \leq 111$) that

$$\text{if} \quad |\mathbf{b}_1| > 2^{3/2} \sqrt{4(K_0 + 111)^2 + 3K_0^2} \quad \text{then}$$
$$H < \text{some constant of the size of } \log K_0.$$

In our case this constant turned out to be equal to 1169.

Thus, the p-adic reduction step applied twice (with $p = 17$ and $p = 19$), combined with the real reduction step, has given the new upper bound

$$H < K_0' := 1169,$$

which is a big progress compared to (9). It is still large, however, therefore we have repeated the same process, with K_0' in place of K_0, and found a new upper bound

$$H < K_0'' := 296, \quad N \leq 14.$$

Then, $n_0 \in \{0,1\}$, $\max\{|a_1|,|a_2|\} \leq 297$, $\max\{n_1,n_2\} \leq 14$, and we had to decide which tuples (n_0,n_1,n_2,a_1,a_2) satisfy (2). It is not realistic to check all tuples in the above ranges separately. Working modulo conveniently chosen primes, we were able to exclude most of them, and the few that remained we checked by straightforward computations. The final list of solutions of (1) is given in the table below.

Final remarks: 1. A detailed exposition of the content of this talk can be found in our paper [9].

2. All the computations needed in this paper have been performed on an AT personal computer. Most of the computer output is included in an appendix of [9].

Table 1. Solutions of (1)

n_0	n_1	n_2	$\pm(x,y)$		
0	0	0	$(1,0)$	$(0,-1)$	$(1,-1)$
0	0	0	$(2,1)$	$(1,-3)$	$(3,-2)$
0	0	1	$(1,2)$	$(2,-3)$	$(3,-1)$
0	0	2	$(4,5)$	$(5,-9)$	$(9,-4)$
0	1	0	$(3,1)$	$(1,-4)$	$(4,-3)$
0	1	0	$(3,2)$	$(2,-5)$	$(5,-3)$
0	1	0	$(15,8)$	$(8,-23)$	$(23,-15)$
0	1	1	$(1,6)$	$(6,-7)$	$(7,-1)$
0	1	1	$(3,5)$	$(5,-8)$	$(8,-3)$
0	1	1	$(28,15)$	$(15,-43)$	$(43,-28)$
0	2	1	$(59,31)$	$(31,-90)$	$(90,-59)$
0	2	1	$(31,15)$	$(15,-46)$	$(46,-31)$
0	2	1	$(18,13)$	$(13,-31)$	$(31,-18)$
0	2	2	$(206,109)$	$(109,-315)$	$(315,-206)$
0	2	5	$(896,37)$	$(37,-933)$	$(933,-896)$
0	3	1	$(97,54)$	$(54,-151)$	$(151,-97)$
1	0	0	$(1,1)$	$(1,-2)$	$(2,-1)$
1	0	1	$(7,4)$	$(4,-11)$	$(11,-7)$
1	0	1	$(13,7)$	$(7,-20)$	$(20,-13)$
1	0	1	$(5,2)$	$(2,-7)$	$(7,-5)$
1	1	0	$(4,1)$	$(1,-5)$	$(5,-4)$
1	1	1	$(10,1)$	$(1,-11)$	$(11,-10)$
1	1	2	$(29,20)$	$(20,-49)$	$(49,-29)$
1	1	3	$(73,13)$	$(13,-86)$	$(86,-73)$
1	2	0	$(4,7)$	$(7,-11)$	$(11,-4)$
1	2	2	$(712,379)$	$(379,-1091)$	$(1091,-712)$

References

[1] A.K. Agrawal, J.H. Coates, D.C. Hunt and A.J. van der Poorten, *Elliptic curves of conductor 11*, Math. Comp. **35** (1980), 991-1002.

[2] W. Ljunggren, *Einige Bemerkungen über die Darstellung ganzer Zahlen durch binäre kubische Formen mit positiver Diskriminante*, Acta Math. **75** (1942), 1-21.

[3] A.K. Lenstra, H.W. Lenstra jr. and L. Lovász, *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515-534.

[4] L.J. Mordell, *Diophantine equations*, Pure and Applied Mathematics Vol. 30, Academic Press, London & New York, 1969.

[5] T.N. Shorey and R. Tijdeman, *Exponential diophantine equations*, Cambridge Tracts in Mathematics Vol. 87, Cambridge University Press, Cambridge, 1986.

[6] N. Tzanakis, *The diophantine equation $x^3 - 3xy^2 - y^3 = 1$ and related equations*, J. Number Th. **18** (1984), 192-205.

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

[8] N. Tzanakis and B.M.M. de Weger, *On the practical solution of the Thue equation*, J. Number Th. **31** (1989), 99-132.

[9] N. Tzanakis and B.M.M. de Weger, *Solving a specific Thue-Mahler equation*, Memorandum No. 793, Faculty of Applied Mathematics, University of Twente, 1989, to appear in Math. Comp.

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

[11] B.M.M. de Weger, *Algorithms for diophantine equations*, CWI-Tract No. 65, Centre for Mathematics and Computer Science, Amsterdam, 1989.

[12] K.R. Yu, *Linear forms in p-adic logarithms II*, Compositio Math. **74** (1990), 15-113.