Publ. Math. Debrecen
71/3-4 (2007), 489–497

Further computational experiences on norm form equations with solutions forming arithmetic progressions

By ANDRÁS BAZSÓ (Debrecen)

Abstract. In this paper we present our computational experiences on those special solutions of the norm form equation $N_{K/\mathbb{Q}}(x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1}) = 1$ for which $x_0, \ldots, x_{n-1} \in \mathbb{Z}$ are consecutive elements of an arithmetic progression.

1. Introduction

The study of the subject of our paper has been initiated by BÉRCZES and PETHŐ [6], [5]. The problem itself first raised when BUCHMANN and PETHŐ [10] found by chance that in the field $K := \mathbb{Q}(\alpha)$ with $\alpha^7 = 3$, the integer

$$10 + 9\alpha + 8\alpha^2 + 7\alpha^3 + 6\alpha^4 + 5\alpha^5 + 4\alpha^6$$

is a unit. This means that the equation

$$N_{K/\mathbb{Q}}(x_0 + x_1\alpha + \cdots + x_6\alpha^6) = 1$$

has a solution $(x_0, \ldots, x_6) \in \mathbb{Z}^7$ such that the coordinates form an arithmetic progression. This led Bérczes and Pethő in [6] to investigate in more general context norm form equations with solutions whose coordinates form an arithmetic progression. They proved general effective and qualitative results in this direction. Further, BÉRCZES and PETHŐ [5] and BÉRCZES, PETHŐ and ZIEGLER [7] considered certain families of norm form equations and for these equations, they found all solutions whose coordinates form an arithmetic progression. The aim of our paper is to extend the result of BÉRCZES and PETHŐ [5].

Mathematics Subject Classification: 11D57, 11D59, 11B25.
Key words and phrases: norm form equation, arithmetic progression, binomial Thue equation.

2. Results

Let α be an algebraic integer of degree $n \geq 3$ and $K =: \mathbb{Q}(\alpha)$. Consider the equation

$$N_{K/\mathbb{Q}}\left(x_0 + x_1\alpha + \cdots + x_{n-1}\alpha^{n-1}\right) = 1 \tag{1}$$

in $x_0, \ldots, x_{n-1} \in \mathbb{Z}$.

Let α be a root of the polynomial $x^n - a$, where a is an integer such that $x^n - a$ is irreducible. Bérczes and Pethő [5] proved that equation (1) has no solution in integers forming an arithmetic progression when $4 \leq a \leq 100$. Now we extend their result for negative values of the parameter a. More precisely, for $-100 \leq a \leq -2$ we determine all such solutions of equation (1) for which $x_0, \ldots, x_{n-1} \in \mathbb{Z}$ are consecutive terms of an arithmetic progression.

Our main result is the following theorem.

Theorem. *Let $n \geq 3$ be an integer, let α be a root of the irreducible polynomial $x^n - a \in \mathbb{Z}[x]$. Put $K := \mathbb{Q}(\alpha)$ and suppose that $-100 \leq a \leq -2$. Then the only solutions of equation (1) which form an arithmetic progression are $(2, 1, 0)$ when $(n, a) = (3, -7)$, and $(-2, -1, 0)$ when $(n, a) = (3, -9)$.*
In the case when $(n, a) = (11, -67)$ our result is conditional and depends on the truth of the generalized Riemann Hypothesis.

3. Auxiliary results

Lemma 3.1 (Á. Pintér)**.** *Let*

$$F(x, y) = ax^n - by^n, \quad a \neq b$$

be a binary form of degree $n \geq 3$, with positive integer coefficients a and b. Set $A = \max\{a, b, 3\}$. Suppose that

$$F(x, y) = c$$

with $x > |y| > 0$, $3\log(1.5|c/b|) \leq 7400\frac{\log A}{\lambda}$ and $\frac{\log 2c}{\log 2} \leq 8\log A$. Then we have

$$n \leq \min\left(7400\frac{\log A}{\lambda},\ 3106\log A\right) := B(A),$$

where λ is an arbitrary constant.

Proof. See Á. Pintér [18]. □

Now we consider the equation

$$Aa^n + Bb^n = Cc^2 \tag{2}$$

in $a, b, c \in \mathbb{Z}$. Following the method of Bennett and Skinner [4] we first associate elliptic curves to solutions (a, b, c) of (2) as follows. We assume that aA, bB and cC are pairwise coprime, and that C is squarefree. Without loss of generality, we may suppose we are in one of the following situations:

(i) $abABC \equiv 1 \pmod 2$ and $b \equiv -BC \pmod 4$,

(ii) $ab \equiv 1 \pmod 2$ and either $\mathrm{ord}_2(B) = 1$ or $\mathrm{ord}_2(C) = 1$,

(iii) $ab \equiv 1 \pmod 2$, $\mathrm{ord}_2(B) = 2$ and $c \equiv -bB/4 \pmod 4$,

(iv) $ab \equiv 1 \pmod 2$, $\mathrm{ord}_2(B) \in \{3, 4, 5\}$ and $c \equiv C \pmod 4$,

(v) $\mathrm{ord}_2(Bb^n) \geq 6$ and $c \equiv C \pmod 4$,

where $\mathrm{ord}_2(u)$ denotes the largest integer k with $2^k | u$.

In cases (i) and (ii), we will consider the curve

$$E_1(a, b, c) : Y^2 = X^3 + 2cCX^2 + BCb^nX.$$

In cases (iii) and (iv), we will consider

$$E_2(a, b, c) : Y^2 = X^3 + cCX^2 + \frac{BCb^n}{4}X,$$

and in (v),

$$E_3(a, b, c) : Y^2 + XY = X^3 + \frac{cC - 1}{4}X^2 + \frac{BCb^n}{64}X.$$

After this via Galois representations, we can associate modular forms to these elliptic curves, so in this way in fact we associate modular forms to the solutions (a, b, c) of equation (2).

For a given prime q and non-zero integer u, set

$$\mathrm{Rad}_q(u) := \prod_{\substack{p \mid u \\ p \neq q}} p$$

where the product is taken over all positive primes p distinct of q and dividing u. Put

$$\epsilon_2 := \begin{cases} 1 & \text{if } \mathrm{ord}_2(Bb^n) = 6 \\ 2 & \text{if } \mathrm{ord}_2(Bb^n) \geq 7 \\ 4 & \text{if } \mathrm{ord}_2(B) = 2 \text{ and } b \equiv -BC/4 \pmod 4 \\ 8 & \text{if } \mathrm{ord}_2(B) = 2 \text{ and } b \equiv BC/4 \pmod 4 \text{ or if } \mathrm{ord}_2(B) \in \{4, 5\} \\ 32 & \text{if } \mathrm{ord}_2(B) = 3 \text{ or if } bBC \text{ is odd} \\ 128 & \text{if } \mathrm{ord}_2(B) = 1 \\ 256 & \text{if } C \text{ is even.} \end{cases}$$

Lemma 3.2 (M. A. Bennett and C. M. Skinner)**.** *Suppose that a, b, c, A, B, C are non-zero integers with aA, bB, cC pairwise coprime, $ab \neq \pm 1$, satisfying equation (2) with $n \neq 7$ a prime and $(n, ABC) = 1$. Then there exists a cuspidal newform $f = \sum_{r=1}^{\infty} c_r q^r$ of weight 2, trivial Nebentypus character and level N, with $N := \mathrm{Rad}_2(AB)\,\mathrm{Rad}_2(C)^2\epsilon_2$.*
Moreover, if we write K_f for the field of definition of the Fourier coefficients c_r of the form f and suppose that p is a prime coprime to nN, then

(i) *if $ab \equiv 0 \pmod p$ then*

$$\mathrm{Norm}_{K_f/\mathbb{Q}}(c_p - a_p) \equiv 0 \pmod n,$$

where $a_p = \pm(p+1)$,

(ii) *otherwise*

$$\mathrm{Norm}_{K_f/\mathbb{Q}}(c_p - a_p) \equiv 0 \pmod n,$$

where $a_p = \pm(p+1)$ or $a_p \in \{x : |x| < 2\sqrt{p},\ x \equiv 0 \pmod 2\}$.
Further, if the solution (a, b, c) arises from a rational cuspidal newform corresponding to an elliptic curve $E/\mathbb{Q}$ then if $p \nmid ab$ we have $a_p = a_p(E) = p + 1 - \#E(\mathbb{F}_p)$, where $\#E(\mathbb{F}_p)$ is the number of points on E over the finite field $\mathbb{F}_p$.

Proof. For a proof see Bennett and Skinner [4], and Bugeaud, Mignotte and Siksek [11]. □

4. Proof of the theorem

First we prove a lemma concerning a special family of generalized Thue-equations, and we use this lemma to prove our Theorem.

Lemma 4.1. *The only solutions of the generalized Thue-equation*

$$X^n - aY^n = (a-1)^2 \tag{3}$$

in (n, a, X, Y) for $-100 \leq a \leq -2$, are those listed in Table 1 below.
In the case when $(n, a) = (11, -67)$ the result depends on the truth of the generalized Riemann Hypothesis.

n	a	(X, Y)
3	-97	$(35, -7)$
3	-63	$(4, 4), (16, 0), (64, -16)$
3	-62	$(1,\ 4)$
3	-61	$(13,\ 3)$
3	-39	$(16, -4)$
3	-35	$(11, -1), (46, -14)$
3	-27	$(10, -2)$
3	-26	$(3, 3), (9, 0), (27, -9)$
3	-25	$(1,\ 3)$
3	-18	$(-5, 3), (7, 1)$
3	-12	$(-11, 5)$
3	-9	$(7, -3)$
3	-7	$(-5, 3), (2, 2), (4, 0), (8, -4)$
3	-6	$(1,\ 2)$
3	-3	$(-2, 2)$
4	-99	$(-10, 0), (10, 0)$
4	-80	$(-9, 0), (-3, -3), (-3, 3), (3, -3), (3, 3), (9, 0)$
4	-79	$(-1, -3), (-1, 3), (1, -3), (1, 3)$
4	-63	$(-8, 0), (8, 0)$
4	-48	$(-7, 0), (7, 0)$
4	-35	$(-6, 0), (6, 0)$
4	-24	$(-5, 0), (5, 0)$
4	-15	$(-4, 0), (-2, -2), (-2, 2), (2, -2), (2, 2), (4, 0)$
4	-14	$(-1, -2), (-1, 2), (1, -2), (1, 2)$
4	-8	$(-3, 0), (3, 0)$
4	-3	$(-2, 0), (2, 0)$
5	-31	$(2, 2), (4, 0), (8, -4)$
5	-30	$(1, 2)$
6	-63	$(2, 2), (-2, -2), (2, -2), (-2, 2), (4, 0), (-4, 0)$
6	-26	$(3, 0), (-3, 0)$
6	-7	$(2, 0), (-2, 0)$
8	-80	$(3, 0), (-3, 0)$
8	-15	$(2, 0), (-2, 0)$
10	-31	$(2, 0), (-2, 0)$
12	-63	$(2, 0), (-2, 0)$

Table 1.

PROOF. Equation (3) is a so-called binomial Thue-equation. We note that a wide range of diophantine problems leads to such equations (see e.g. [1], [2], [3], [12], [13], [15], [17], [19], [18]).

Clearly, it is enough to solve equation (3) for $n = 4$ and in the cases when n is an odd prime. The other cases are simple consequences of these.

As a first step we use Lemma 3.1. Clearly, the conditions of Lemma 3.1 are fulfilled, so it provides an upper bound $B(a)$ for the degree n of the Thue-equation (3) in terms of a. Since $|a| \leq 100$, this shows that in order to prove Lemma 4.1 we have to consider only finitely many cases for n. The following table contains the approximate value of the bound $B(a)$ for some values of $|a|$.

$\|a\|$	10	20	30	40	50	60	70	80	90	100
$B(a)$	7151	9304	10564	11457	12150	12717	13195	13610	13976	14303

Table 2.

The second step is to use a well known local argument (see e.g. [16], [20], [3] and [5]) to prove that apart of a few exceptions equation (3) has no solutions in X, Y for $-100 \leq a \leq -2$ and $11 \leq n \leq B(a)$. For sake of completeness, we sketch the main idea of this local method. Choose a small integer k such that $p = 2kn + 1$ is a prime. Then both X^n and Y^n are either $2kth$ roots of unity (mod p) or zero. Thus we have to check the congruence

$$X^n - aY^n \equiv (a-1)^2 \pmod{p}$$

only in $(2k+1)^2$ cases. Programmed in the computer algebra package MAGMA, this method works very efficiently. Those values of $11 \leq n \leq B(a)$ and $-100 \leq a \leq -2$ for which this method does not prove the unsolvability of equation (3) are listed in Table 3.

n	11	11	11	11	11	11	11	11	13	13	13	13	13
a	-2	-36	-45	-46	-55	-67	-78	-89	-8	-12	-21	-28	-52

n	13	13	13	13	13
a	-71	-76	-81	-82	-91

n	17	17	17	17	17	17	19	19	19	19	19	19	23
a	-9	-42	-45	-46	-52	-100	-14	-51	-60	-68	-77	-99	-94

Table 3.

The third step is to solve one by one the remaining equations. Wherever it is possible we use the Thue-solver implemented in the computer algebra packages MAGMA [9] and PARI [21].

To solve the equations corresponding to pairs (n, a) with $n \in \{3, 4, 5, 7\}$ and $-100 \leq a \leq -2$ we use the package MAGMA. In order to solve the "exceptional" equations corresponding to pairs (n, a) listed in Table 3 we use the Thue-solver included in PARI. (For the main ideas behind the latest improvements on this Thue-solver implemented by G. Hanrot see [14] and [8].)

In the case when $(n,a) = (23,-94)$ the Thue-solvers of the mentioned computer algebra packages are unable to solve equation (3), and if

$$(n,a) \in \{(11,-89),(11,-67),(11,-46),(13,-82),(19,-77)\},$$

using PARI we are able to get only conditional result assuming the generalized Riemann Hypothesis.

If $n = 23$ and $a = -94$, we use Lemma 3.2 (i). First using the local approach with $p = 599$ we prove that equation (3) might have only solutions with $xy \equiv 0 \pmod{p}$ and then we use Lemma 3.2 (i) with this value of p. Here both for the local computations and for the computation of the needed Fourier coefficients of all occurring newforms we use again MAGMA.

If

$$(n,a) \in \{(11,-89),(11,-46),(13,-82),(19,-77)\},$$

we use Lemma 3.2 (ii). For instance, we consider the case when $n = 11$, $a = -89$. Equation (3) then takes the form

$$a^{11} + 89b^{11} = (-90)^2. \tag{4}$$

Let us suppose that we have a solution (a,b,c) of (4) with the conditions of Lemma 3.2. Then $\epsilon_2 = 32$ since bBC is odd and we have to consider the space of modular forms of level

$$N = \mathrm{Rad}_2(1 \cdot 89) \cdot \mathrm{Rad}_2(1)^2 \cdot 32 = 89 \cdot 32 = 2848.$$

17 cuspidal newforms occur at this level. Let us denote them by $f_1, \ldots, f_{17}$ and put $p = 23$. Then using MAGMA we get a contradiction on the case of all of these newforms if $a_p = a_{23} = \pm 24$ or $a_{23} \in \{x : |x| < 2\sqrt{23},\ x \equiv 0 \pmod 2\}$ except f_1 and f_4 that are both rational newforms. Analyzing the conditions on (a,b,c,A,B,C) we get that we can only be in case (i) among the above mentioned (i)–(v) cases. So we associate to the solution (a,b,c) of equation (4) the elliptic curve E_1 that now takes the form

$$E_1(a,b,c) : Y^2 = X^3 - 180X^2 + 89b^{11}X.$$

The local method shows that $b^{11} \equiv 22 \pmod{23}$ always holds. Thus the curve E_1 has the following form over $\mathbb{F}_{23}$:

$$E_1 :\ Y^2 = X^3 + 4X^2 + 3X,$$

which is independent of (a,b,c). For the number of points on this curve over $\mathbb{F}_{23}$ we get that $\#E_1(\mathbb{F}_{23}) = 24$ so we have

$$a_{23} = 23 + 1 - 24 = 0.$$

The Fourier series and the 23rd Fourier coefficient of f_1 and f_4 are

$$f_1 = q + 2q^5 - 2q^7 - 3q^9 + 4q^{11} + 4q^{13} - 2q^{17} + 8q^{19} + 6q^{23} + O\left(q^{24}\right),\ c_{23} = 6$$

and

$$f_4 = q + 2q^5 + 2q^7 - 3q^9 - 4q^{11} + 4q^{13} - 2q^{17} - 8q^{19} - 6q^{23} + O\left(q^{24}\right),\ c_{23} = -6,$$

respectively. Thus we get a contradiction in both cases since the corresponding norms are not divisible by 11. In the other cases we do similar computations.

Unfortunately in the case $n = 11$, $a = -67$ we find no way to prove the result unconditionally. □

Proof of the Theorem. Let $x_0, \dots, x_{n-1} \in \mathbb{Z}$ be a solution of equation (1) which forms an arithmetic progression and put $d := x_{i+1} - x_i$ for $i = 1, \dots, n-1$. Then equation (1) has the form

$$N_{K/\mathbb{Q}}\Big((1 + \alpha + \alpha^2 + \cdots + \alpha^{n-1})x_0 + (\alpha + 2\alpha^2 + \cdots + (n-1)\alpha^{n-1})d\Big) = 1. \quad (5)$$

In [6], Bérczes and Pethő showed that any solution x_0, d of equation (5) leads to a solution X, Y of equation (3) and these solutions are related to each other by the formulas $X := -x_0(a-1) - dan$ and $Y := -x_0(a-1) - dan + d(a-1)$. Lemma 4.1 gives us all solutions of equation (3), and these solutions are listed in Table 1.

Now to prove our Theorem, we have to check whether a solution of equation (3) leads to an integral solution of equation (1), which has coordinates forming an arithmetic progression, or not. Using Table 1 we can verify that this condition is fulfilled only if $(n, a, X, Y) \in \{(3, -7, -5, 3), (3, -9, 7, -3)\}$. Any other solution (X, Y) of equation (3) leads to a pair (x_0, d), where x_0 and d are not both integers. This concludes the proof of our Theorem. □

References

[1] M. A. Bennett, Rational approximation to algebraic numbers of small height: the Diophantine equation $|ax^n - by^n| = 1$, *J. Reine Angew. Math.* **535** (2001), 1–49.

[2] M. A. Bennett, Products of consecutive integers, *Bull. London Math. Soc.* **36** (2004), 683–694.

[3] M. A. Bennett, K. Győry and Á. Pintér, On the Diophantine equation $1^k + 2^k + \ldots + x^k = y^n$, *Compos. Math.* **140** (2004), 1417–1431.

[4] M. A. Bennett and C. M. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.* **56** (2004), 23–54.

[5] A. Bérczes and A. Pethő, Computational experiences on norm form equations with solutions from an arithmetic progression, *Glasnik Matematički. Serija III* **41**(61) (2006), 1–8.

[6] A. Bérczes and A. Pethő, On norm form equations with solutions forming arithmetic progressions, *Publ. Math. Debrecen* **65** (2004), 281–290.

[7] A. Bérczes, A. Pethő and V. Ziegler, Parametrized norm form equations with arithmetic progressions, *Journal of Symbolic Computation* **41** (2006), 790–810.

[8] Y. Bilu, G. Hanrot and P. M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, *J. Reine Angew. Math.* **539** (2001), 75–122.

[9] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[10] J. Buchmann and A. Pethő, Computation of independent units in number fields by Dirichlet's method, *Math. Comp.* **52** (1989), 149–159, S1–S14.

[11] Y. Bugeaud, M. Mignotte and S. Siksek, Classical and modular approaches to exponential Diophantine equations II: The Legesgue–Nagell equation, *Compositio Mathematica* **142** (2006), 31–62.

[12] K. Győry, I. Pink and A. Pintér, Power values of polynomials and binomial Thue-Mahler equations, *Publ. Math. Debrecen* **65** (2004), 341–362.

[13] K. Győry and Á. Pintér, Almost perfect powers in products of consecutive integers, *Monatsh. Math.* **145** (2005), 19–33.

[14] G. Hanrot, Solving Thue equations without the full unit group, *Math. Comp.* **69** (2000), 395–405.

[15] G. Hanrot, N. Saradha and T. N. Shorey, Almost perfect powers in consecutive integers, *Acta Arith.* **99** (2001), 13–25.

[16] A. Kraus, Majorations effectives pour l'équation de Fermat généralisée, *Canad. J. Math.* **49** (1997), 1139–1161.

[17] L. J. Mordell, Diophantine Equations, *Academic Press*, *London*, 1969.

[18] A. Pintér, On the power values of power sums, *J. Number Theory* (*to appear*).

[19] T. N. Shorey and R. Tijdeman, Exponential Diophantine equations, *Cambridge Univ. Press*, *Cambridge – New York*, 1986.

[20] S. Siksek and J. E. Cremona, On the Diophantine equation $x^2 + 7 = y^m$, *Acta Arith.* **109** (2003), 143–149.

[21] The PARI Group, Bordeaux, PARI/GP, version, 2004, available from `http://pari.math.u-bordeaux.fr/`, `2.1.5`.

ANDRÁS BAZSÓ
INSTITUTE OF MATHEMATICS
UNIVERSITY OF DEBRECEN
H-4010 DEBRECEN, P.O. BOX 12
HUNGARY

E-mail: bazsoa@math.klte.hu

(Received May 17, 2006; revised March 12, 2007)