ARITHMETIC PROGRESSIONS IN THE SOLUTION SETS OF NORM FORM EQUATIONS

ATTILA BÉRCZES, LAJOS HAJDU, AND ATTILA PETHŐ

1. Introduction

Let K be an algebraic number field of degree k, and let $\alpha_1, \ldots, \alpha_n$ be linearly independent elements of K over $\mathbb{Q}$. Denote by $D \in \mathbb{Z}$ the common denominator of $\alpha_1, \ldots, \alpha_n$ and put $\beta_i = D\alpha_i$ $(i = 1, \ldots, n)$. Note that $\beta_1, \ldots, \beta_n$ are algebraic integers of K. Let m be a non-zero integer and consider the norm form equation

$$N_{K/\mathbb{Q}}(x_1\alpha_1 + \ldots + x_n\alpha_n) = m \tag{1.1}$$

in integers $x_1, \ldots, x_n$. Let H denote the solution set of (1.1) and $|H|$ the size of H. Note that if the $\mathbb{Z}$-module generated by $\alpha_1, \ldots, \alpha_n$ contains a submodule, which is a full module in a subfield of $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ different from the imaginary quadratic fields and $\mathbb{Q}$, then this equation can have infinitely many solutions (see e.g. Schmidt [19]). Various arithmetical properties of the elements of H were studied in [11] and [8]. In the present paper we are concerned with arithmetical progressions in H. Arranging the elements of H in an $|H| \times n$ array $\mathcal{H}$, one may ask at least two natural questions about arithmetical progressions appearing in H. The "horizontal" one: do there exist infinitely many rows of $\mathcal{H}$, which form arithmetic progressions; and the "vertical" one: do there exist arbitrary long arithmetic progressions in some column of $\mathcal{H}$? Note that the first question is meaningful only if $n > 2$.

The "horizontal" problem was treated by Bérczes and Pethő [4] by proving that if $\alpha_i = \alpha^{i-1}$ $(i = 1, \ldots, n)$ then in general $\mathcal{H}$ contains only finitely many

2000 Mathematics Subject Classification: 11D57, 11D45, 11B25.

Keywords and Phrases: norm form equations, arithmetic progressions.

The research was supported in part by grants T48791 and T67580 of the Hungarian National Foundation for Scientific Research, the János Bolyai Research Fellowship of the Hungarian Academy of Sciences, and by the National Office for Research and Technology.

effectively computable "horizontal" AP's and they were able to localize the possible exceptional cases. Later Bérczes and Pethő [5], Bérczes Pethő and Ziegler [6] and Bazsó [2] computed all horizontal AP's in the solution sets of norm form equations corresponding to the fields generated by the polynomials $x^n - a, 2 \leq a \leq 100$, $x^3 - (a-1)x^2 - (a+2)x - 1, a \in \mathbb{Z}$ and $x^n + a, 2 \leq a \leq 100$, respectively.

For quadratic norm form equations, which are called Pell equations if K is a real quadratic field, only the "vertical" problem is interesting. In this direction Pethő and Ziegler [18] proved among others that the length of the "vertical" AP's in $\mathcal{H}$ is bounded by a constant, which depends on the coefficients of the (quadratic) form and on m. On the other hand, they proved that every three term AP occurs in the second column of infinitely many $\mathcal{H}$. Dujella, Pethő and Tadić [7] was able to extend this result to four term AP's.

The main goal of the present paper is to generalize the result of Pethő and Ziegler [18] to arbitrary norm form equations. In the sequel *AP in H* always means a "vertical" arithmetical progression belonging to $\mathcal{H}$. A sequence in H, with the property that all the corresponding coordinate sequences form "vertical" AP's, will be called an *algebraic AP in H*.

2. Results

Now we summarize our main results.

Theorem 2.1. *Let* $(x_1^{(j)}, \ldots, x_n^{(j)})$ $(j = 1, \ldots, t)$ *be a sequence of distinct elements in* H *such that* $x_i^{(j)}$ *is an arithmetic progression for some* $i \in \{1, \ldots, n\}$. *Then we have* $t \leq c_1$, *where* $c_1 = c_1(k, m, D)$ *is an explicitly computable constant.*

Theorem 2.2. *The set* H *contains at most* c_3 *arithmetic progressions of the form* $\underline{x} + k\underline{d}$ $(k = -1, 0, 1)$. *Here* $c_3 = c_3(k, m, D)$ *is an explicitly computable constant,* $\underline{x} = (x_1, \ldots, x_n)$, d *is a non-zero integer, and* $\underline{d}$ *is the* n*-tuple with all entries equal to* d.

By Theorem 2.1 the length of any AP in H is bounded. In the particular case $k = 2$, H does not contain any algebraic AP (see Pethő and Ziegler [18]). However, it is not possible to give a bound for the number of AP-s in H for $k \geq 3$. It is demonstrated by the following example. Let $P(x) = x(x-1)\dots(x-k+1)+(-1)^k$ and denote by α one of its roots. It was proved in [14] (Lemma 2.2, see also [1, 13] and [17]), that $P(x)$ is irreducible and the conjugates of α are $\alpha+1, \dots, \alpha+k-1$. Thus these k numbers are units of norm 1 in the algebraic number field $\mathbb{Q}(\alpha)$, moreover they form an AP of length k. If μ is an algebraic integer in $\mathbb{Q}(\alpha)$ of norm m then $\mu\alpha, \mu(\alpha+1), \dots, \mu(\alpha+k-1)$ also have norm m, and form an AP of length k.

The next theorem shows that in general if H contains algebraic AP-s at all, then it contains infinitely many.

Theorem 2.3. *Suppose that $n = k \geq 3$. Let $t \geq 3$ be an integer. If H contains a non-constant t-term algebraic AP, then it contains infinitely many.*

Now we prove that the algebraic AP's from the example before Theorem 2.3 are the longest ones. More precisely, we have the following theorem.

Theorem 2.4. *Let K be an algebraic number field of degree k. Assume that $\alpha_1, \dots, \alpha_t \in K$ have the same field norm and form a non-trivial AP. Then $t \leq k$.*

Remark. We note that M. Newman ([16], see also [17]) proved that the length of arithmetic progressions consisting of units of an algebraic number field of degree k is at most k. Theorem 2.4 is a generalization of his result.

To formulate the next result, for a non-zero integer a let $\omega(a)$ denote the number of prime divisors of a, and for a prime p denote by $\mathrm{ord}_p(a)$ the highest exponent u such that p^u divides a.

Theorem 2.5. *Suppose that the Galois group of the normal closure of K is doubly transitive. Then the number of those solutions $(x_1, \dots, x_n)$ of equation (1.1), for which there exists another solution $(y_1, \dots, y_n) \neq (x_1, \dots, x_n)$, such that $\prod_{i=1}^n (x_i - y_i) = 0$, is bounded by*

$$\Psi(k, n, mD^k) \exp\left(k(12n)^{6n}\right)$$

where

$$\Psi(k,n,mD^k) := \binom{k}{n-1}^{\omega(mD^k)} \cdot \prod_{\substack{p\mid m \\ p \text{ prime}}} \binom{\operatorname{ord}_p(mD^k)+n-1}{n-1}.$$

Theorem 2.6. *Let S be a set of s rational primes, and let T be the set of integers without prime divisors outside S. Suppose that the Galois group of the normal closure of K is doubly transitive. Then the number of those solutions $(x_1,\dots,x_n)$ of equation (1.1), for which there exists another solution $(y_1,\dots,y_n) \neq (x_1,\dots,x_n)$, such that $x_i - y_i \in T$ for some $i \in \{1,\dots,n\}$, is bounded by*

$$\Psi(k,n,mD^k) \cdot \exp\left((s+k)(12n)^{6n+3}\right),$$

where Ψ is the function defined in Theorem 2.5.

Remark. By the help of Theorems 2.5 and 2.6 one can easily give a bound for the number of sequences $\mathbf{x}_j = (x_1^{(j)},\dots,x_n^{(j)}) \in H$ such that one of the coordinates of $\mathbf{x}_j$ forms an arithmetic progression whose difference is zero or is an S-unit, respectively.

3. Auxiliary results

In this section we present some lemmas which will be needed in the proofs of our theorems. For this purpose we need to introduce some notation. Let L be a number field of degree l and denote by U_L the unit group of L. The next statement is an immediate consequence of a result of Hajdu [12]. Note that a similar result was independently proved by Jarden and Narkiewicz [15]

Lemma 3.1. *Let n be an integer and let A be a finite subset of L^n. There exists a constant $C_1 = C_1(l,n,|A|)$ such that the length of any non-constant arithmetic progression in the set*

$$\left\{ \sum_{i=1}^{n} a_i y_i : (a_1,\dots,a_n) \in A,\ (y_1,\dots,y_n) \in U_L^n \right\}$$

is at most C_1.

For some other arithmetical properties of the set occurring in Lemma 3.1, see [11].

Let K be a number field of degree k, $\alpha_1, \ldots, \alpha_n$ linearly independent algebraic integers in K, $m \in \mathbb{Z}$, and $\lambda \in K$. Consider now the equation

$$N_{K/\mathbb{Q}}(\alpha_1 x_1 + \cdots + \alpha_n x_n + \lambda) = m \quad \text{in} \quad x_1, \ldots, x_n \in \mathbb{Z}. \tag{3.2}$$

The next lemma is a special case of Corollary 8 of [3].

Lemma 3.2. *Suppose that $\alpha_1, \ldots, \alpha_n$ and λ are linearly independent over $\mathbb{Q}$. Then the number of solutions of equation (3.2) does not exceed the bound*

$$\left(2^{17}k\right)^{\left(\frac{2}{3}(n+1)(n+2)(2n+3)-4\right)(\omega(m)+1)}.$$

Let F be an algebraically closed field of characteristic 0. Write F^* for the multiplicative group of nonzero elements of F, and let $(F^*)^n$ be the direct product consisting of n-tuples $\mathbf{x} = (x_1, \ldots, x_n)$ with $x_i \in F^*$ for $i = 1, \ldots, n$. For $x, y \in (F^*)^n$ write $x * y = (x_1 y_1, \ldots, x_n y_n)$. Let Γ be a subgroup of $(F^*)^n$ and suppose that $(a_1, \ldots, a_n) \in (F^*)^n$. Consider the so-called generalized unit equation

$$a_1 x_1 + \ldots + a_n x_n = 1 \tag{3.3}$$

in $\mathbf{x} = (x_1, \ldots, x_n) \in \Gamma$. A solution $\mathbf{x}$ is called non-degenerate, if no subsum of the left hand side of (3.3) vanishes, that is $\sum_{i \in I} a_i x_i \neq 0$ for any nonempty subset I of $\{1, \ldots, n\}$. The next lemma is Theorem 1.1 of Evertse, Schlickewei and Schmidt [10].

Lemma 3.3. *Suppose that Γ has finite rank r. Then the number of non-degenerate solutions $\mathbf{x} \in \Gamma$ of equation (3.3) is bounded by*

$$\exp\left((6n)^{3n}(r+1)\right).$$

Let $\mathcal{M}$ be the $\mathbb{Z}$-module generated by the elements $\alpha_1, \ldots, \alpha_n$. Clearly, equation (1.1) can be transformed to the equation

$$N_{K/\mathbb{Q}}(\delta) = m \quad \text{in} \quad \delta \in \mathcal{M}. \tag{3.4}$$

Lemma 3.4. *The set of solutions of (3.4) is contained in some union* $\delta_1\mathcal{O}_K^* \cup \cdots \cup \delta_t\mathcal{O}_K^*$, *where*

$$t \le \Psi(k,n,m) = \binom{k}{n-1}^{\omega(m)} \cdot \prod_{\substack{p\mid m\\ p \text{ prime}}} \binom{\mathrm{ord}_p(m)+n-1}{n-1}$$

and $\delta_1,\dots,\delta_t$ *are solutions of (3.4).*

Proof. This is a special case of Lemma 4 of [9]. □

4. Proofs

Proof of Theorem 2.1. Recall that H is the solution set of (1.1), D is the common denominator of $\alpha_1,\dots,\alpha_n$, and $\beta_i = D\alpha_i$ $(i=1,\dots,n)$.

Suppose first that we have a non-constant sequence $(x_1^{(j)},\dots,x_n^{(j)})$ $(j = 1,\dots,t)$ in H such that $x_i^{(j)}$ is constant for some $i \in \{1,\dots,n\}$. Let $\lambda := x_i^{(j)} \cdot \beta_i$. Then equation (1.1) is of the shape (3.2) and by Lemma 3.2 we see that the number of such solutions of (1.1) (i.e. t) is bounded by

$$\left(2^{17}k\right)^{(\frac{2}{3}n(n+1)(2n+1)-4)(\omega(mD^k)+1)} \le c_1(k,m,D).$$

Assume next that $(x_1^{(j)},\dots,x_n^{(j)}) \in H$ for $j=1,\dots,t$ such that $x_i^{(j)}$ forms a non-constant arithmetic progression for some $i \in \{1,\dots,n\}$. Writing $\sigma_1,\dots,\sigma_k$ for the isomorphisms of K into $\mathbb{C}$, for $u = 1,\dots,k$ we have

$$x_1\sigma_u(\beta_1) + \ldots + x_n\sigma_u(\beta_n)\sigma_u(\varepsilon)\sigma_u(\mu)$$

where μ is an element of norm mD^k and ε is a unit in the $\mathbb{Z}$-module $\mathbb{Z}[\beta_1,\dots,\beta_n]$. By Lemma 3.4 μ can be chosen from a set having at most $\Psi(k,n,mD^k)$ elements. Consider a fixed value of μ. Choose the order of the isomorphisms $\sigma_1,\dots,\sigma_k$ such that the matrix

$$B \begin{pmatrix} \sigma_1(\beta_1) & \ldots & \sigma_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \ldots & \sigma_n(\beta_n) \end{pmatrix} \tag{4.5}$$

has non-zero determinant. Hence we have

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = B^{-1} \begin{pmatrix} \sigma_1(\varepsilon)\sigma_1(\mu) \\ \vdots \\ \sigma_n(\varepsilon)\sigma_n(\mu) \end{pmatrix}. \tag{4.6}$$

Writing

$$B^{-1}\begin{pmatrix}\gamma_{11} & \cdots & \gamma_{1n}\\ \vdots & \ddots & \vdots\\ \gamma_{n1} & \cdots & \gamma_{nn}\end{pmatrix} \tag{4.7}$$

we get

$$x_i = a_{i1}y_1 + \ldots + a_{in}y_n$$

for all $i = 1, \ldots, n$, where $a_{ih} = \gamma_{ih}\sigma_h(\mu)$ and $y_h = \sigma_h(\varepsilon)$ for $h = 1, \ldots, n$. Noting that the y_h $(h = 1, \ldots, n)$ are units in the splitting field L of K, and $\deg(L) \le k!$, using $n \le k$ the theorem follows from Lemma 3.1. □

Proof of Theorem 2.2. Obviously, in view of Theorem 2.1 it is sufficient to give an upper bound for the number of three-term progressions in H. For this purpose, assume that $(x_1, \ldots, x_n)$ is the middle term of a three-term arithmetic progression in H, with common difference $d\underline{1}$. Denote by U_K the unit group of the ring of algebraic integers of the field K. Put

$$\mu_{\pm 1} = (x_1 \pm d)\beta_1 + \ldots + (x_n \pm d)\beta_n \text{ and } \mu_0 = x_1\beta_1 + \ldots + x_n\beta_n.$$

Note that $N_{K/\mathbb{Q}}(\mu_{-1}) = N_{K/\mathbb{Q}}(\mu_0) = N_{K/\mathbb{Q}}(\mu_1) = mD^k$, and further that $\mu_h = \varepsilon_h\mu_h^*$ $(h = -1, 0, 1)$ where $\varepsilon_{-1}, \varepsilon_0, \varepsilon_1 \in U_K$ and $\mu_{-1}^*, \mu_0^*, \mu_1^*$ belong to a finite set whose cardinality is bounded in terms of k, m, D. Thus we have

$$\mu_{-1}^*\varepsilon_{-1} - 2\mu_0^*\varepsilon_0 + \mu_1^*\varepsilon_1 = 0.$$

Hence Lemma 3.3 implies that

$$(\varepsilon_{-1}, \varepsilon_0, \varepsilon_1) = \varepsilon(\varepsilon_{-1}^*, \varepsilon_0^*, \varepsilon_1^*)$$

with some $\varepsilon \in U_K$, where $(\varepsilon_{-1}^*, \varepsilon_0^*, \varepsilon_1^*)$ belongs to a finite subset of U_K^3, of cardinality bounded by some constant depending only on k, m, D. Thus we conclude that

$$\mu_h = \varepsilon\lambda_h \quad (h = -1, 0, 1)$$

holds, where $\varepsilon \in U_K$ and $\lambda_{-1}, \lambda_0, \lambda_1$ belong to a finite set of cardinality depending only on k, m, D again. Observe that $d = \varepsilon(\lambda_1 - \lambda_0)$ holds, and further that this d can be rational for at most one choice of $\varepsilon \in U_K$ (up to a factor -1), for any fixed $(\lambda_{-1}, \lambda_0, \lambda_1)$. Hence the theorem follows. □

Proof of Theorem 2.3. Suppose that $(x_1^{(j)},\dots,x_n^{(j)})$ $(j=1,\dots,t)$ is a non-constant algebraic AP in H. Let ε be an arbitrary unit in $\mathbb{Z}[\beta_1,\dots,\beta_n]$ of norm 1, and define $(y_1^{(j)},\dots,y_n^{(j)})$ by

$$y_1^{(j)}\beta_1+\ldots+y_n^{(j)}\beta_n=\varepsilon(x_1^{(j)}\beta_1+\ldots+x_n^{(j)}\beta_n) \text{ for } j=1,\dots,t.$$

Obviously, then $(y_1^{(j)},\dots,y_n^{(j)})$ $(j=1,\dots,t)$ is a non-constant algebraic AP in H. As there are infinitely many units in $\mathbb{Z}[\beta_1,\dots,\beta_n]$ of norm 1, the theorem follows. □

Proof of Theorem 2.4. Denote by m the common norm of $\alpha_1,\dots,\alpha_t$. As these numbers form an AP, we have $\alpha_i=\alpha_1+(i-1)(\alpha_2-\alpha_1), i=1,\dots,t$. This implies $\frac{\alpha_i}{\beta}=\frac{\alpha_1}{\beta}+i-1$ with $\beta=\alpha_2-\alpha_1$. Put M for the norm of β and $P(x)=x^u+p_{u-1}x^{u-1}+\cdots+p_0, p_j\in\mathbb{Q}$ for the minimal polynomial of $\frac{\alpha_1}{\beta}$. It is well known that the defining polynomial of $\frac{\alpha_1}{\beta}$ is a power of its minimal polynomial, i.e. $u|k$ and $p_0^{k/u}=(-1)^k m/M$. If $k=u$ then we even have $p_0=(-1)^k m/M$ otherwise, because both p_0 and m/M are rational numbers, there are at most two possibilities for p_0, which differ from each other only in their sign.

Consider the polynomials $P_i(x)=P(x-(i-1)), i=1,\dots,t$. They are with $P(x)$ irreducible and we have

$$P_i\left(\frac{\alpha_i}{\beta}\right)=P\left(\frac{\alpha_i}{\beta}-(i-1)\right)P\left(\frac{\alpha_1}{\beta}\right)=0,$$

i.e. $\frac{\alpha_i}{\beta}$ is a root of $P_i(x)$, which together with the irreducibility of $P_i(x)$ implies that it is the minimal polynomial of $\frac{\alpha_i}{\beta}$. Thus its constant term is equal to p_0 if $k=u$ and may differ from p_0 only in its sign, otherwise. Hence $P(-i+1), i=1,\dots,t$ is constant if $k=u$ or can assume only at most two different values. If $k=u$ this implies $P(x)=x(x-1)\dots(x-t+1)+p_0$ and we have $t\le k$ as stated. If $u<k$ then there exists a subset $I\subseteq\{1,\dots,t\}$ of size $|I|\ge t/2$ such that $P(-i+1)$ takes the same value for all $i\in I$. By the theory of interpolation the degree of P must be at least $|I|$, i.e. $u\ge|I|\ge t/2$. On the other hand, $u<k$ and $u|k$ imply $u\le k/2$. ¿From the last two inequalities we get $t\le k$ in this case, too. □

Proof of Theorem 2.5. We shall bound the number of those solutions of equation (1.1), for which there exists a solution $(y_1,\dots,y_n)\neq(x_1,\dots,x_n)$

with $x_i = y_i$ for some $i \in \{1, \dots, n\}$. Now equation (1.1) means that

$$\beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n = \mu_1 \varepsilon_1 \tag{4.8}$$

and

$$\beta_1 y_1 + \beta_2 y_2 + \cdots + \beta_n y_n = \mu_2 \varepsilon_2 \tag{4.9}$$

where μ_1, μ_2 are elements of norm mD^k and $\varepsilon_1, \varepsilon_2$ are units in the $\mathbb{Z}$-module generated by $\beta_1, \dots, \beta_n$. By Lemma 3.4 both μ_1 and μ_2 can be chosen from a set having at most $\Psi(k, n, mD^k)$ elements. Consider fixed values of μ_1 and μ_2. Denote again by $\sigma_1, \dots, \sigma_k$ the isomorphic embeddings of K into $\mathbb{C}$, choosing their order such that the matrix B in (4.5) has nonzero determinant. Using (4.7), equation (4.8) leads to equation (4.6). This means that

$$x_i = \sum_{j=1}^{n} \gamma_{ij} \sigma_j(\mu_1) \sigma_j(\varepsilon_1). \tag{4.10}$$

Similarly, using equation (4.9) we can show that

$$y_i = \sum_{j=1}^{n} \gamma_{ij} \sigma_j(\mu_2) \sigma_j(\varepsilon_2). \tag{4.11}$$

One can easily check that $\gamma_{ij} \neq 0$ for at least two indices $j \in \{1, \dots, n\}$. Thus without loss of generality we may assume that $\gamma_{i1}, \dots, \gamma_{iN}$ are nonzero and $\gamma_{i,N+1} = \cdots = \gamma_{in} = 0$, for some $2 \leq N \leq n$. Now subtracting equations (4.10) and (4.11) we get

$$\sum_{j=1}^{N} \left(\gamma_{ij} \sigma_j(\mu_1) \sigma_j(\varepsilon_1) - \gamma_{ij} \sigma_j(\mu_2) \sigma_j(\varepsilon_2) \right) = 0. \tag{4.12}$$

This is a homogeneous unit equation consisting of $2N$ terms. We shall bound the number of solutions of this equation. First we count the non-degenerate solutions of (4.12). Dividing the equation by the last term we obtain

(4.13)
$$\sum_{j=1}^{N-1} \left(\frac{\gamma_{ij} \sigma_j(\mu_1)}{\gamma_{in} \sigma_N(\mu_2)} \frac{\sigma_j(\varepsilon_1)}{\sigma_N(\varepsilon_2)} - \frac{\gamma_{ij} \sigma_j(\mu_2)}{\gamma_{iN} \sigma_N(\mu_2)} \frac{\sigma_j(\varepsilon_2)}{\sigma_N(\varepsilon_2)} \right) + \frac{\sigma_N(\mu_1)}{\sigma_N(\mu_2)} \frac{\sigma_N(\varepsilon_1)}{\sigma_N(\varepsilon_2)} = 1,$$

which is an inhomogeneous unit equation having $2N-1$ terms. We easily see that all solutions to this equation are contained in the subgroup

$$\Gamma=\left\{\left(\frac{\sigma_1(\varepsilon_1)}{\sigma_N(\varepsilon_2)},\frac{\sigma_1(\varepsilon_2)}{\sigma_N(\varepsilon_2)},\frac{\sigma_2(\varepsilon_1)}{\sigma_N(\varepsilon_2)},\frac{\sigma_2(\varepsilon_2)}{\sigma_N(\varepsilon_2)},\dots,\frac{\sigma_N(\varepsilon_1)}{\sigma_N(\varepsilon_2)}\right)\ \mid\ \varepsilon_1,\varepsilon_2\in\mathcal{O}_K^*\right\}$$

of $(\mathbb{C}^*)^{2N-1}$. Clearly, this group has rank at most $2r_K$, where r_K is the unit rank of the field K. Indeed, if $\eta_1,\dots,\eta_{r_K}$ denotes a fundamental system of units in K then, the subgroup Γ_0 of $(\mathbb{C}^*)^{2N-1}$, generated by the vectors

$$\mathbf{a}_j=(\sigma_1(\eta_j),1,\sigma_2(\eta_j),1,\dots,1,\sigma_N(\eta_j))\quad(j=1,\dots,r_K),$$

and

$$\mathbf{b}_i=\left(\frac{1}{\sigma_N(\eta_j)},\frac{\sigma_1(\eta_j)}{\sigma_N(\eta_j)},\frac{1}{\sigma_N(\eta_j)},\frac{\sigma_2(\eta_j)}{\sigma_N(\eta_j)},\dots,\frac{\sigma_{N-1}(\eta_j)}{\sigma_N(\eta_j)},\frac{1}{\sigma_N(\eta_j)}\right)\ (j=1,\dots,r_K)$$

has rank at most $2r_K$. Further, the factor group Γ/Γ_0 is a torsion group. This means that the solutions of equation (4.13) belong to a subgroup of rank at most of $2k-2$ of $(\mathbb{C}^*)^{2N-1}$. Thus, $\frac{\sigma_1(\varepsilon_1)}{\sigma_N(\varepsilon_2)}$ is contained in a set of at most

$$\exp\left((12N-6)^{6N-3}(2k-1)\right)$$

elements. Fix now such a value. Then using that the Galois group of K is doubly transitive, we see that $\frac{\sigma_l(\varepsilon_1)}{\sigma_j(\varepsilon_2)}$ is also fixed for each $j,l\in\{1,\dots,k\}$. By multiplying the ratios $\frac{\sigma_1(\varepsilon_1)}{\sigma_j(\varepsilon_2)}$ for $j\in\{1,\dots,k\}$ and using that $\prod_{j=1}^k\sigma_j(\varepsilon_2)=\pm1$ we get that ε_1 may assume at most $2k$ values. Similarly, ε_2 may assume at most $2k$ values. These altogether show that the number of non-degenerate solutions of equation (4.12) is bounded by

$$\exp\left((12N-6)^{6N-2}(4k-2)\right). \tag{4.14}$$

Now we have to estimate the number of degenerate solutions of (4.12), too. If $\gamma_{ij}\sigma_j(\mu_1)\sigma_j(\varepsilon_1)-\gamma_{ij}\sigma_j(\mu_2)\sigma_j(\varepsilon_2)=0$ for all $j\in\{1,\dots,N\}$ then we get that $\sigma_l(\mu_1)\sigma_l(\varepsilon_1)\sigma_l(\mu_2)\sigma_l(\varepsilon_2)$ for some $l\in\{1,\dots,N\}$ and thus $\mu_1\varepsilon_1=\mu_2\varepsilon_2$. Now subtracting equations (4.8) and (4.9) and using that $\beta_1,\dots,\beta_n$ are linearly independent, we get that $x_j=y_j$ for all $j\in\{1,\dots,n\}$, which is a contradiction. Thus we must have one of the following two cases:

(i) Equation (4.12) has a minimal vanishing sub-sum (i.e. a sub-sum with no further vanishing sub-sums) which contains both $\sigma_j(\varepsilon_1)$ and $\sigma_l(\varepsilon_2)$ for some $j\neq l$, $j,l\in\{1,\dots,N\}$. Similarly to the case of the non-degenerate solutions we can prove that the number of solutions of (4.12) is bounded by the expression in (4.14).

(ii) Equation (4.12) has both a minimal vanishing sub-sum which contains $\sigma_j(\varepsilon_1)$ and $\sigma_l(\varepsilon_1)$ for some $j \neq l$, $j, l \in \{1, \ldots, N\}$, and a minimal vanishing sub-sum which contains $\sigma_u(\varepsilon_2)$ and $\sigma_v(\varepsilon_2)$ for some $u \neq v$, $u, v \in \{1, \ldots, N\}$. Further, these vanishing sub-sums contain at most N terms. Thus we infer again a much better bound than the bound (4.14) on the number of solutions in this case.

Finally, we have 2^{2N-1} possibilities for choosing the considered sub-sums, so altogether the number of solutions $(\varepsilon_1, \varepsilon_2)$ of equation (4.12) is bounded by

$$\exp\left((12N-6)^{6N-1}(4k-2)\right). \tag{4.15}$$

Thus (using that $N \leq n$) the number of those solutions of equation (1.1), for which there exists a solution $(y_1, \ldots, y_n) \neq (x_1, \ldots, x_n)$ with $x_i = y_i$, is bounded by

$$\Psi(k, n, mD^k) \exp\left((12n-6)^{6n-1}(4k-2)\right).$$

Thus the number of those solutions $(x_1, \ldots, x_n)$ of equation (1.1), for which there exists another solution $(y_1, \ldots, y_n) \neq (x_1, \ldots, x_n)$, such that $\prod_{i=1}^n (x_i - y_i) = 0$ is bounded by

$$n\Psi(k, n, mD^k) \exp\left((12n-6)^{6n-1}(4k-2)\right) \leq \Psi(k, n, mD^k) \exp\left(k(12n)^{6n}\right).$$

□

Proof of Theorem 2.6. We start the proof of the present theorem exactly in the same way as the proof of Theorem 2.5. The first difference is that instead of equation (4.12) we get

$$\sum_{j=1}^{N} \left(\gamma_{ij}\sigma_j(\mu_1)\sigma_j(\varepsilon_1) - \gamma_{ij}\sigma_j(\mu_2)\sigma_j(\varepsilon_2)\right) = d \in T. \tag{4.16}$$

Now divide this equation by d to get an inhomogeneous S-unit equation having $2N$ terms. Using Lemma 3.3 we can bound (similarly to the proof of Theorem 2.5) the possibilities for either the values of $\frac{\sigma_u(\varepsilon_1)}{d}$, or the values of

$\frac{\sigma_u(\varepsilon_2)}{d}$ for some u, depending on the vanishing subsums in the unit equation. This bound is given by

$$\exp\left((12N)^{6N}(s+2k-1)\right). \tag{4.17}$$

Since $d \in \mathbb{Z}$ and $\sigma_u(\varepsilon_1)$ is a unit, thus if $\frac{\sigma_u(\varepsilon_1)}{d}$ is fixed, then d may assume at most two values and by fixing one of those, $\sigma_u(\varepsilon_1)$ becomes also fixed. Then we can fix ε_2, too. A similar argument works also when first we are able to fix $\frac{\sigma_u(\varepsilon_2)}{d}$. Thus for the number of solutions of equation (1.1), for which there exists another solution $(y_1, \dots, y_n) \neq (x_1, \dots, x_n)$, such that $x_i - y_i \in T$ for some $i \in \{1, \dots, n\}$, is bounded by

$$\Psi(k, n, mD^k) \exp\left((s+k)(12n)^{6n+3}\right).$$

□

Acknowledgement. The research was supported in part by the National Office for Research and Technology. The authors are grateful to the referee for his useful and helpful remarks.

References

[1] N.C. Ankeny, R. Brauer and S. Chowla, *A note on the class-numbers of algebraic number fields*, Amer J. Math. **78** (1956), 51–61.

[2] A. Bazsó, *Further Computational Experiences on Norm Form Equations with Solutions Forming Arithmetic Progressions*, Publ. Math. Debrecen, **71** (2007), 489–497.

[3] A. Bérczes and K. Győry, *On the number of solutions of decomposable polynomial equations*, Acta Arith. **101** (2002), 171–187.

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

[5] A. Bérczes and A. Pethő, *Computational experiences on norm form equations with solutions forming arithmetic progressions*, Glasnik Math., **41** (2006), 1–8.

[6] A. Bérczes, A. Pethő and V. Ziegler, *Parameterized Norm Form Equations with Arithmetic progressions*, J. Symbolic Comput. **41** (2006), 790–810.

[7] A. Dujella, A. Pethő and P. Tadić, *On arithmetic progressions on Pellian equations*, Acta Math. Hungar., to appear.

[8] G. Everest and K. Győry, *On some arithmetical properties of solutions of decomposable form equations*, Math. Proc. Cambridge Philos. Soc. **139** (2005), 27–40.

[9] J.-H. Evertse and K. Győry, *The number of families of solutions of decomposable form equations*, Acta Arith. **80** (1997), 367–394.

[10] J.-H. Evertse, H. P. Schlickewei and W. M. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. of Math. (2), **155** (2002), 807–836.

[11] K. Győry, M. Mignotte and T. N. Shorey, *On some arithmetical properties of weighted sums of S-units*, Math. Pannon. **1** (1990), 25–43.

[12] L. Hajdu, *Arithmetic Progressions in Linear Combinations of S-units*, Periodica Math. Hungar. **54** (2007), 175-181.

[13] F. Halter-Koch, *Unabhängige Einheitensysteme für eine allgemeine Klasse algebraischer Zahlkörper*, Abh. Math. Sem. Univ. Hamburg **43** (1975), 85–91.

[14] F. Halter-Koch, G. Lettl, A. Pethő and R. Tichy, *Thue equations associated with Ankeny-Brauer-Chowla number fields*, J. London Math. Soc. **60** (1999), 1–20.

[15] M. Jarden and W. Narkiewicz, *On sums of units*, Monatsh. Math. **150** (2007), 327–332.

[16] M. Newman, *Units in arithmetic progression in an algebraic number field,* Proc. Amer. Math. Soc., **43** (1974), 266–268.

[17] M. Newman, *Consecutive units*, Proc. Amer. Math. Soc., **108** (1990), 303–306.

[18] A. Pethő and V. Ziegler, *Arithmetic progressions on Pell equations*, J. Number Theory, to appear.

[19] W.M. Schmidt, *Norm form equations*, Ann. of Math., **96** (1972), 526–551.

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

L. Hajdu
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: hajdul@math.klte.hu

A. Pethő
Faculty of Informatics, 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: pethoe@inf.unideb.hu