On norm form equations with solutions forming arithmetic progressions

Attila Pethő
(University of Debrecen, Hungary)

based on joint works with Attila Bérczes

Luminy, 19 May, 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

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

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

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.

Results

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

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

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

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

Theorem 1. Let α be an algebraic integer of degree $n \geq 3$ over $\mathbb{Q}$ 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. 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. **Does there exist infinitely many exceptions?**

Theorem 3. 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'.

Note. This result is proved originally with the assumption $K = \mathbb{Q}(\beta')$, but analyzing the proof it is clear that it works in our case, too.

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

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

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. 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 $n = 2^u 31^v, u = 0, 1, v \in \mathbb{Z}_+$.

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* $n \neq 2^u 31^v$ $(u = 0, 1, v \in \mathbb{Z}_+)$*, 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

Lemma 4. (Pintér, 2004) Let

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

be a binary form of degree $n \geq 3$, with positive integer cofficients 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

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

The local method:

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

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

only in a “few” cases. Programmed in MAGMA, this method works very efficiently.

Lemma 5. (Bennett, 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 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 $N := \mathrm{Rad}_2(AB)\mathrm{Rad}_2(C)^2 \varepsilon_2$, 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

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

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

Lemma 6. (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 and $(n, ABC) = 1$. Then for f, N as in Lemma 5 we have

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

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

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

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