Publ. Math. Debrecen
65/3-4 (2004), 281–290

On norm form equations with solutions forming arithmetic progressions

By ATTILA BÉRCZES (Debrecen) and ATTILA PETHŐ (Debrecen)

To the memory of our friend Béla Brindza

Abstract. In the present paper we investigate such solutions of norm form equations $N_{K/\mathbb{Q}}(x_0+x_1\alpha+x_2\alpha^2+\cdots+x_{n-1}\alpha^{n-1}) = m$ for which $x_0, \ldots, x_{n-1} \in \mathbb{Z}$ are consecutive elements in an arithmetic progression.

1. Introduction

Buchmann and Pethő [3] 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

$$N_{K/\mathbb{Q}}(x_0 + x_1\alpha + \cdots + x_6\alpha^6) = 1 \tag{1.1}$$

Mathematics Subject Classification: 11D57, 11D59, 11B25.
Key words and phrases: norm form equation, Thue equation, arithmetic progression.
The research was supported in part by the Hungarian Academy of Sciences (A.B.), the Netherlands Organization for Scientific Research (A.B., A.P.), by grants F34981 (A.B.), N34001 (A.B., A.P.) T42985 (A.B., A.P.) and T38225 (A.B., A.P.) of the Hungarian National Foundation for Scientific Research and by the FKFP grant 3272-13066/201 (A.B.).

has a solution $(x_0, \dots, x_6) \in \mathbb{Z}^7$ such that the coordinates form an arithmetic progression. In this note we generalize (1.1) in three directions: first, we consider arbitrary number fields, second the integer on the right hand side of equation (1.1) is not restricted to 1, and finally it is allowed that the solutions form only nearly an arithmetic progression.

2. Results

To be more precise, let $K := \mathbb{Q}(\alpha)$ be an algebraic number field of degree n and $m \in \mathbb{Z}$ an integer. Consider the equation

$$N_{K/\mathbb{Q}}(x_0 + x_1\alpha + x_2\alpha^2 + \cdots + x_{n-1}\alpha^{n-1}) = m \quad \text{in } x_0, \dots, x_{n-1} \in \mathbb{Z}. \tag{2.2}$$

First we are interested in solutions of equation (2.2) which form nearly an arithmetic progression. To define what is meant by this notion, let $X = \max\{|x_0|, \dots, |x_{n-1}|\}$. The sequence $\{x_0, \dots, x_{n-1}\}$ forms nearly an arithmetic progression if there exists $d \in \mathbb{Z}$ and $0 < \delta \in \mathbb{R}$ such that

$$|(x_i - x_{i-1}) - d| < X^{1-\delta}, \quad i = 1, \dots, n-1. \tag{2.3}$$

Our main result is the following theorem.

Theorem 2.1. *Let α be an algebraic integer of degree $n \geq 3$ over $\mathbb{Q}$ and put $K := \mathbb{Q}(\alpha)$. Suppose that the algebraic number $\beta := \frac{n\alpha^n}{\alpha^n - 1} - \frac{\alpha}{\alpha - 1}$ is of degree at least 3, over $\mathbb{Q}$. Then there exists an effectively computable constant $c_1 > 0$ depending only on n, m and the regulator of K such that for any $0 < \delta < c_1$ and any solution of equation (2.2) with property (2.3) we have*

$$|x_i| < B \quad \text{for } i = 0, \dots, n-1,$$

where B is again an effectively computable constant depending only on n, m, δ, the regulator of K, and on the height of α.

In the special case when $\delta = 1$ we get a finiteness result concerning solutions of equation (2.2) which form an arithmetic progression.

Theorem 2.2. *Let α be an algebraic integer of degree $n \geq 3$ over $\mathbb{Q}$ and put $K := \mathbb{Q}(\alpha)$. Equation (2.2) has only finitely many solutions*

in $x_0, \ldots, x_{n-1} \in \mathbb{Z}$ *such that* $x_0, \ldots, x_{n-1}$ *are consecutive terms of an arithmetic progression, provided that none of the following two cases hold*

(i) α *has minimal polynomial of the form*

$$x^n - bx^{n-1} - \cdots - bx + (bn + b - 1)$$

with $b \in \mathbb{Z}$*;*

(ii) $\beta := \frac{n\alpha^n}{\alpha^n - 1} - \frac{\alpha}{\alpha - 1}$ *is a real quadratic number.*

Remark. In the example of Buchmann and Pethő [3] the minimal polynomial of α is $x^7 - 3$, which does not fit into case (i). Moreover $\mathbb{Q}(\alpha)$ is primitive, which excludes case (ii). Hence (1.1) has only finitely many solutions, the coordinates of which form an arithmetic progression. Later we will show, that the only solution of (1.1) such that the coordinates form an arithmetic progression is $(10, 9, 8, 7, 6, 5, 4)$.

Remark. Case (i) appears quite often. Indeed, elementary computation shows that the polynomial $x^n - bx^{n-1} - \ldots - bx + (bn + b - 1)$ is irreducible for $n = 2$ if $b \notin \{-3, 0, 12, 15\}$ and is irreducible for $n = 3$ if $b \notin \{-14, 0\}$. In contrast we found only one quartic integral α with defining polynomial $x^4 + 2x^3 + 5x^2 + 4x + 2$ such that the corresponding β is a real quadratic number. It is a root of $x^2 - 4x + 2$. Allowing however α not to be integral we can obtain a lot of examples.

Corollary 2.1. *Let* α *and* K *be as in Theorem 2.2, and suppose that* (i) *of Theorem 2.2 holds. Then there are infinitely many integers* m *such that equation* (2.2) *has infinitely many solutions* $x_0, \ldots, x_{n-1} \in \mathbb{Z}$ *such that* $x_0, \ldots, x_{n-1}$ *are consecutive terms of an arithmetic progression.*

Corollary 2.2. *Let* α *and* K *be as in Theorem 2.2, and suppose that* (ii) *of Theorem 2.2 holds. Then there are infinitely many integers* m *such that equation* (2.2) *has infinitely many solutions* $x_0, \ldots, x_{n-1} \in \mathbb{Z}$ *such that* $x_0, \ldots, x_{n-1}$ *are consecutive terms of an arithmetic progression.*

Theorem 2.3. *For any* $n \in \mathbb{N}$ $(n \geq 3)$ *there exists an algebraic integer* α *of degree* n *over* $\mathbb{Q}$ *such that the equation*

$$N_{K/\mathbb{Q}}(x_0 + x_1\alpha + x_2\alpha^2 + \cdots + x_{n-1}\alpha^{n-1}) = \pm 1 \text{ in } x_0, \ldots, x_{n-1} \in \mathbb{Z}, \quad (2.4)$$

where $K := \mathbb{Q}(\alpha)$, has a solution $(x_0, \dots, x_{n-1})$ having coordinates which are consecutive terms in an arithmetic progression. More precisely, the following statements are true:

(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 $(2n-1, 2n-2, \dots, n)$, $(-2n+1, -2n+2, \dots, -n)$, $(-1, -1, \dots, -1)$ and $(1, 1, \dots, 1)$ and for even $n \in \mathbb{N}$ the n-tuples $(2n-1, 2n-2, \dots, n)$, $(-2n+1, -2n+2, \dots, -n)$, $(-1, -1, \dots, -1)$, $(1,1,\dots,1)$, $(-4n+1,-4n+3,\dots,-2n+1)$ and $(4n-1, 4n-3, \dots, 2n-1)$ are the only solutions of equation (2.4) 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-tuples $\left(\frac{-3n+1}{2}, \frac{-3n+3}{2}, \dots, \frac{-n-1}{2}\right)$, $\left(\frac{3n-1}{2}, \frac{3n-3}{2}, \dots, \frac{n+1}{2}\right)$ are the only solutions of equation (2.4) which form an arithmetic progression, and for even $n \in \mathbb{N}$ there are no such solutions at all.*

The last theorem means that for any $n \geq 3$ there exists a unit ε of degree n such that there exists a $\mathbb{Q}$-basis $\omega_1, \dots, \omega_n$ of $\mathbb{Q}(\varepsilon)$ with the property that if $\varepsilon = \sum_{i=1}^{n} x_i \omega_i$ then the sequence $x_1, \dots, x_n$ is an arithmetic progression with positive difference. This answers partially problem CNTA 88:14 of [4]. The cited problem asks not for a $\mathbb{Q}$-basis but for an integral basis, which is usually not the case in our examples.

3. Proof of Theorems 2.1 and 2.2 and Corollaries 2.1 and 2.2

Put $c_i := (x_i - x_{i-1}) - d$. Then using (2.3), equation (2.2) can be written in the form

$$N_{K/\mathbb{Q}}\big((1 + \alpha + \alpha^2 + \cdots + \alpha^{n-1})x_0 + (\alpha + 2\alpha^2 + \cdots + (n-1)\alpha^{n-1})d + \mu\big) = m, \quad (3.5)$$

where $\mu = c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}$. Using that $x + 2x^2 + \cdots + (n-1)x^{n-1} = x(\frac{x^n-1}{x-1})'$ from (3.5) we get

$$N_{K/\mathbb{Q}}\left(\left(\frac{\alpha^n - 1}{\alpha - 1}\right)x_0 + \left(\frac{n\alpha^{n+1} - n\alpha^n - \alpha^{n+1} + \alpha}{(\alpha-1)^2}\right)d + \mu\right) = m, \quad (3.6)$$

which can be transformed to

$$N_{K/\mathbb{Q}}\left(\frac{\alpha^n-1}{\alpha-1}\right)N_{K/\mathbb{Q}}(x_0+\beta d+\lambda)=m, \tag{3.7}$$

where $\beta := \frac{n\alpha^n}{\alpha^n-1}-\frac{\alpha}{\alpha-1}$ and $\lambda := \mu\frac{\alpha-1}{\alpha^n-1}$. Put $M = N_{K/\mathbb{Q}}(\alpha^n-1)$ and multiply (3.7) by M^n. Then $\beta' = M\beta$ and $\lambda' = M\lambda$ are integers in K because α^n-1 divides M in $\mathbb{Z}_K$. Thus we obtain

$$N_{K/\mathbb{Q}}(Mx_0+\beta' d+\lambda')=m_1, \tag{3.8}$$

with $m_1 = M^n m/N_{K/\mathbb{Q}}(\frac{\alpha^n-1}{\alpha-1}) \in \mathbb{Z}$.

For $\gamma \in K$ let $\boxed{\gamma} = \max\{|\gamma^{(1)}|,\dots,|\gamma^{(n)}|\}$, the height of γ. To prove Theorem 2.1 we need the following:

Lemma 3.1. *Let K be an algebraic number field of degree $n \geq 3$ over $\mathbb{Q}$. Let $\beta' \in \mathbb{Z}_K$ be of degree at least three. Consider the equation*

$$N_{K/\mathbb{Q}}(x+\beta' y+\lambda')=m \tag{3.9}$$

in $x, y \in \mathbb{Z}$ and $\lambda' \in \mathbb{Z}_K$ with $\boxed{\lambda'} < \max\{|x|,|y|\}^{1-\delta}, 0<\delta<1$. Then there exist effectively computable constants $c_1, c_2 > 0$ depending only on n and the regulator of K such that for the solutions of equation (3.9) with $0<\delta<c_1$ we have

$$\max\{|x|,|y|\} < B_0^{c_2 1/\delta\log(1/\delta)},$$

where the effectively computable constant B_0 depends only on n, m and on the height of β'.

Proof. This is Theorem 1 of [5] except that there is assumed that $K = \mathbb{Q}(\beta')$. However analyzing the proof it is clear that it works in the slightly modified form too. □

Proof of Theorem 2.1. Let us assume that $x_0,\dots,x_{n-1} \in \mathbb{Z}$ with $X = \max\{|x_0|,\dots,|x_{n-1}|\}$ are solution of (2.2), which form a nearly arithmetic progression, i.e. there exist $d \in \mathbb{Z}$ with (2.3). Then choosing e.g. $i = 1$ we get $|d| < 3X$. Clearly,

$$\boxed{\mu} = \boxed{c_1\alpha + c_2\alpha^2+\cdots+c_{n-1}\alpha^{n-1}} \leq X^{1-\delta}\cdot\left(\boxed{\alpha}+\boxed{\alpha}^2+\cdots+\boxed{\alpha}^{n-1}\right),$$

so we get that in equation (3.8) the height of the unknown λ' is bounded by a constant times $X^{1-\delta}$. Further, by assumption β has degree at least 3 over $\mathbb{Q}$, thus also the degree of β' is at least 3. For equation (3.8) the assumptions of Lemma 3.1 are fulfilled, and so there exist effectively computable constants c_1, c_2 depending only on n and the regulator of K such that if $0 \leq \delta < c_1$ the inequality $\max\{|Mx_0|, |d|\} < B_0^{c_2 1/\delta \log(1/\delta)}$ holds, which implies

$$|x_i| < B \quad \text{for } i = 0, \ldots, n-1,$$

where B is an effectively computable constant depending only on n, m, δ, the regulator of K, and on the height of α. □

Proof of Theorem 2.2. The assumptions of Theorem 2.1 are fulfilled with any δ. Further, (3.7) holds with $\lambda = 0$, and we have

$$N_{K/\mathbb{Q}}\left(\frac{\alpha^n - 1}{\alpha - 1}\right) N_{K/\mathbb{Q}}(x_0 + \beta d) = m, \tag{3.10}$$

where $\beta := \frac{n\alpha^n}{\alpha^n - 1} - \frac{\alpha}{\alpha - 1}$.

If $\deg \beta \geq 3$ by Theorem 2.2 there are only finitely many solutions. Further, if β is an imaginary quadratic number, then the finiteness of the number of solutions follows trivially. So there are two more cases, to be considered.

First, if β is a real quadratic number, then we have exactly case (ii) of Theorem 2.2.

Second, if β is a rational number, then there are $a, b \in \mathbb{Z}$ with $\gcd(a, b) = 1$, such that $\beta = \frac{a}{b}$. Then we have

$$\frac{n\alpha^n}{\alpha^n - 1} - \frac{\alpha}{\alpha - 1} = \frac{a}{b}$$

and thus

$$\left(n - \frac{a}{b} - 1\right)\alpha^n - \alpha^{n-1} - \cdots - \alpha + \frac{a}{b} = 0$$

which leeds to

$$(nb - a - b)\alpha^n - b\alpha^{n-1} - \cdots - b\alpha + a = 0. \tag{3.11}$$

Since α is an algebraic integer of degree n, we have $nb - a - b \mid a$ and $nb - a - b \mid b$. However, since $\gcd(a, b) = 1$, we get $nb - a - b = \pm 1$. Now

equation (3.11) leads to

$$\pm\alpha^n - b\alpha^{n-1} - \cdots - b\alpha + nb - b \mp 1 = 0.$$

By changing b to $-b$ if necessary, this means that the minimal polynomial of α is of the form

$$x^n - bx^{n-1} - \cdots - bx + (bn - b - 1)$$

with $b \in \mathbb{Z}$, and this means that we are in case (i) of Theorem 2.2. This concludes the proof of Theorem 2.2. □

Proof of Corollary 2.1. Suppose that (i) of Theorem 2.2 holds, i.e.

$$\alpha^n - b\alpha^{n-1} - \cdots - b\alpha + nb - b - 1 = 0,$$

and put $a := nb - b - 1$. Then clearly $\gcd(a, b) = 1$, and

$$(nb - a - b)\alpha^n - b \cdot \frac{\alpha^n - \alpha}{\alpha - 1} + a = 0,$$

so we have

$$(n - \frac{a}{b} - 1)\alpha^n - \frac{\alpha^n - \alpha}{\alpha - 1} + \frac{a}{b} = 0,$$

which implies

$$n\alpha^n - \frac{\alpha(\alpha^n - 1)}{\alpha - 1} = (\alpha^n - 1)\frac{a}{b}.$$

Thus we have

$$\frac{n\alpha^n}{\alpha^n - 1} - \frac{\alpha}{\alpha - 1} = \frac{a}{b} \in \mathbb{Q},$$

which means that equation (3.10) takes the form

$$N_{K/\mathbb{Q}}\left(\frac{\alpha^n - 1}{\alpha - 1}\right)(x_0 + \frac{a}{b}d)^n = m. \tag{3.12}$$

Now put $m := m_0^n \cdot N_{K/\mathbb{Q}}(\frac{\alpha^n - 1}{\alpha - 1})$. Clearly, there are infinitely many $m_0 \in \mathbb{Z}$ such that $m \in \mathbb{Z}$, and in each such case (3.12) is equivalent to

$$x_0 + \frac{a}{b}d = m_0.$$

Multiplying by b this leads to the linear diophantine equation

$$bx_0 + ad = bm_0,$$

which has infinitely many solutions in $x_0, d \in \mathbb{Z}$. □

Proof of Corollary 2.2. The situation is similar to that of Corollary 2.1. More precisely, if β is a real quadratic number, then (3.10) leads to a Pellian equation, so we can choose m from an infinite set such that (3.10) has infinitely many solutions. □

4. Proof of Theorem 2.3

Lemma 4.1. *If $n \geq 3$ is an odd integer, then the pairs $(1,0)$, $(-1,0)$, $(1,1)$ and $(-1,-1)$, and if $n \geq 3$ is an even integer then the pairs $(1,0)$, $(-1,0)$, $(1,1)$, $(-1,-1)$, $(-1,1)$ and $(1,-1)$ are the only solutions of the equation*

$$X^n - 2Y^n = \pm 1 \quad X, Y \in \mathbb{Z}. \tag{4.13}$$

Proof of Lemma 4.1. Note that $(1,1)$ is a solution of (4.13) for any $n \geq 3$. By Theorem 1.1 of Bennett [1] equation (4.13) has at most 1 solution in positive integers X, Y. In the case when n is odd, there are no solutions X, Y with different signs. Thus any solution of equation (4.13) which is distinct from those listed in Lemma 4.1 would induce a solution of (4.13) with X, Y positive and $(X, Y) \neq (1,1)$, but this is indeed impossible by Bennett's Theorem. □

Lemma 4.2. *The pairs $(-1,1)$ and $(1,-1)$ are the only solutions of the equation*

$$X^n - 3Y^n = \pm 4 \quad X, Y \in \mathbb{Z}$$

where $n \geq 3$ is an odd integer. For even integers $n \geq 3$ the above equation has no solutions.

Proof of Lemma 4.2. For $n = 3$ and $n = 4$ the result can be checked easily using the computer algebra package Magma. For $n \geq 5$ this is a simple consequence of Theorem 1.5 of [2]. □

If the minimal polynomial of α is $x^n - a$, then equation (2.4) via (3.6) can be transformed to the form

$$N_{K/\mathbb{Q}}\left(\frac{1}{(\alpha-1)^2}\right) \cdot N_{K/\mathbb{Q}}\left(x_0(a-1)(\alpha-1) + d(an(\alpha-1) - (a-1)\alpha)\right) = \pm 1, \tag{4.14}$$

which can be rewritten as

$$\frac{1}{(a-1)^2}N_{K/\mathbb{Q}}\big((-x_0(a-1)-dan) + \alpha(x_0(a-1)+dan-d(a-1))\big)=\pm 1. \quad (4.15)$$

Using again that the defining polynomial of α is x^n-a, from (4.15) we get

$$\big(-x_0(a-1)-dan\big)^n + (-1)^{n+1}a\big(x_0(a-1)+dan-d(a-1)\big)^n=\pm(a-1)^2. \quad (4.16)$$

Put $X := -x_0(a-1)-dan$ and $Y := -x_0(a-1)-dan+d(a-1)$. So we get the equation

$$X^n - aY^n = \pm(a-1)^2. \quad (4.17)$$

Now consider the case $a=2$. Then by Lemma 4.1 $(X,Y)=(1,0)$, $(-1,0)$, $(1,1)$ and $(-1,-1)$ are the only solutions of (4.17) when n is odd. From this we get $(x_0,d)=(2n-1,-1)$, $(-2n+1,1)$, $(-1,0)$ and $(1,0)$, respectively. This means that the n-tuples $(2n-1,2n-2,\dots,n)$, $(-2n+1,-2n+2,\dots,-n)$, $(-1,-1,\dots,-1)$ and $(1,1,\dots,1)$ are the only solutions of the equation (2.4) which form an arithmetic progression, for each odd $n\in\mathbb{N}$, $(n\geq 3)$.

When n is even, then by Lemma 4.1 equation (4.17) has two more solutions, namely $(X,Y)=(-1,1)$ and $(1,-1)$. In these cases we have $(x_0,d)=(-4n+1,2)$, $(4n-1,-2)$, respectively. This means that in this case the only solutions of the equation (2.4) which form an arithmetic progression, are those listed in the case of odd n, and the n-tuples $(-4n+1,-4n+3,\dots,-2n+1)$ and $(4n-1,4n-3,\dots,2n-1)$. This concludes the proof of (i) of Theorem 2.3.

Now take $a=3$. By Lemma 4.2 equation (4.17) with $a=3$ has no solution for n even. Thus the equation (2.4) has no solutions which form an arithmetic progression for $n\in\mathbb{N}$ even. Further, for each odd $n\in\mathbb{N}$ $(n\geq 3)$ the pairs $(X,Y)=(-1,1)$ and $(1,-1)$ are the only solutions of (4.17). From this we get $(x_0,d)=\big(\frac{-3n+1}{2},1\big)$ and $\big(\frac{3n-1}{2},-1\big)$, respectively. This in turn means that the n-tuples $\big(\frac{-3n+1}{2},\frac{-3n+3}{2},\dots,\frac{-n-1}{2}\big)$, $\big(\frac{3n-1}{2},\frac{3n-3}{2},\dots,\frac{n+1}{2}\big)$ are the only solutions of the equation (2.4) which form an arithmetic progression, for each odd $n\in\mathbb{N}$, $(n\geq 3)$. This concludes the proof of (ii) of Theorem 2.3.

Remark. From the proof of Theorem 2.3 it is clear that equation (1.1) has the only solution $(10, 9, 8, 7, 6, 5, 4)$ the coordinates of which form an arirhmetic progression.

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, V. Vatsal and S. Yazdani, Ternary Diophantine equations of signature $(p, p, 3)$, *Compositio Math.* (2004) (*to appear*).

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

[4] R. K. Guy, Canadian Number Theory Association unsolved problems 1988, in: Number theory (Banff, AB, 1988), *de Gruyter*, *Berlin*, 1990, 193–206.

[5] V. G. Sprindžuk, Representation of numbers by the norm forms with two dominating variables, *J. Number Theory* **6** (1974), 481–486, Collection of articles dedicated to K. Mahler on the occasion of his seventieth birthday.

attila 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: berczesa@math.klte.hu

attila pethő
faculty of informatics
university of debrecen
h-4010 debrecen, p.o. box 12
hungary

E-mail: pethoe@inf.unideb.hu

(Received June 3, 2004; revised August 26, 2004)