

S-Unit Equations and Integer Solutions to Exponential Diophantine Equations

Noriko HIRATA-KOHNO

October 19, 2004

S 単数方程式と指数方程式の整数解
日本大学理工学部数学科
平田典子

Abstract

In this article, we present some new applications of unit equations and linear forms in logarithms to obtain a simple upper bound for the number of the purely exponential Diophantine equations. The main idea essentially relies on a refined result of a bound for the number of the solutions to *S*-unit equations, due to F. Beukers and H. P. Schlickewei as well as that by J. -H. Evertse, H. P. Schlickewei and W.M. Schmidt [Be-Schl] [E-Schl-Schm]. The tool to obtain a bound for the size of the solutions is the theory of linear forms in *m*-adic logarithms where *m* denotes a positive integer not necessarily a prime.

Keywords: Diophantine approximation, Unit equation, Linear forms in logarithms, Exponential Diophantine equations.

1 Introduction

Let us denote by \mathbb{Z} the set of the rational integers. Let $a, b, c \in \mathbb{Z}$ where $a, b, c \geq 2$ and $(a, b, c) = 1$.

Consider the exponential Diophantine equation

$$a^x + b^y = c^z \tag{1}$$

in unknowns $a, b, c, x, y, z \in \mathbb{Z}$, $x, y, z \geq 1$.

In this case, we see $(a, b, c) = 1 \iff (a, b) = 1 \iff (a, c) = 1 \iff (b, c) = 1$.

Let us recall a conjecture due to Tijdeman (sometimes called Beal's conjecture):

Conjecture 1. (*Tijdeman*) The equation $a^x + b^y = c^z$ has no solutions in $(a, b, c, x, y, z) \in \mathbb{Z}^6$ with $a, b, c \geq 2, x, y, z \geq 3$.

The equation in the conjecture concerns 6 unknowns. It is known that the *abc*-conjecture of Masser-Osterlé type implies that there is an effective positive number H which depends only on the $\varepsilon > 0$ in the *abc*-conjecture such that Conjecture 1 is true for $x, y, z \geq H$.

It is also investigated by Darmon-Granville, Darmon-Merel, Kraus, Bennett and others that the number of the solutions a, b, c to (1) is finite if x, y, z are fixed with $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} < 1$.

When we consider again the six numbers as unknowns, a slightly different question is asked;

Conjecture 2. (*Fermat-Catalan*) If $\frac{1}{x} + \frac{1}{y} + \frac{1}{z} < 1$ then the number of the solutions in $(a, b, c, x, y, z) \in \mathbb{Z}^6$ with $a, b, c \geq 2, x, y, z \geq 2$ is finite.

For example some solutions to the equation of Conjecture 2 including large ones found by Beukers-Zagier are as follows.

Example 1. $2^5 + 7^2 = 3^4$
 $7^3 + 13^2 = 2^9$
 $2^7 + 17^3 = 71^2$
 $3^5 + 11^4 = 122^2$
 $17^7 + 76271^3 = 21063928^2$
 $1414^3 + 2213459^2 = 65^7$
 $9262^3 + 15312283^2 = 113^7$
 $43^8 + 96222^3 = 30042907^2$
 $33^8 + 1549034^2 = 15613^3$.

2 Our problem

Up to now, we assume till the end of the text that the integers a, b, c are fixed. We then consider x, y, z as unknowns only. Precisely, let us fix $a, b, c \in \mathbb{Z}$ with $a, b, c \geq 2, (a, b, c) = 1$ and consider the equation

$$a^x + b^y = c^z \quad (2)$$

in unknowns $x, y, z \in \mathbb{Z}$ with $x, y, z \geq 2$.

In 1993, K. Malher used p -adic Thue-Siegel method to show that the solutions x, y, z to (2) are only finitely many. The bound for the number of the solutions should depend on $\omega(abc)$ the number of the primes dividing abc . A. O. Gel'fond gave in 1940 a lower bound of linear forms in p -adic logarithms and then a bound for the

size of the solutions, namely an effectively calculable constant $C > 0$ depending only on a, b, c such that $\max\{|x|, |y|, |z|\} < C$.

Around 1994, Terai and J smanowicz conjectured (see for example [Cao-Dong]) that if there exists a solution (x_0, y_0, z_0) then this is the only solution:

Conjecture 3. (Terai and J smanowicz) *The number of the solutions to the equation (2) is at most 1.*

There are several investigations concerning with Conjecture 3 by N. Terai, Z. Li, or others. They essentially show that there exist particular examples of a, b, c where Conjecture 3 holds. Remark that the identity $2^n + 2^n = 2^{n+1}$ does not give infinitely many solutions. It is also noted that there are trivial identities:

$$2^{n+2} + (2^n - 1)^2 = (2^n + 1)^2 \quad (a = 2 \text{ or } a = 2^{n+1}, b = 2^n - 1, c = 2^n + 1)$$

$$2^1 + 2^n - 1 = 2^n + 1 \quad (a = 2, b = 2^n - 1, c = 2^n + 1).$$

Among the knowns, we quote an example of Conjecture 3 which is made by Terai;

Example 2. (Terai)

Suppose that u is even, $a = u^3 - 3u$, $b = 3u^2 - 1$, b is a prime, $c = u^2 + 1$, and that there exists a prime l such that l divides $u^2 - 3$ with $3|e$ for an integer $e > 0$ satisfying $2^e - 1$ is divisible by l . Then the equation (2) has the only solution $(2, 2, 3)$.

3 Our statement

Firstly we state a theorem which is quick to obtain.

Theorem 1. *Let N be the number of the solutions to (2). Then we have*

$$N \leq 2^{36}.$$

The advantage of Theorem 1 is the fact that the number N is *independent* of the number a, b, c especially of $\omega(abc)$.

It might be possible to refine the bound in Theorem 1 ; we will prove this by a forthcoming article.

Secondly we show a bound for the size of the solutions:

Theorem 2. *Suppose that c is odd and that c has the prime decomposition $c = p_1^{r_1} p_2^{r_2} \cdots p_l^{r_l}$. Suppose that there exists an integer $g \in \mathbb{Z}$, $g \geq 2$ coprime with c such that*

$$v_{p_i}(a^g - 1) \geq r_i$$

and

$$v_{p_i}(b^g - 1) \geq 1$$

for any prime $p_i | c$. Then we have

$$\max\{|x|, |y|, |z|\} \leq 2^{288} \sqrt{abc} (\log(abc))^3.$$

4 Outline of the proof

Theorem 1 is easily implied by the following theorem due to F. Beukers and H. P. Schlickewei [Be-Schl]. Their result corresponds to a refinement in a low-dimensional case of a theorem by J. -H. Evertse, H. P. Schlickewei and W.M. Schmidt [E-Schl-Schm].

Theorem 3. *(Evertse-Schlickewei-Schmidt) Let $n \in \mathbb{Z}$, $n \geq 1$. Let K be an algebraic closed field with characteristic 0, Γ be a finitely generated subgroup of the multiplicative group $(K - \{0\})^n$. Denote by $r < \infty$ the number of the generators of Γ . Let $a_i \in K - \{0\}$. Consider the equation $a_1 X_1 + \cdots + a_n X_n = 1$ in unknowns X_1, \dots, X_n in Γ supposed the subsum satisfying $\sum_{i \in I} a_i X_i \neq 0$ for any non-empty proper subset I of $\{1, 2, \dots, n\}$. Then we have that the number of the solutions $(x_1, \dots, x_n) \in \Gamma^n$ to the equation $a_1 X_1 + \cdots + a_n X_n = 1$ is at most*

$$\exp((6n)^{3n}(r+1)).$$

When $n = 2$, a refinement of the above is as follows:

Theorem 4. *(Beukers-Schlickewei) Let $n = 2$. Then we have that the number of the solutions $(x_1, x_2) \in \Gamma^2$ to the equation $a_1 X_1 + a_2 X_2 = 1$ is at most*

$$2^{9(r+1)}.$$

Proof of Theorem 1

It is enough to apply the theorem of Beukers-Schlickewei. Our equation is $a^x + b^y = c^z$, thus

$$\frac{a^x}{c^z} + \frac{b^y}{c^z} = 1.$$

We see that it turns out to consider the equation $X + Y = 1$ with X, Y in “ a, b, c -units”, namely in $\Gamma = \langle a, b, c \rangle = \{a^k b^l c^m \mid k, l, m \in \mathbb{Z}\}$. Thus just use Beukers-Schlickewei with $r = 3$ to arrive at 2^{36} .

When a, b, c are distinct primes, then we may use Evertse’ bound $3 \cdot 7^{12}$.

If we consider $S = \{p|abc\}$ we do not get independence of $\omega(abc)$ in the statement.

Proof of Theorem 2

Let m be an integer ≥ 2 not necessarily a prime. The concept of linear forms in m -adic logarithms is basically introduced by Malher and is revisited by Y. Bugeaud.

Recall the definition of m -adic valuation. Let $m = p_1^{r_1} \cdots p_l^{r_l}$ where $p_1 < \cdots < p_l$ are primes, $r_1, \dots, r_l \in \mathbb{Z}, > 0$. Let $x \in \mathbb{Z}, x \neq 0$. We recall that the p -adic valuation is $v_p(x) :=$ the greatest integer $v \geq 0$ such that $p^v | x$. Following this, we define

$$\begin{aligned} v_m(x) &:= \text{the greatest integer } v \geq 0 \text{ such that } m^v | x \\ &= \min_{1 \leq i \leq l} \left[\frac{v_{p_i}(x)}{r_i} \right] \end{aligned}$$

where $[\cdot]$ denotes the Gauss' symbol.

For a rational number $\frac{a}{b} \neq 0$, $a, b \in \mathbb{Z}, (a, b) = 1$, we define $v_m\left(\frac{a}{b}\right) := v_m(a) - v_m(b)$.

We state a variant of a lemma of Y. Bugeaud by removing some specific conditions. Denote here by $h(\cdot)$ the absolute logarithmic height. Theorem 2 is deduced by using Lemma 1:

Lemma 1. *Let $\Lambda := \alpha_1^{b_1} - \alpha_2^{b_2} \neq 0$ where $\alpha_1, \alpha_2 \in \mathbb{Q}, \alpha_1 \neq \pm 1, b_1, b_2 \in \mathbb{Z}, b_1, b_2 > 0$. Let $m = p_1^{r_1} \cdots p_l^{r_l}$. Suppose $v_{p_i}(\alpha_1) = v_{p_i}(\alpha_2) = 0$ for any $p_i | m$. Suppose further that there exists an integer $g \in \mathbb{Z}, g > 0$, coprime with m such that*

$$v_{p_i}(\alpha_1^g - 1) \geq r_i,$$

$$v_{p_i}(\alpha_2^g - 1) \geq 1$$

and moreover

$$v_2(\alpha_1^g - 1) \geq 2,$$

$$v_2(\alpha_2^g - 1) \geq 2$$

if $2 | m$. Then there exists an effectively computable constant $C > 0$ depending on the data with

$$v_m(\Lambda) \leq \frac{Cm^2}{\max(\log m, 1)^2} \left(\log \left(\frac{|b_1|}{\log A_1} + \frac{|b_2|}{\log A_2} \right) \right)^2 \log A_1 \log A_2$$

where $\log A_i \geq \max(h(\alpha_i), \log m)$ ($i = 1, 2$).

References

- [Be-Schl] F. Beukers & H. P. Schlickewei, *The equation $x+y=1$ in finitely generated groups*, Acta Arith. 78. 2, 189–199, 1996.
- [Cao-Dong] Zhenfu Cao & Xiaolei Dong, *An application of a lower bound for linear forms in two logarithms to the Terai-Jésmanowicz conjecture*, Acta Arith. 110, 153–164, 2003.

- [E-Schl] J. -H. Evertse & H. P. Schlickewei, *The Absolute Subspace Theorem and linear equations with unknowns from a multiplicative group*, in *Number Theory in Progress, I*, (eds. K. Györy, H. Iwaniec, J. Urbanowicz), Walter de Gruyter, 121–142, 1999.
- [E-Schl-Schm] J. -H. Evertse, H. P. Schlickewei & W.M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, *Ann. Math.* 155, 1–30, 2002.
- [Pa-Schf] A. N. Parshin & I. R. Schfarevich (eds.), N. I. Fel'dman & Yu. V. Nesterenko (authors), *Number Theory IV*, *Encyclopaedia of Mathematical Sciences* vol. 44, 1998.
- [Schm1] W. M. Schmidt, *Diophantine approximation*, *Lecture Notes in Math.*, 785, Springer, 1980.
- [Schm2] W. M. Schmidt, *Diophantine approximation and Diophantine Equations*, *Lecture Notes in Math.*, 1467, Springer, 1991.
- [Sho-T] T. N. Shorey & R. Tijdeman, *Exponential Diophantine Equations*, *Cambridge Tracts in Math.*, Vol. 87, Cambridge Univ. Press, 1986.
- [Wa] M. Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups*, *Grundlehren der Math. Wissenschaften* 326, Springer, 2000.
- [Wü] G. Wüstholz, *A Panorama of Number Theory*, Cambridge Univ. Press, 2002.

Noriko HIRATA-KOHNO
Dept. of Mathematics
College of Science and Technology
NIHON University
Kanda, Chiyoda, Tokyo 101-8308
JAPAN