On diophantine equations with solutions forming arithmetic progressions

Attila Pethő

(University of Debrecen, Hungary)

based on joint works with Attila Bérczes (Debrecen) and Volker Ziegler (Graz)

Klagenfurt, 19 September, 2005

Let $\alpha_1 = 1, \alpha_2, \ldots, \alpha_m$ be linearly independent algebraic numbers over $\mathbb{Q}$ and put $K := \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$. Let $n := [K : \mathbb{Q}]$. For any $\alpha \in K$, denote by $\alpha^{(i)}$ the conjugates of α. Put

$$l^{(i)}(\mathbf{X}) = X_1 + \alpha_2^{(i)} X_2 + \ldots + \alpha_n^{(i)} X_n$$

for $i = 1, \ldots, n$. There exists a non-zero $a_0 \in \mathbb{Z}$ such that the form

$$F(\mathbf{X}) := a_0 N_{K/\mathbb{Q}}(\alpha_1 X_1 + \ldots + \alpha_m X_m) = a_0 \prod_{i=1}^{n} l^{(i)}(\mathbf{X})$$

has integer coefficients. Such a form is called a **norm form**.

The equation

$$a_0 N_{K/\mathbb{Q}}(\alpha_1 x_1 + \ldots + \alpha_m x_m) = b \tag{1}$$

in $x_1, \ldots, x_m \in \mathbb{Z}$ is called a **norm form equation**.

If the $\mathbb{Q}$ vector space spanned by $\alpha_1, \ldots, \alpha_m$ has a subspace, which is proportional to a full $\mathbb{Z}$-module of an algebraic number field, different from $\mathbb{Q}$ and the imaginary quadratic field, then $\alpha_1\mathbb{Z} + \ldots + \alpha_m\mathbb{Z}$ is called degenerate.
In that case it is easy to see, that (2) can have infinitely many solutions.
For non-degenerate norm form equations **W.M. Schmidt** (1971) proved that the number of their solutions is finite. This result is ineffective.
For a large class of norm form equations **K. Győry and Z.Z. Papp** (1978): finiteness + explicit upper bounds.

Motivation

Buchmann and Pethő found twenty years ago, as a byproduct of a search for independent units 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

$$N_{K/\mathbb{Q}}(x_0 + x_1\alpha + \ldots + x_6\alpha^6) = 1 \qquad (2)$$

has a solution $(x_0, \ldots, x_6) \in \mathbb{Z}^7$ such that the coordinates form an arithmetic progression.

Our goals: Generalize (2) in three directions, and investigate those solutions which form an arithmetic progression:

- we consider arbitrary number fields

- the integer on the right hand side of equation (2) is not restricted to 1

- it is allowed that the solutions form only nearly an arithmetic progression

- compare with related results.

Theoretical results

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

$$N_{K/\mathbb{Q}}(x_0 + x_1\alpha + x_2\alpha^2 + \ldots + x_{n-1}\alpha^{n-1}) = m. \tag{3}$$

Let $X = \max\{|x_0|, \ldots, |x_{n-1}|\}$. We say that the sequence $\{x_0, \ldots, x_{n-1}\}$ forms nearly an arithmetic progression if there exists $d \in \mathbb{Z}$ and $0 < \delta \in \mathbb{R}$ such that

$$|(x_i - x_{i-1}) - d| \leq X^{1-\delta}, \quad i = 1, \ldots, n-1. \tag{4}$$

Theorem 1. [Bérczes, Pethő (2004)] Let α be an algebraic integer of degree $n \geq 3$ and put $K := \mathbb{Q}(\alpha)$. Suppose that

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

is an algebraic number 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 $0 \leq \delta < c_1$ and any solution of equation (3) with the property (4) we have

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

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 proved a nearly complete finiteness result.

Theorem 2. [Bérczes, Pethő (2004)] Let α be an algebraic integer of degree $n \geq 3$ over $\mathbb{Q}$ and put $K := \mathbb{Q}(\alpha)$. Equation (3) 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 non of the following two cases hold

(i) α has minimal polynomial of the form

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

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

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

Remark. 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.

Problem 1. Does there exist infinitely many exceptions?

Theorem 3. [Bérczes, Pethő (2004)] For any $n \in \mathbf{N}$ $(n \geq 3)$ there exists an algebraic integer α of degree n over $\mathbb{Q}$ such that the equation

$$N_{K/\mathbb{Q}}(x_0 + x_1\alpha + x_2\alpha^2 + \ldots + x_{n-1}\alpha^{n-1}) = \pm 1, \qquad (5)$$

where $K := \mathbb{Q}(\alpha)$, has a solution $(x_0, \ldots, x_{n-1}) \in \mathbb{Z}^n$ having coordinates which are consecutive terms in an arithmetic progression.

More precisely, the following statements are true:

(i) If $\alpha^n = 2, n \geq 3$, then for odd $n \in \mathbf{N}$ the n-tuples $(2n-1, 2n-2, \ldots, n)$, $(-2n+1, -2n+2, \ldots, -n)$, $(-1, -1, \ldots, -1)$ and $(1, 1, \ldots, 1)$;
for even $n \in \mathbf{N}$ the n-tuples $(2n-1, 2n-2, \ldots, n)$, $(-2n+1, -2n+2, \ldots, -n)$, $(-1, -1, \ldots, -1)$, $(1, 1, \ldots, 1)$, $(-4n+1, -4n+3, \ldots, -2n+1)$ and $(4n-1, 4n-3, \ldots, 2n-1)$
are the only solutions of equation (5) which form an arithmetic progression.

(ii) If $\alpha^n = 3, n \geq 3$, then for each odd $n \in \mathbf{N}$ the n-tuples $(\frac{-3n+1}{2}, \frac{-3n+3}{2}, \ldots, \frac{-n-1}{2})$, $(\frac{3n-1}{2}, \frac{3n-3}{2}, \ldots, \frac{n+1}{2})$ are the only solutions of equation (5) which form an arithmetic progression, and for even $n \in \mathbf{N}$ there are no such solutions at all.

On the proof of Theorem 1

Put $c_i := (x_i - x_{i-1}) - d$. Then equation (3) can be written in the form

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

where $\mu = c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1}$. It can be transformed to

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

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

Lemma 1. [Sprindžuk, 1974] 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

$$N_{K/\mathbb{Q}}(x + \beta' y + \lambda') = m \tag{6}$$

in $x, y \in \mathbb{Z}$ and $\lambda' \in \mathbb{Z}_K$ with $|\overline{\lambda'}| < \max\{|x|, |y|\}^{1-\delta}, 0 < \delta < 1$. 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 (6) 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'.

On the proof of Theorem 3

If the minimal polynomial of α is $x^n - a$, then equation (5) can be transformed to the form

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

which can be rewritten as

$$(-x_0(a-1)-dan)^n+(-1)^{n+1}a\left(x_0(a-1)+dan-d(a-1)\right)^n=\pm(a-1)^2.$$

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

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

The following two lemmas complete the proof of Theorem 3.

Lemma 2. [Bennett; 2001] 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

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

Lemma 3. [Bennett, Vatsal, Yazdani; 2004] The pairs $(-1, 1)$ and $(1, -1)$ are the only solutions of the equation

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

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

Computational experiences

Theorem 4. [Bérczes, Pethő (200?)] Let α be a root of the irreducible polynomial $x^n - a \in \mathbb{Z}[x]$, and put $K := \mathbb{Q}(\alpha)$. The equation

$$N_{K/\mathbb{Q}}(x_0 + x_1\alpha + x_2\alpha^2 + \ldots + x_{n-1}\alpha^{n-1}) = 1 \tag{7}$$

has no solutions in integers $x_0, \ldots, x_{n-1}$ which are consecutive elements of an arithmetic progression, if $4 \leq a \leq 100$ (with the possible exception $a = 93$ and $n = 31, 31^2$).

To prove this result, similarly to the proof of Theorem 3, we transform our equation (7) to

$$X^n - aY^n = (a-1)^2 \tag{8}$$

with $X := -x_0(a-1) - dan$ and $Y := -x_0(a-1) - dan + d(a-1)$.

Now we try to completely solve equation (8) for $4 \leq a \leq 100$. Clearly, it is enough to consider the cases where n is an odd prime, or 4.

Lemma 1 *The only solutions of equation (8) for $4 \leq a \leq 100$, if $a \neq 93$ or if $a = 93$ and $n \neq 31, 31^2$, are those listed in the following Table.*

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	$(1, -4)$

n	a	(X,Y)
3	73	$(8,-4)$
3	74	$(47,11)$
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	$(1,-2)$

The method contains the following ingredients:

- Baker's method, for bounding n in terms of a (Bakery)
- Finding contradictions $\pmod{p}$
- Solving the remaining equations via MAGMA, where possible
- Using theory of modular forms

Shanks' simplest cubic field:

What happens if we are choosing another parametrized family of fields, e.g. Shanks' simplest cubic.
Let $f_a = x^3 - (a-1)x^2 - (a+2)x - 1$ and denote by α one of its zeroes.

Theorem 5. [Bérczes, Pethő, Ziegler, (200?)] The only solution to

$$|N_{\mathbb{k}/\mathbb{Q}}(x_0 + x_1\alpha + x_2\alpha^2)| \leq |2a + 1|$$

such that $x_0 < x_1 < x_2$ is an arithmetic progression are
$(x_0, x_1, x_2) = \pm(-2j, -j, 0), (-j, 0, j), (0, j, 2j); |j| \leq |2a + 1|$
except when

$a = 1, (x_0, x_1, x_2) = \pm(-7, -2, 3), (-3, -1, 1), (-1, 3, 7)$

$a = 2, (x_0, x_1, x_2) = \pm(-97, -35, 27), (-36, -13, 10), (-27, -10, 7),$

$(-19, -7, 5), (-1, 2, 5), (-4, 5, 14), (-7, 9, 25), (-9, 13, 35), (-25, 36, 97)$

$a = 4, (x_0, x_1, x_2) = \pm(-7, -2, 3), (-3, -1, 1), (-1, 3, 7)$

$a = 7, (x_0, x_1, x_2) = \pm(-5, -1, 3)$

$a = 16, (x_0, x_1, x_2) = \pm(-28, -3, 22)$

Putting $x_0 = X - Y, x_1 = X, x_2 = X + Y$ we obtain

$$|N_{\mathbb{k}/\mathbb{Q}}(\beta)| \leq |2a + 1|, \quad \beta = (1 + \alpha + \alpha^2)X - (1 - \alpha^2)Y.$$

By Lemmermeyer and Pethő (1995) β is associated to 1 or one of the conjugates of $\alpha - 1$.

We need an independent system of units with maximal rank and its index in the group of units of $\mathbb{Z}[\alpha]$! By E. Thomas (1979) any two different conjugates of α form such a system.

The rest is then a careful analysis of linear form in logarithms of algebraic numbers and formal numerical analysis of the appearing numbers.

Related results on elliptic curves:

Let $E/\mathbb{Q}$ be an elliptic curve. An arithmetic progression on E is a sequence of at least three points $P_1, \ldots, P_s \in E(\mathbb{Q})$ whose x-coordinate form an arithmetic progression (A. Bremner, 1999). To find three-by-three magic squares whose entries are perfect squares is related to arithmetic progression on E. He proved that there exist infinitely many elliptic curves over $\mathbb{Q}$ such that each of them admits an arithmetic progression of length 8.

Allowing quartic models of elliptic curves G. Campbell (2003) found examples on which are lying 9 points in arithmetic progression.

Let $P_t(x) = (x^2 - 9x - 4t)\prod_{i=0}^{9}(x - i)$, where $t \in \mathbb{Q} \setminus \{\pm 1, \pm 2, \pm 4, -5, -6, -8, -11\}$. By U. Maciej (2005) there exist polynomials $Q_t(x), F_t(x)$ with rational coefficients such that $F_t(x)$ of degree 4 and with $P_t(x) = Q_t(x)^2 - F_t(x)$. This implies that on the elliptic curves $y^2 = F_t(x)$ there are lying 10 points whose x coordinate form an arithmetic progression.

Starting from a polynomial of degree 4, whose coefficients depend on 5 parameters, than specializing the parameters appropriately there is constructed infinitely many quartic elliptic curves containing 12 points in arithmetic progression.

Problem 2. Does there exist an absolute bound on the length of arithmetic progressions lying on an elliptic curve? An upper bound depending on the rank of the curve, assuming it is given in Weierstrass normal form exists by a result of J. Silverman.

Problem 3. What about, if we are interested in the solutions of norm form equations? More precisely, consider the solutions $(x_0, \ldots, x_{n-1})$ of

$$N_{K/\mathbb{Q}}(x_0 + x_1\alpha + x_2\alpha^2 + \ldots + x_{n-1}\alpha^{n-1}) = m. \tag{9}$$

Give an upper bound on its solutions such that the x_0 coordinates form an arithmetic progression. Using the theory of S-unit equations such an upper bound can be proved, which depends on the parameters of the equation, but does there exists a bound, which depends only on the degree of the field. For example **does there exist Pell equations, which have arbitrary long arithmetic solutions?**