COMPUTATIONAL EXPERIENCES ON NORM FORM EQUATIONS WITH SOLUTIONS FORMING ARITHMETIC PROGRESSIONS

ATTILA BÉRCZES AND ATTILA PETHŐ

ABSTRACT. In the present paper we solve the equation $N_{K/\mathbb{Q}}(x_0+x_1\alpha+x_2\alpha^2+\cdots+x_{n-1}\alpha^{n-1})=1$ in $x_0,\ldots,x_{n-1}\in\mathbb{Z}$, such that $x_0,\ldots,x_{n-1}$ is an arithmetic progression, where α is a root of the polynomial x^n-a, for all integers $2\le a\le 100$ and $n\ge 3$.

1. INTRODUCTION

In [6] we investigated a problem which originates in an article of Buchmann and Pethő [9]. More precisely, they 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 diophantine 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 us in [6] to investigate in more general context norm form equations with solutions whose coordinates form an arithmetic progression. There we proved effective and qualitative results in the topic. Here we summarize our computational experiences with solutions of special norm form equations whose coordinates form an arithmetic progression.

2000 Mathematics Subject Classification: 11D57, 11D59, 11B25.

Keywords and Phrases: norm form equation, arithmetic progression, binomial Thue equation.

The research was supported in part by the Hungarian Academy of Sciences (A.B.), by grants T42985 (A.B., A.P.), T38225 (A.B., A.P.) and T48791 (A.B.) of the Hungarian National Foundation for Scientific Research.

2. Results

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

$$N_{K/\mathbb{Q}}(x_0 + x_1\alpha + x_2\alpha^2 + \cdots + x_{n-1}\alpha^{n-1}) = 1 \text{ in } x_0, \ldots, x_{n-1} \in \mathbb{Z}. \tag{1}$$

Let α be a root of the polynomial $x^n - a$, where a is an integer such that $x^n - a$ is irreducible. For $2 \leq a \leq 100$ we determine all such solutions of equation (1) for which $x_0, \ldots, x_{n-1}$ are consecutive terms in an arithmetic progression. The case $a = 2, 3$ was already considered in [6]. For sake of completeness we include the following theorem, which was proved there.

Theorem 2.1. *Let α be an algebraic integer of degree n and consider equation (1).*

(i) *If α is a root of the polynomial $x^n - 2$ $(n \geq 3)$ then for odd $n \in \mathbb{N}$ the n-tuples $(2n-1, 2n-2, \ldots, n)$, $(1, 1, \ldots, 1)$ and for even $n \in \mathbb{N}$ the n-tuples $(2n-1, 2n-2, \ldots, n)$, $(-2n+1, -2n+2, \ldots, -n)$, are the only solutions of equation (1) which form an arithmetic progression.*

(ii) *If α is a root of the polynomial $x^n - 3$ $(n \geq 3)$ then for each odd $n \in \mathbb{N}$ the n-tuple $(\frac{3n-1}{2}, \frac{3n-3}{2}, \ldots, \frac{n+1}{2})$ is the only solution of equation (1) which forms an arithmetic progression, and we note, that for even $n \in \mathbb{N}$ there are no such solutions at all.*

Now we present our main result:

Theorem 2.2. *Let $n \geq 3$ be an integer, let α be a root of the irreducible polynomial, $x^n - a \in \mathbb{Z}[x]$, and put $K := \mathbb{Q}(\alpha)$. Suppose that $4 \leq a \leq 100$. Then equation (1) has no solutions in integers $x_0, \ldots, x_{n-1} \in \mathbb{Z}$ which are consecutive elements in an arithmetic progression.*

3. Proof of Theorem 2.2

3.1. **Reduction to the equation $X^n - aY^n = (a-1)^2$.** Put $d := x_{i+1} - x_i$. Then equation (1) has the form

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

In [6] we have shown that any solution x_0, d of the equation (2) leads to a solution X, Y of the equation

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

and these solutions are related to each other by the formulas $X := -x_0(a-1) - dan$ and $Y := -x_0(a-1) - dan + d(a-1)$.

Now to prove Theorem 2.2 we need to solve completely equation (3) for $4 \leq a \leq 100$. Equation (3) is a so-called binomial Thue equation, and a wide range of diophantine problems leads to such equations (see e.g. [1], [2], [3], [11], [12], [14], [17], [21], [18]).

Lemma 3.1. *The only solutions of equation (3) for* $4 \leq a \leq 100$ *are those listed in Table 1.*

Table 1: Table 1

n	a	(X, Y)
3	9	$(-8,-4), (-2,-2), (4,0)$
6	9	$(2,0), (-2,0)$
3	10	$(1,-2), (11,5)$
3	19	$(7,1)$
3	28	$(-27,-9), (-3,-3), (9,0)$
6	28	$(3,0), (-3,0)$
3	29	$(1,-3)$
3	36	$(13,3)$
3	37	$(10,-2)$
3	38	$(7,-3), (11,-1)$
3	57	$(-8,-4)$
3	65	$(-64,-16), (-4,-4), (16,0)$
6	65	$(4,0), (-4,0)$
12	65	$(2,0), (-2,0)$
3	66	$(1,-4)$
3	73	$(8,-4)$
3	74	$(47,11)$

n	a	(X, Y)
3	93	$(118, 26)$
4	5	$(6, 4), (-6, 4), (-6, -4), (6, -4), (2, 0), (-2, 0)$
4	10	$(3, 0), (-3, 0)$
4	17	$(4, 0), (-4, 0)$
8	17	$(2, 0), (-2, 0)$
4	26	$(5, 0), (-5, 0)$
4	37	$(6, 0), (-6, 0)$
4	50	$(7, 0), (-7, 0)$
4	65	$(8, 0), (-8, 0), (12, 4), (-12, 4), (-12, -4), (12, -4)$
4	82	$(9, 0), (-9, 0)$
8	82	$(3, 0), (-3, 0)$
4	90	$(37, 12), (-37, 12), (-37, -12), (37, -12)$
5	33	$(-8, -4), (-2, -2), (4, 0)$
10	33	$(2, 0), (-2, 0)$
5	34	$(1, -2)$

Lemma 3.1 provides an easy way to prove Theorem 2.2. Indeed, we have to show that no solution of the equation (3) leads to an integral solution of equation (1), which has coordinates forming an arithmetic progression.

Since $X := -x_0(a-1) - dan$ and $Y := -x_0(a-1) - dan + d(a-1)$, if a solution of (3) leads to an integral solution of equation (1) with coordinates forming an arithmetic progression, then we also have $a - 1 \mid Y - X$. Using Table 1 we can verify that this condition is fulfilled only if $(n, a, X, Y) = (3, 93, 118, 26)$. However, in this case we see that $x_0 = \frac{118-3\cdot 93}{92}$, which is not an integer.

Thus if we want to conclude the proof of Theorem 2.2, it remains us to prove Lemma 1. Clearly, it is enough to consider the cases where n is an odd prime, or 4, since the other cases are simple consequences of these.

3.2. **Baker-type bound for the degree.** First we need an upper bound for the degree n of the Thue-equation (3) in terms of a. Here we use a result of Pintér [18], which is a refinement of a theorem of Mignotte [16], achieved by iterative use of Baker's method.

Lemma 3.2. (Á. Pintér) *Let*

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

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

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

Since we have to deal with the case $4 \leq a \leq 100$ this lemma reduces our proof to a finite problem in terms of a and n, which means that there remain finitely many Thue-equations to be solved. However, the above bound is too large to make it possible to solve directly all the remaining Thue-equations. Thus we use local arguments in order to prove the insolvability of most of the remaining equations.

3.3. **Local arguments.** Here we adapt to our case a well-known local method which was used recently by Kraus [15], by Siksek and Cremona [22], and by Bennett [2].

Choose a small integer k such that $p = 2kn + 1$ is a prime. Then X^n and Y^n are both either $2k$-th roots of unity $\pmod p$ or zero. Thus we have to check

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

only in $(2k+1)^2$ cases. Programmed in MAGMA, this method works very efficiently, and proves that the majority of the equations

$$X^n - aY^n = (a-1)^2$$

with $4 \leq a \leq 100$ and $n \leq B(a)$ has no solution.

3.4. **The remaining cases.** There are several such equations for which this method does not give any contradiction. These have to be solved individually. To do so we use the computer algebra packages PARI and MAGMA which are able to solve Thue equations of moderate degrees, and when it is needed we also use the most advanced techniques for solving binomial Thue-equations involving the theory of modular forms. This approach is analogues to that employed by Wiles [25] to prove Fermat's Last Theorem. These methods were developed and improved by several authors. For relevant references see [4], [5], [10], [15], [19], [20]. Our application of these methods also involved computations using MAGMA.

First we present the method using the theory of modular forms. This is based on the following two lemmas. The first one is a theorem of Bennett and Skinner [4], and the second one a theorem of Kraus [15].

Lemma 3.3. (M.A. Bennet 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*

$$Aa^n + Bb^n = Cc^2$$

with $n \geq 7$ a prime. Then there exists a cuspidal newform $f = \sum_{r=1}^{\infty} c_r q^r$ of weight 2, trivial Nebentypus character and level $N := Rad_2(AB)Rad_2(C)^2\varepsilon_2$, where

$$\varepsilon_2 := \begin{cases} 1 & \text{if } \mathrm{ord}_2(Bb^n) = 6 \\ 2 & \text{if } \mathrm{ord}_2(Bb^n) \geq 7 \\ 4 & \text{if } \mathrm{ord}_2(B) = 2 \text{ and } b \equiv -BC/4 \pmod 4 \\ 8 & \text{if } \mathrm{ord}_2(B) = 2 \text{ and } b \equiv BC/4 \pmod 4, \\ & \text{or if } \mathrm{ord}_2(B) \in \{4, 5\} \\ 32 & \text{if } \mathrm{ord}_2(B) = 3 \text{ or if } bBC \text{ is odd} \\ 128 & \text{if } \mathrm{ord}_2(B) = 1 \\ 256 & \text{if } C \text{ is even.} \end{cases}$$

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*

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

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

(ii) *otherwise*

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

where $a_p = \pm(p+1)$ *or* $a_p \in \{x \ : \ |x| < 2\sqrt{p},\ x \equiv 0 \pmod{2}\}$.

Lemma 3.4. (A. Kraus) *Suppose that* a, b, c, A, B, C *are non-zero integers with* aA, bB, cC *pairwise coprime,* $ab \neq \pm 1$, *satisfying*

$$Aa^n + Bb^n = Cc^n$$

with $n \geq 5$ *a prime. Then there exists a cuspidal newform* $f = \sum_{r=1}^{\infty} c_r q^r$ *of weight* 2, *trivial Nebentypus character and level* $N := Rad_2(AB)Rad_2(C)^2\varepsilon_n$, *where*

$$\varepsilon_n := \begin{cases} 1 & \text{if } \operatorname{ord}_2(ABC) = 4 \\ 2 & \text{if } \operatorname{ord}_2(ABC) = 0 \text{ or if } \operatorname{ord}_2(ABC) \geq 5 \\ 8 & \text{if } \operatorname{ord}_2(ABC) = 2 \text{ or } 3 \\ 32 & \text{if } \operatorname{ord}_2(ABC) = 1. \end{cases}$$

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*

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

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

(ii) *otherwise*

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

where $a_p = \pm(p+1)$ *or* $a_p \in \{x \ : \ |x| < 2\sqrt{p},\ x \equiv p+1 \pmod{4}\}$.

These two deep and involved lemmas give a straightforward way to prove that equation (3) has no solutions for fixed values of a.

3.5. **Computational aspects.** The cases with $n = 3, 4, 5, 7$ were solved using the algorithms for solving Thue equations in the computer algebra packages PARI [24] and MAGMA [8]. The cases $(a, n) = (11, 17)$ and $(a, n) = (43, 17)$ were solved using Lemma 3.3 (ii). The cases $(a, n) = (23, 11)$, $(a, n) = (35, 13)$ and $(a, n) = (77, 13)$ were solved using Lemma 3.4 (ii). When solving the case $(a, n) = (31, 13)$ first we proved $79 \mid XY$ using the local approach, and then we used Lemma 3.4 (i), with the prime $p = 79$. Similarly, when solving the case $(a, n) = (9, 19)$ first we proved $571 \mid XY$ and then we used Lemma 3.4 (i) with this prime.

In the remaining cases we solved the Thue equations using the development version 2.2.8 of PARI which includes a new version of the routine for solving Thue-equations. (In these cases neither the stable version of PARI nor the one of MAGMA was able to solve the occurring Thue equations.) Some of the main ideas behind this new program can be found in the papers [7] and [13]. Since at the moment this is included only in the unstable version of PARI we used it only if we were not able to apply the other methods. These cases were the following: $(a, n) \in \{(33, 11), (33, 13), (41, 19), (56, 19), (57, 17), (58, 17), (61, 19), (74, 13), (79, 11), (83, 11), (85, 17), (88, 13), (94, 13), (95, 11), (95, 19), (96, 19), (99, 17)\}$.

We were unable to solve the equation

$$X^{31} - 93Y^{31} = 92^2.$$

We would like thank the referee for letting us know how to prove that this equation has no solutions. Suppose that $(X, Y) = (A, B)$ is an integral solution of the above equation. If we follow the method of [4], depending on whether $B \equiv 1 \pmod 4$ or $B \equiv -1 \pmod 4$, we may consider the elliptic curves

$$E_1 \ : \ y^2 = x^3 + 184x^2 - 93B^{31}x$$

or

$$E_2 \ : \ y^2 = x^3 + 184x^2 + A^{31}x,$$

respectively. Now by Lemma 3.3 of [4] we see that the associated mod 31 Galois representation arises from a weight 2 cuspidal newform $\sum c_n q^n$ of level $N = 32 \cdot 93 = 2976$. One can check (either by MAGMA or from

Stein's Modular Forms Database) that

$$c_5 \equiv 0, \pm 2, \pm 4, \pm 6 \pmod{31}$$

provides a contradiction for all such newforms, except two. These are numbered by $2976, 3$ and $2976, 4$ in Stein's database [23], and both of them corresponds to elliptic curves over $\mathbb{Q}$ with rational 2-torsion. In both cases we have $c_{17} = 4$. Computing the number of points over $GF(17)$ on E_1 and E_2, for each choice of A and B modulo 17, we find that this number is never 14 and thus we get a contradiction in all cases.

Acknowledgement. We would like to thank again the referee for solving equation $X^{31} - 93Y^{31} = 92^2$ for us, and also for his other valuable remarks, given in his report.

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 $1^k + 2^k + \cdots + x^k = y^n$, *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] M. A. Bennett, M. Vatsal and S. Yazdani, Ternary Diophantine equations of signature $(p, p, 3)$, *Compositio Math.*, **140** (2004), 1399–1416.

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

[7] 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.

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

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

[10] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's last theorem, *J. Reine Angew. Math.*, **490** (1997), 81–100.

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

[12] K. Győry and Á. Pintér, Almost perfect powers in products of consecutive integers, *Monatsh. Math.*, **145** (2005), 19–33.
[13] G. Hanrot, Solving Thue equations without the full unit group, *Math. Comp.*, **69** (2000), 395–405.
[14] G. Hanrot, N. Saradha and T. N. Shorey, Almost perfect powers in consecutive integers, *Acta Arith.*, **99** (2001), 13–25.
[15] A. Kraus, Majorations effectives pour l'équation de Fermat généralisée, *Canad. J. Math.*, **49** (1997), 1139–1161.
[16] M. Mignotte, A note on the equation $ax^n - by^n = c$. *Acta Arith.*, **75** (1996), 287–295.
[17] L. J. Mordell, *Diophantine equations*, Academic Press, London, 1969.
[18] Á. Pintér, On the power values of power sums, *J. Number Theory*, to appear.
[19] K. A. Ribet, On the equation $a^p + 2^\alpha b^p + c^p = 0$, *Acta Arith.*, **79** (1997), 7–16.
[20] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, *Duke Math. J.*, **54** (1987), 179–230.
[21] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Univ. Press, Cambridge–New York, 1986.
[22] S. Siksek and J. E. Cremona, On the Diophantine equation $x^2 + 7 = y^m$, *Acta Arith.*, **109** (2003), 143–149.
[23] W. Stein, *The Modular Forms Database*, `http://modular.ucsd.edu/Tables` (2004).
[24] The PARI Group, Bordeaux, *PARI/GP, version* `2.1.5`, 2004, available from `http://pari.math.u-bordeaux.fr/`.
[25] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math. (2)*, **141** (1995), 443–551.

A. Bérczes
Institute of Mathematics, University of Debrecen
Number Theory Research Group, Hungarian Academy of Sciences and University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail address: `berczesa@math.klte.hu`

A. Pethő
Faculty of Informatics, University of Debrecen
H-4010 Debrecen, P.O. Box 12, Hungary
E-mail address: `pethoe@inf.unideb.hu`