J. Korean Math. Soc. **41** (2004), No. 4, pp. 717–735

A CLASS OF EXPONENTIAL CONGRUENCES IN SEVERAL VARIABLES

Geumlan Choi and Alexandru Zaharescu

Abstract. A problem raised by Selfridge and solved by Pomerance asks to find the pairs (a, b) of natural numbers for which $2^a - 2^b$ divides $n^a - n^b$ for all integers n. Vajaitu and one of the authors have obtained a generalization which concerns elements $\alpha_1, \ldots, \alpha_k$ and β in the ring of integers $\mathbf{A}$ of a number field for which

$$\sum_{i=1}^{k} \alpha_i \beta^{a_i} \quad \text{divides} \quad \sum_{i=1}^{k} \alpha_i z^{a_i} \text{ for any } z \in \mathbf{A}.$$

Here we obtain a further generalization, proving the corresponding finiteness results in a multidimensional setting.

1. Introduction

A problem raised by Selfridge (see Guy [1], problem B47) asks to find the pairs (a, b) of natural numbers for which $2^a - 2^b$ divides $n^a - n^b$ for all integers n. By using results of Schinzel [4] and Velez [6], Pomerance [2] solved Selfridge's problem. It turns out that there are exactly 14 pairs (a, b), with $a > b$, which satisfy the above property. The problem was also solved by Sun Qi and Zhang Ming Zhi in [5]. A more general question has been investigated in [7]. Let K be a number field and let $\mathbf{A}$ be its ring of integers. Choose nonzero elements $\alpha_1, \ldots, \alpha_k$ and β in $\mathbf{A}$, β not a unit, and consider the set of k-tuples $(a_1, \ldots, a_k)$ of natural numbers for which

$$(1.1) \qquad \sum_{i=1}^{k} \alpha_i \beta^{a_i} \quad \text{divides} \quad \sum_{i=1}^{k} \alpha_i z^{a_i} \text{ for any } z \in \mathbf{A}.$$

In order to avoid certain degenerate situations, when one does have infinitely many solutions, in [7] only those k-tuples $(a_1, \ldots, a_k)$ have

Received April 4, 2003.

2000 Mathematics Subject Classification: 11A07.

Key words and phrases: exponential congruences, algebraic integers, polynomials of several variables.

been considered for which

$$\sum_{i\in S}\alpha_i\beta^{a_i}\neq 0, \tag{1.2}$$

for any non empty subset S of $\{1,2,\dots,k\}$. Then it was shown in [7] that there are only finitely many k-tuples $(a_1,\dots,a_k)$ satisfying both conditions (1.1) and (1.2) above. In case where $K=\mathbb{Q}$ or K is an imaginary quadratic field one can strengthen the conclusion of the above result. More precisely, it is shown in [7] that for such fields K, given nonzero elements $\alpha_1,\dots,\alpha_k\in\mathbf{A}$ there are only finitely many elements β in $\mathbf{A}$ for which there exist natural numbers $a_1,\dots,a_k$, not all zero, satisfying relations (1.1) and (1.2) above.

In the present paper we study a multidimensional version of the problem. For example, in the two dimensional case, one may ask for which natural numbers a, b, c, d, with $a>b$ and $c>d$,

$$(2^a-2^b)(2^c-2^d) \quad \text{divides} \quad (n^a-n^b)(m^c-m^d) \text{ for any } n,m\in\mathbb{Z}. \tag{1.3}$$

Here if we set $m=2$, we see that (a,b) has to be a solution to the original problem of Selfridge. Similarly, by letting $n=2$ we find that (c,d) also has to be a solution of that problem. On the other hand, if both (a,b) and (c,d) are solutions to the problem of Selfridge, then a, b, c, d will satisfy (1.3). It follows that (1.3) has exactly 196 solutions. We are interested to see whether such a finiteness result holds in more generality, where the polynomial $P(n,m)=(n^a-n^b)(m^c-m^d)$ is replaced for instance by a polynomial $P(n,m)$ which does not decompose as a product of two polynomials of one variable each. The general two dimensional problem we pose is the following. Let K be a number field and let $\mathbf{A}$ be its ring of integers. Choose a $k\times l$ matrix $(\alpha_{ij})_{\substack{1\le i\le k\\1\le j\le l}}$ with entries in $\mathbf{A}$, and two elements $\beta,\gamma\in\mathbf{A}$. Then consider the set of pairs $(\mathbf{a},\mathbf{b})\in\mathbb{N}^k\times\mathbb{N}^l$, $\mathbf{a}=(a_1,\dots,a_k)$, $\mathbf{b}=(b_1,\dots,b_l)$, for which

$$\sum_{\substack{1\le i\le k\\1\le j\le l}}\alpha_{ij}\beta^{a_i}\gamma^{b_j} \quad \text{divides} \quad \sum_{\substack{1\le i\le k\\1\le j\le l}}\alpha_{ij}z^{a_i}w^{b_j} \text{ for any } z,w\in\mathbf{A}. \tag{1.4}$$

The problem is to find circumstances under which (1.4) has only finitely many solutions $(\mathbf{a},\mathbf{b})\in\mathbb{N}^k\times\mathbb{N}^l$. More generally, we consider for any n an n-dimensional version of the problem. Thus we replace the matrix $(\alpha_{ij})_{\substack{1\le i\le k\\1\le j\le l}}$ by a system of elements in $\mathbf{A}$ of the form $(\alpha_{i_1,\dots,i_n})_{\substack{1\le i_1\le k_1\\ \cdots\cdots\\ 1\le i_n\le k_n}}$ and instead of the pair (β,γ) we select an n-tuple

$(\beta_1,\ldots,\beta_n)$ of nonzero elements in $\mathbf{A}$. Then we consider the set of n-tuples $(\mathbf{a_1},\ldots,\mathbf{a_n}) \in \mathbb{N}^{k_1} \times \mathbb{N}^{k_2} \times \cdots \times \mathbb{N}^{k_n}$, $\mathbf{a}_j = (a_{j_1},\ldots,a_{jk_j})$ for $1 \le j \le n$, such that

(1.5)
$$\sum_{\substack{1\le i_1\le k_1\\ \cdots\cdots\\ 1\le i_n\le k_n}} \alpha_{i_1,\ldots,i_n}\beta_1^{a_{1i_1}}\cdots\beta_n^{a_{ni_n}} \quad \text{divides} \quad \sum_{\substack{1\le i_1\le k_1\\ \cdots\cdots\\ 1\le i_n\le k_n}} \alpha_{i_1,\ldots,i_n} z_1^{a_{1i_1}}\cdots z_n^{a_{ni_n}}$$

for any $z_1,\ldots,z_n \in \mathbf{A}$. Generalizing (1.2), in what follows we will only be concerned with those solutions $(\mathbf{a}_1,\ldots,\mathbf{a}_n)$ to (1.5) for which

$$\sum_{(i_1,\ldots,i_n)\in S} \alpha_{i_1,\ldots,i_n}\beta_1^{a_{1i_1}}\cdots\beta_n^{a_{ni_n}} \ne 0 \tag{1.6}$$

for any nonempty subset S of $\{1,2,\ldots,k_1\} \times \cdots \times \{1,2,\ldots,k_n\}$. Then we prove the following result.

THEOREM 1. *Let* $\mathbf{A}$ *be the ring of integers in an algebraic number field. Fix* n *and choose nonzero elements* $\beta_1,\ldots,\beta_n \in \mathbf{A}$, *none of them a unit, and let* $\alpha_{i_1,\ldots,i_n} \in \mathbf{A}$, *for* $1 \le i_1 \le k_1,\ldots,1 \le i_n \le k_n$. *Then there are only finitely many* n*-tuples* $(\mathbf{a}_1,\ldots,\mathbf{a}_n) \in \mathbb{N}^{k_1} \times \cdots \times \mathbb{N}^{k_n}$ *satisfying relations* (1.5) *and* (1.6) *above.*

Again in some cases we can strengthen the result.

THEOREM 2. *Let* $\mathbf{A}$ *be the ring of rational integers* $\mathbb{Z}$ *or the ring of integers in an imaginary quadratic field. Fix* n *and choose nonzero elements* $\alpha_{i_1,\ldots,i_n} \in \mathbf{A}$, *for* $1 \le i_1 \le k_1,\ldots,1 \le i_n \le k_n$. *Then there are only finitely many* n*-tuples* $(\beta_1,\ldots,\beta_n)$ *with* $\beta_j \in \mathbf{A}$, $j = 1,\ldots,n$ *for which there exists* $(\mathbf{a}_1,\ldots,\mathbf{a}_n) \in \mathbb{N}^{k_1} \times \cdots \times \mathbb{N}^{k_n}$ *with none of the tuples* $\mathbf{a}_1,\ldots,\mathbf{a}_n$ *having all the components equal to zero, such that* (1.5) *and* (1.6) *are satisfied.*

2. Some lemmas

Fix a number field K and let $\mathbf{A}$ be its ring of integers. Here and throughout the paper Norm$(\cdot)$ stands for Norm$_{K/\mathbb{Q}}(\cdot)$. We first recall some results from [7].

LEMMA 1. *Let* $\alpha_1,\ldots,\alpha_k$ *and* β *be nonzero complex numbers, with* $|\beta| \ne 1$. *Then there exists a constant* $c > 0$, *depending on* $\alpha_1,\ldots,\alpha_k$

and β, such that for any $(a_1, \ldots, a_k) \in \mathbb{N}^k$ satisfying (1.2) *we have*

$$\left|\sum_{i=1}^{k} \alpha_i \beta^{a_i}\right| \geq c \max\left\{|\beta|^{a_1}, \ldots, |\beta|^{a_k}\right\}.$$

This is Lemma 1 of [7].

LEMMA 2. *Let $g(X) \in \mathbf{A}[X]$, $g(X) = \sum_{i=1}^{k} \alpha_i X^{a_i}$, where $\alpha_1 \neq 0$, $a_1 > a_2 > \cdots > a_k$, $\Delta(g) = \prod_{i=2}^{k}(a_1 - a_i)$, and denote by $J(g)$ the ideal of $\mathbf{A}$ generated by the set $\{g(z) : z \in \mathbf{A}\}$. Then for any prime ideal P of $\mathbf{A}$ which divides $J(g)$, at least one of the following holds true:*

$$\begin{aligned} &(i) \quad P \quad \textit{divides} \quad \alpha_1, \quad \textit{or} \\ &(ii) \quad \mathrm{Norm}(P) - 1 \quad \textit{divides} \quad \Delta(g). \end{aligned}$$

This is lemma 2 of [7].

LEMMA 3. *Let $\alpha_1, \ldots, \alpha_k$, $a_1, \ldots, a_k$, $g(X)$, $\Delta(g)$ and $J(g)$ be as in Lemma 2. Then for any prime ideal P of $\mathbf{A}$ which divides $J(g)$, one has*

$$\begin{aligned} &v_P\left(J(g)\right) \\ &\leq \left(1 + \frac{1}{\mathrm{Norm}(P) - 1}\right)^{k-1} \left(v_P\left(\alpha_1 \Delta(g)\right) + \mathrm{Norm}(P)\right) - \mathrm{Norm}(P), \end{aligned}$$

where $v_P\left(J(g)\right)$ and $v_P\left(\alpha_1 \Delta(g)\right)$ denote the exponent of P in $J(g)$ and respectively in $\alpha_1 \Delta(g)$.

This is Corollary 1 in [7].

Next, we generalize the above results, as follows.

LEMMA 4. *Let $\alpha_{i_1,\ldots,i_n}$ with $1 \leq i_1 \leq k_1, \ldots, 1 \leq i_n \leq k_n$, be complex numbers, and let $\beta_1, \ldots, \beta_n$ be nonzero complex numbers, with $|\beta_j| \neq 1$ for $1 \leq j \leq n$. Then there exists a real number $c > 0$ such that for any $(\mathbf{a}_1, \ldots, \mathbf{a}_n) \in \mathbb{N}^{k_1} \times \cdots \times \mathbb{N}^{k_n}$ satisfying* (1.6) *we have*

$$\left|\sum_{\substack{1 \leq i_1 \leq k_1 \\ \cdots\cdots \\ 1 \leq i_n \leq k_n}} \alpha_{i_1,\ldots,i_n} \beta_1^{a_{1i_1}} \cdots \beta_n^{a_{ni_n}}\right| \geq c \prod_{j=1}^{n} \max\left\{|\beta_j|^{a_{j1}}, \ldots, |\beta_j|^{a_{jk_j}}\right\}. \tag{2.1}$$

Proof. We proceed to prove the lemma by induction on n. For $n = 1$ the statement reduces to Lemma 1 above. Let $n > 1$ and assume that the statement holds for $n-1$. With $k_2, \ldots, k_n$ fixed, we proceed to prove the lemma by induction on k_1. In case $k_1 = 1$, the left hand side of (2.1) reduces to

$$|\beta_1^{a_{11}}| \cdot \left| \sum_{\substack{1 \le i_2 \le k_2 \\ \cdots\cdots \\ 1 \le i_n \le k_n}} \alpha_{1, i_2, \dots, i_n} \beta_2^{a_{2i_2}} \cdots \beta_n^{a_{ni_n}} \right|, \tag{2.2}$$

and the existence of the required constant $c > 0$ follows by the induction hypothesis. Let now $k_1 > 1$ and assume that the statement holds for $k_1 - 1$. Denote

$$S = \sum_{\substack{1 \le i_1 \le k_1 \\ \cdots\cdots \\ 1 \le i_n \le k_n}} \alpha_{i_1, \dots, i_n} \beta_1^{a_{1i_1}} \cdots \beta_n^{a_{ni_n}}. \tag{2.3}$$

Choose $i^* \in \{1, 2, \dots, k_1\}$ such that

$$a_{1i^*} = \begin{cases} \max\{a_{11}, \dots, a_{1k_1}\}, & \text{if } |\beta_1| > 1 \\ \min\{a_{11}, \dots, a_{1k_1}\}, & \text{if } |\beta_1| < 1. \end{cases} \tag{2.4}$$

In both cases we have

$$|\beta_1|^{a_{1i^*}} = \max\left\{ |\beta_1|^{a_{11}}, \dots, |\beta_1|^{a_{1k_1}} \right\}. \tag{2.5}$$

Next, choose $j^* \in \{1, 2, \dots, k_1\}$, $j^* \ne i^*$, such that $|\beta_1|^{a_{1j^*}}$ is as large as possible. Thus

$$|\beta_1|^{a_{1j^*}} = \max\{|\beta_1|^{a_{1j}} : 1 \le j \le k_1, j \ne i^*\}. \tag{2.6}$$

The idea is that if $|\beta_1|^{a_{1i^*}}$ is much larger than $|\beta_1|^{a_{1j^*}}$, then the sum of terms with $i_1 = i^*$ on the right side of (2.3) will dominate the sum of terms with $i_1 \ne i^*$. To be precise, let us write S in the form

$$S = S_1 + S_2, \tag{2.7}$$

where

$$S_1 = \beta_1^{a_{1i^*}} \sum_{\substack{1 \le i_2 \le k_2 \\ \cdots\cdots \\ 1 \le i_n \le k_n}} \alpha_{i^*, i_2, \dots, i_n} \beta_2^{a_{2i_2}} \cdots \beta_n^{a_{ni_n}}, \tag{2.8}$$

and

$$S_2 = \sum_{\substack{1 \le i_1 \le k_1 \\ i_1 \ne i^*}} \beta_1^{a_{1i_1}} \sum_{\substack{1 \le i_2 \le k_2 \\ \cdots\cdots \\ 1 \le i_n \le k_n}} \alpha_{i_1, \dots, i_n} \beta_2^{a_{2i_2}} \cdots \beta_n^{a_{ni_n}}. \tag{2.9}$$

By the induction hypothesis applied to the sum on the right side of (2.8) we know that there is a constant $c^* > 0$, depending on $\beta_2, \dots, \beta_n$ and on the coefficients $\alpha_{i^*, i_2, \dots, i_n}$, such that

(2.10)

$$\left| \sum_{\substack{1 \le i_2 \le k_2 \\ \cdots\cdots \\ 1 \le i_n \le k_n}} \alpha_{i^*, i_2, \dots, i_n} \beta_2^{a_{2i_2}} \cdots \beta_n^{a_{ni_n}} \right| \ge c^* \prod_{j=2}^{n} \max \left\{ |\beta_j|^{a_{j1}}, \dots, |\beta_j|^{a_{jk_j}} \right\}.$$

Combining (2.10) with (2.5) and (2.8), we see that

$$|S_1| \ge c^* \prod_{j=1}^{n} \max \left\{ |\beta_j|^{a_{j1}}, \dots, |\beta_j|^{a_{jk_j}} \right\}. \tag{2.11}$$

On the other hand, from (2.6) and (2.9) it follows that

$$\begin{aligned} |S_2| &\le \sum_{\substack{1 \le i_1 \le k_1 \\ i_1 \ne i^*}} |\beta_1|^{a_{1j^*}} \sum_{\substack{1 \le i_2 \le k_2 \\ \cdots\cdots \\ 1 \le i_n \le k_n}} |\alpha_{i_1, \dots, i_n}| \, |\beta_2|^{a_{2i_2}} \cdots |\beta_n|^{a_{ni_n}} \\ &\le C |\beta_1|^{a_{1j^*}} \prod_{j=2}^{n} \max \left\{ |\beta_j|^{a_{j1}}, \dots, |\beta_j|^{a_{jk_j}} \right\}, \end{aligned} \tag{2.12}$$

where we denote

$$C = \sum_{\substack{1 \le i_1 \le k_1 \\ \cdots\cdots \\ 1 \le i_n \le k_n}} |\alpha_{i_1, \dots, i_n}|. \tag{2.13}$$

We distinguish two cases. Assume first that

$$c^* |\beta_1|^{a_{1i^*}} \ge 2C |\beta_1|^{a_{1j^*}}. \tag{2.14}$$

Then, from (2.11), (2.12) and (2.14) it follows that $|S_1| \ge 2|S_2|$, so

$$|S| \ge \frac{|S_1|}{2} \ge \frac{c^*}{2} \prod_{j=1}^{n} \max \left\{ |\beta_j|^{a_{j1}}, \dots, |\beta_j|^{a_{jk_j}} \right\}, \tag{2.15}$$

and hence (2.1) holds in this case, with $c = \frac{c^*}{2}$. Assume now that

$$c^* |\beta_1|^{a_{1i^*}} < 2C |\beta_1|^{a_{1j^*}}. \tag{2.16}$$

Let

$$D = \left[\left| \frac{\log \left(\frac{2C}{c^*} \right)}{\log |\beta_1|} \right| \right], \tag{2.17}$$

where $[\cdot]$ denotes the integer part. By (2.16) and (2.17) it follows that

$$|a_{1i^*} - a_{1j^*}| \leq D. \tag{2.18}$$

By the definition of i^* and j^* we also know that $a_{1i^*} \geq a_{1j^*}$ if $|\beta_1| > 1$, and $a_{1i^*} \leq a_{1j^*}$ if $|\beta_1| < 1$. Denote

$$d = \begin{cases} a_{1i^*} - a_{1j^*}, & \text{if } |\beta_1| > 1 \\ a_{1j^*} - a_{1i^*}, & \text{if } |\beta_1| < 1. \end{cases} \tag{2.19}$$

Then d is a non-negative integer, bounded by D. Now the point is that for each fixed value of d, we may view the sum S, corresponding to the n-tuple $(\mathbf{a}_1, \mathbf{a}_2, \dots, \mathbf{a}_n)$, as a sum corresponding to another n-tuple, in which $\mathbf{a}_2, \dots, \mathbf{a}_n$ are the same, while $\mathbf{a}_1$ has one of its components removed. More precisely, if $|\beta_1| > 1$ then we remove from $\mathbf{a}_1$ the component a_{1i^*}, and respectively if $|\beta_1| < 1$ then we remove from $\mathbf{a}_1$ the component a_{1j^*}. Then we use (2.19) on the right side of (2.3), in order to write S in terms of $\mathbf{a}_2, \dots, \mathbf{a}_n$ and the components of $\mathbf{a}_1$ that were not removed. Thus the same sum S, which was initially of type $k_1 \times k_2 \times \cdots \times k_n$, can be viewed as a sum of type $(k_1 - 1) \times k_2 \times \cdots \times k_n$. Obviously, in doing this, the new coefficients will depend on d. We may use the induction hypothesis, and conclude that (2.1) holds for our sum S, with a constant $c = c_d > 0$ depending on d. We now choose c to be the smallest of the constants c_d, for $0 \leq d \leq D$, and this completes the proof of the lemma. □

LEMMA 5. *Let* $g(X_1, \dots, X_n) \in \mathbf{A}[X_1, \dots, X_n]$, $g(X_1, \dots, X_n) = \sum_{\substack{1 \leq i_1 \leq k_1 \\ \cdots\cdots \\ 1 \leq i_n \leq k_n}} \alpha_{i_1, \dots, i_n} X_1^{a_{1i_1}} \cdots X_n^{a_{ni_n}}$, *where* $k_1, \dots, k_n \geq 1$, $\alpha_{1,\dots,1} \neq 0$, $a_{j1} > a_{j2} > \cdots > a_{jk_j}$ *for* $1 \leq j \leq n$, $\Delta(g) = \prod_{j=1}^{n} \prod_{i=2}^{k_j} (a_{j1} - a_{ji})$, *and denote by* $J(g)$ *the ideal of* $\mathbf{A}$ *generated by the set* $\{g(z_1, \dots, z_n) : z_1, \dots, z_n \in \mathbf{A}\}$. *Then for any prime ideal* P *of* $\mathbf{A}$ *which divides* $J(g)$, *at least one of the following holds true:*

$$\begin{aligned} &(i) \quad P \quad \textit{divides} \quad \alpha_{1,\dots,1}, \quad \textit{or} \\ &(ii) \quad \mathrm{Norm}(P) - 1 \quad \textit{divides} \quad \Delta(g). \end{aligned}$$

Proof. We prove the lemma by induction on n. For $n = 1$ the statement reduces to the statement of Lemma 2 above. Let $n > 1$ and assume that the statement holds for $n - 1$. Choose a polynomial $g(X_1, \dots, X_n)$ as in the statement of the lemma, and let P be a prime ideal of $\mathbf{A}$ which divides $J(g)$. We write $g(X_1,\dots,X_n)$ as a polynomial in X_1, with coefficients in $\mathbf{A}\,[X_2,\dots,X_n]$, say

$$\begin{aligned}(2.20)\quad g(X_1,\dots,X_n) = h_1(X_2,\dots,X_n)X_1^{a_{11}} + h_2(X_2,\dots,X_n)X_1^{a_{12}} + \cdots \\ + \cdots + h_{k_1}(X_2,\dots,X_n)X_1^{a_{1k_1}}.\end{aligned}$$

Next, we assign arbitrary values $z_2,\dots,z_n \in \mathbf{A}$ to the variables $X_2,\dots,X_n$, and consider the polynomial in one variable

$$(2.21)\qquad f(X_1) = g(X_1,z_2,\dots,z_n) = \sum_{i=1}^{k_1} h_i(z_2,\dots,z_n)X_1^{a_{1i}}.$$

We know that P divides $f(z_1)$ for any $z_1 \in \mathbf{A}$, thus P divides $J(f)$. Applying Lemma 2 to the polynomial $f(X_1)$, we find that at least one of the following holds true:

$$(2.22)\qquad P \quad \text{divides} \quad h_1(z_2,\dots,z_n)$$

for this particular choice of $z_2,\dots,z_n$, or

$$(2.23)\qquad \operatorname{Norm}(P) - 1 \quad \text{divides} \quad \Delta(f).$$

If (2.23) holds, then we are done, since obviously $\Delta(f)$ divides $\Delta(g)$. Suppose now that (2.23) fails. Then (2.22) will hold true for any choice of $z_2,\dots,z_n$ in $\mathbf{A}$. In this case P will divide the ideal $J(h_1)$ generated by the set $\{h_1(z_2,\dots,z_n) : z_2,\dots,z_n \in \mathbf{A}\}$. Applying the induction hypothesis to the polynomial $h_1(X_2,\dots,X_n)$, we see that at least one of the following holds true:

$$(2.24)\qquad P \quad \text{divides} \quad \alpha_{1,\dots,1}, \quad \text{or}$$

$$(2.25)\qquad \operatorname{Norm}(P) - 1 \quad \text{divides} \quad \Delta(h_1).$$

Here $\Delta(h_1)$ divides $\Delta(g)$, and the lemma is proved. □

LEMMA 6. *With notation as in Lemma 5, for any prime ideal P of $\mathbf{A}$ which divides $J(g)$ one has*

$$\begin{aligned}(2.26)\qquad v_P(J(g)) \le \left(1 + \frac{1}{\operatorname{Norm}(P)-1}\right)^{k_1+\cdots+k_n-n} \\ \cdot \left(v_P\left(\alpha_{1,\dots,1}\Delta(g)\right) + \operatorname{Norm}(P)\right) - \operatorname{Norm}(P).\end{aligned}$$

Proof. We prove the lemma by induction on n. For $n = 1$ the statement reduces to Lemma 3 above. Let $n > 1$ and assume that the statement holds for $n-1$. Choose a polynomial $g(X_1, \dots, X_n)$ as in the statement of the lemma, and let P be a prime ideal of $\mathbf{A}$ which divides $J(g)$. As in the proof of Lemma 5 we write $g(X_1, \dots, X_n)$ as a polynomial in X_1 with coefficients in $\mathbf{A}[X_2, \dots, X_n]$,

$$g(X_1, \dots, X_n) = \sum_{i=1}^{k_1} h_i(X_2, \dots, X_n) X_1^{a_{1i}}. \tag{2.27}$$

Then, for any $z_2, \dots, z_n \in \mathbf{A}$, consider the polynomial in one variable

$$f(X_1) = g(X_1, z_2, \dots, z_n) = \sum_{i=1}^{k_1} h_i(z_2, \dots, z_n) X_1^{a_{1i}}. \tag{2.28}$$

We know that P divides the ideal $J(f)$ generated by the set $\{f(z_1) : z_1 \in \mathbf{A}\}$. Applying Lemma 3 to the polynomial $f(X_1)$, we obtain

$$\begin{aligned} v_P(J(f)) \leq &\left(1 + \frac{1}{\operatorname{Norm}(P) - 1}\right)^{k_1 - 1} \\ &\cdot \left(v_P\left(h_1(z_2, \dots, z_n)\Delta(f)\right) + \operatorname{Norm}(P)\right) - \operatorname{Norm}(P). \end{aligned} \tag{2.29}$$

Evidently $J(g)$ divides $J(f)$. Thus $v_P(J(g)) \leq v_P(J(f))$, and combining this with (2.29) we find that

$$\begin{aligned} v_P(J(g)) \leq &\left(\left(1 + \frac{1}{\operatorname{Norm}(P) - 1}\right)^{k_1 - 1} - 1\right) \operatorname{Norm}(P) \\ &+ \left(1 + \frac{1}{\operatorname{Norm}(P) - 1}\right)^{k_1 - 1} v_P(\Delta(f)) \\ &+ \left(1 + \frac{1}{\operatorname{Norm}(P) - 1}\right)^{k_1 - 1} v_P(h_1(z_2, \dots, z_n)). \end{aligned} \tag{2.30}$$

Since (2.30) holds for any $z_2, \dots, z_n \in \mathbf{A}$, and since the set

$$\{h_1(z_2, \dots, z_n) : z_2, \dots, z_n \in \mathbf{A}\}$$

generates the ideal $J(h_1)$, we deduce that

$$\begin{aligned}(2.31)\qquad v_P\left(J(g)\right) \le {} & \left(\left(1+\frac{1}{\mathrm{Norm}(P)-1}\right)^{k_1-1}-1\right)\mathrm{Norm}(P)\\ & +\left(1+\frac{1}{\mathrm{Norm}(P)-1}\right)^{k_1-1} v_P(\Delta(f))\\ & +\left(1+\frac{1}{\mathrm{Norm}(P)-1}\right)^{k_1-1} v_P(J(h_1)).\end{aligned}$$

Applying the induction hypothesis to the polynomial $h_1(X_2,\ldots,X_n)$, we have

$$\begin{aligned}(2.32)\qquad v_P(J(h_1)) \le {} & \left(1+\frac{1}{\mathrm{Norm}(P)-1}\right)^{k_2+\cdots+k_n-(n-1)}\\ & \cdot\left(v_P\left(\alpha_{1,\ldots,1}\Delta(h_1)\right)+\mathrm{Norm}(P)\right)-\mathrm{Norm}(P).\end{aligned}$$

Combining (2.31) with (2.32) and using the fact that

$$\Delta(g)=\Delta(f)\Delta(h_1),$$

which implies $v_P(\Delta(g))=v_P(\Delta(f))+v_P(\Delta(h_1))$, we derive

$$\begin{aligned}(2.33)\quad v_P(J(g)) \le {} & \left(\left(1+\frac{1}{\mathrm{Norm}(P)-1}\right)^{k_1-1}-1\right)\mathrm{Norm}(P)\\ & +\left(1+\frac{1}{\mathrm{Norm}(P)-1}\right)^{k_1-1} v_P(\Delta(f))\\ & +\left(1+\frac{1}{\mathrm{Norm}(P)-1}\right)^{k_1+k_2+\cdots+k_n-n}\\ & \cdot\left(v_P\left(\alpha_{1,\ldots,1}\Delta(h_1)\right)+\mathrm{Norm}(P)\right)\\ & -\left(1+\frac{1}{\mathrm{Norm}(P)-1}\right)^{k_1-1}\mathrm{Norm}(P)\\ = {} & \left(1+\frac{1}{\mathrm{Norm}(P)-1}\right)^{k_1+\cdots+k_n-n}\\ & \cdot\left(v_P\left(\alpha_{1,\ldots,1}\Delta(h_1)\right)+\mathrm{Norm}(P)\right)\\ & +\left(1+\frac{1}{\mathrm{Norm}(P)-1}\right)^{k_1-1} v_P(\Delta(f))-\mathrm{Norm}(P)\end{aligned}$$

$$\leq \left(1+\frac{1}{\mathrm{Norm}(P)-1}\right)^{k_1+\cdots+k_n-n}$$
$$\cdot\left(v_P\left(\alpha_{1,\ldots,1}\Delta(g)\right)+\mathrm{Norm}(P)\right)-\mathrm{Norm}(P).$$

This completes the proof of Lemma 6. □

As in [7], we now take advantage of the fact that the right hand side of (2.26), as a function of P, with $\mathbf{A}, k_1, \ldots, k_n$ and g fixed, is bounded: the coefficient of $v_P\left(\alpha_{1,\ldots,1}\Delta(g)\right)$ is bounded by $2^{k_1+\cdots+k_n-n}$, and the function $x \mapsto \left(1+\frac{1}{x-1}\right)^{k_1+\cdots+k_n-n} x - x$ is bounded as $x \to \infty$. Taking these facts into account, we infer the following result.

Corollary 1. *There are integers $l_1, l_2 > 0$, depending on $k_1, \ldots, k_n$ and $\mathbf{A}$, such that, with the notations from Lemma 5, we have*

$$v_P(J(g)) \leq l_2 v_P\left(\alpha_{1,\ldots,1}\Delta(g)\right)$$

for any prime ideal P for which $v_P(J(g)) \geq l_1$.

Combining Corollary 1 with Lemma 5, we obtain the following result, which is a generalization of Proposition 2 from [7].

Lemma 7. *There are constants $l_3, l_4, l_5, l_6 > 0$, depending on $k_1, \ldots,$ k_n and $\mathbf{A}$, such that for any $g(X_1, \ldots, X_n)$ as in Lemma 5, one has*

$$\mathrm{Norm}(J(g)) \leq l_3 \left|\mathrm{Norm}(\alpha_{1,\ldots,1})\right|^{l_4} \exp\left(l_5 a^{\frac{l_6}{\log\log a}}\right),$$

where $a = \max\{a_{11}, a_{21}, \ldots, a_{n1}, 3\}$.

Proof. Let $g(X_1, \ldots, X_n)$ be as in Lemma 5. We decompose $J(g) = J_1 J_2$, where J_1 contains those primes P for which $v_P(J(g)) < l_1$, and J_2 contains those primes P for which $v_P(J(g)) \geq l_1$. Then form Corollary 1 it follows that J_2 divides $\left(\alpha_{1,\ldots,1}\Delta(g)\right)^{l_2}$. Therefore

(2.34)
$$\mathrm{Norm}(J_2) \leq \left|\mathrm{Norm}\left(\alpha_{1,\ldots,1}\Delta(g)\right)\right|^{l_2} = \left|\mathrm{Norm}(\alpha_{1,\ldots,1})\right|^{l_2} |\Delta(g)|^{l_2[K:\mathbb{Q}]}.$$

Note that $|\Delta(g)| \leq \prod_{j=1}^{n} a_{j1}^{k_j-1} \leq a^{k_1+\cdots+k_n-n}$ and $\log a \leq a^{\frac{l_6}{\log\log a}}$, uniformly in a for l_6 large enough. This clearly gives an upper bound of the required type for $\mathrm{Norm}(J_2)$. Let now $J_0 = \prod_{\substack{P \mid J_1 \\ P \text{ prime}}} P$. Since J_1 divides $J_0^{l_1}$, one has $\mathrm{Norm}(J_1) \leq (\mathrm{Norm}(J_0))^{l_1}$. Thus in order to complete the proof of the lemma, it remains to prove an upper bound of the required type for J_0. To proceed, we first remove from J_0 all the prime divisors of 2, if there are any such divisors, and we also remove any prime divisor of $\alpha_{1,\dots,1}$. Note that the norm of the product of all the removed prime divisors is bounded by $|\mathrm{Norm}(2\alpha_{1,\dots,1})|$. Hence we are left with a square free divisor of $J(g)$, call it J_3, which is relatively prime to $2\alpha_{1,\dots,1}$. Lemma 5 implies that for any prime divisor P of J_3, $\mathrm{Norm}(P)-1$ divides $\Delta(g)$. Note that any positive integer equals $\mathrm{Norm}(P) - 1$ for at most $[K : \mathbb{Q}]$ prime ideals P in $\mathbf{A}$. It follows that $\prod_{\substack{P|J_3 \\ P \text{ prime}}} (\mathrm{Norm}(P) - 1)$ divides $\prod_{d|\Delta(g)} d^{[K:\mathbb{Q}]}$. This last product equals $\Delta(g)^{\frac{1}{2}[K:\mathbb{Q}]\sigma_0(\Delta(g))}$, where $\sigma_0(\Delta(g))$ denotes the number of divisors of $\Delta(g)$. For $\sigma_0(\Delta(g))$ one has the well known upper bound (see Ramanujan [3])

$$\sigma_0(\Delta(g)) \le c(\epsilon)\Delta(g)^{\frac{\log 2+\epsilon}{\log\log \Delta(g)}}$$

for any fixed $\epsilon > 0$. Note also that since $\mathrm{Norm}(P) \ge 3$ for any prime P which divides J_3, we have $\mathrm{Norm}(P) < (\mathrm{Norm}(P) - 1)^2$, and hence

$$\mathrm{Norm}(J_3) < \prod_{\substack{P|J_3 \\ P \text{ prime}}} (\mathrm{Norm}(P) - 1)^2 .$$

By combining the above inequalities one obtains an upper bound of the required type for $\mathrm{Norm}(J_3)$, and the lemma is proved. □

3. Proof of Theorem 1

Proof. We prove the theorem by induction on n. For $n = 1$ the statement reduces to Theorem 1 in [7]. Let $n > 1$ and assume that the statement holds true for $n - 1$. Next, we proceed by induction on k_1. If $k_1 = 1$, then (1.5) says that

(3.1)
$$\beta_1^{a_{11}} \sum_{\substack{1\le i_2\le k_2 \\ \cdots\cdots \\ 1\le i_n\le k_n}} \alpha_{1,i_2,\dots,i_n}\beta_2^{a_{2i_2}}\cdots\beta_n^{a_{ni_n}} \text{ divides } z_1^{a_{11}} \sum_{\substack{1\le i_2\le k_2 \\ \cdots\cdots \\ 1\le i_n\le k_n}} \alpha_{1,i_2,\dots,i_n} z_2^{a_{2i_2}}\cdots z_n^{a_{ni_n}}$$

for any $z_1, z_2, \dots, z_n \in \mathbf{A}$. In particular, if we set $z_2 = \beta_2, \dots, z_n = \beta_n$, from (3.1) it follows that $\beta_1^{a_{11}}$ divides $z_1^{a_{11}}$ for any $z_1 \in \mathbf{A}$. We take $z_1 = 1$, then $\beta_1^{a_{11}}$ divides 1, and since β_1 is not a unit it follows that $a_{11} = 0$. Using this in (3.1), we find that

(3.2)
$$\sum_{\substack{1\le i_2\le k_2 \\ \cdots\cdots \\ 1\le i_n\le k_n}} \alpha_{1,i_2,\dots,i_n}\beta_2^{a_{2i_2}}\cdots\beta_n^{a_{ni_n}} \quad \text{divides} \quad \sum_{\substack{1\le i_2\le k_2 \\ \cdots\cdots \\ 1\le i_n\le k_n}} \alpha_{1,i_2,\dots,i_n} z_2^{a_{2i_2}}\cdots z_n^{a_{ni_n}}$$

for any $z_2, \dots, z_n \in \mathbf{A}$. The induction hypothesis now shows that there are only finitely many tuples $(\mathbf{a}_2, \dots, \mathbf{a}_n)$ satisfying the above conditions, and this completes the proof in case $k_1 = 1$. Let now $k_1 > 1$ and assume that the statement of the theorem holds for $k_1 - 1$. We order the components $a_{11}, \dots, a_{1k_1}$ of the vector $\mathbf{a}_1$ according to their size. To make a choice, assume that we have $a_{11} \geq a_{12} \geq \cdots \geq a_{1k_1}$. If at least one of these inequalities is an equality, that is, if two of the integers $a_{11}, a_{12}, \dots, a_{1k_1}$ are equal, then we are left with $k_1 - 1$ independent integers, and the finiteness of the number of solutions follows from the induction hypothesis. We may then assume in the following that we have strict inequalities $a_{11} > a_{12} > \cdots > a_{1k_1}$. In order to complete the induction step from $k_1 - 1$ to k_1, which will also complete the proof of the theorem, we start an induction argument with respect to k_2. The case $k_2 = 1$ is easily settled by a reasoning similar to the one employed in the case $k_1 = 1$, establishing analogs of relations (3.1) and (3.2) in the process. Let now $k_2 > 1$ and assume that the statement of the theorem holds for $k_2 - 1$. As before, we order the components of the vector $\mathbf{a}_2$ according to their size. To make a choice, assume that $a_{21} \geq a_{22} \geq \cdots \geq a_{2k_2}$. Again if at least one of these inequalities is an equality, the statement of the theorem follows by the induction hypothesis. We may then assume for the rest of the proof that we have strict inequalities $a_{21} > a_{22} > \cdots > a_{2k_2}$. Next, we proceed by induction on k_3, then on $k_4, \dots$, and finally on k_n. When we arrive at that stage where one uses induction on k_n, we order the components of $\mathbf{a}_n$ according to their size, say $a_{n1} \geq a_{n2} \geq \cdots \geq a_{nk_n}$. Then, arguing as before, we may assume that these inequalities are strict, otherwise the statement of the theorem holds by the induction hypothesis. Thus, in order to complete the proof of the theorem, we are left with the case where $k_1 > 1, \dots, k_n > 1$, and we have strict inequalities $a_{j1} > a_{j2} > \cdots > a_{jk_j}$ for any $j \in \{1, 2, \dots, n\}$. We are then under the assumptions from Lemmas 5, 6 and 7. Consider the polynomial

$$g(X_1, \dots, X_n) = \sum_{\substack{1 \leq i_1 \leq k_1 \\ \cdots\cdots \\ 1 \leq i_n \leq k_n}} \alpha_{i_1, \dots, i_n} X_1^{a_{1i_1}} \cdots X_n^{a_{ni_n}}. \tag{3.3}$$

By Lemma 7 it follows that

$$\operatorname{Norm}(J(g)) \leq l_3 \left|\operatorname{Norm}(\alpha_{1,\dots,1})\right|^{l_4} \exp\left(l_5 a^{\frac{l_6}{\log\log a}}\right), \tag{3.4}$$

where $a = \max\{a_{11}, a_{21}, \dots, a_{n1}, 3\}$, $J(g)$ is the ideal of $\mathbf{A}$ generated by the set $\{g(z_1, \dots, z_n) : z_1, \dots, z_n \in \mathbf{A}\}$, and l_3, l_4, l_5, l_6 are positive constants which depend on $k_1, \dots, k_n$ and the ring $\mathbf{A}$. From (1.5) we know that

$$S := \sum_{\substack{1 \le i_1 \le k_1 \\ \cdots\cdots \\ 1 \le i_n \le k_n}} \alpha_{i_1,\dots,i_n} \beta_1^{a_{1i_1}} \cdots \beta_n^{a_{ni_n}} \tag{3.5}$$

is a divisor of $J(g)$. It follows that $\mathrm{Norm}(S)$ divides $\mathrm{Norm}(J(g))$, and from (3.4) we derive

$$|\mathrm{Norm}(S)| \le l_3 \,|\mathrm{Norm}(\alpha_{1,\dots,1})|^{l_4} \exp\left(l_5 a^{\frac{l_6}{\log\log a}} \right). \tag{3.6}$$

Let now σ be any embedding of K into $\mathbb{C}$. By applying Lemma 4 to $\sigma(S)$ it follows that there exists a constant $c_\sigma > 0$, which depends on the numbers $\sigma(\beta_1), \dots, \sigma(\beta_n)$ and $\sigma(\alpha_{i_1,\dots,i_n})$ with $1 \le i_1 \le k_1, \dots, 1 \le i_n \le k_n$, such that

$$\begin{aligned} |\sigma(S)| &= \left| \sum_{\substack{1 \le i_1 \le k_1 \\ \cdots\cdots \\ 1 \le i_n \le k_n}} \sigma(\alpha_{i_1,\dots,i_n}) \sigma(\beta_1)^{a_{i_1}} \cdots \sigma(\beta_n)^{a_{i_n}} \right| \\ &\ge c_\sigma \prod_{j=1}^{n} \max\{|\sigma(\beta_j)|^{a_{j1}}, \dots, |\sigma(\beta_j)|^{a_{jk_j}}\}. \end{aligned} \tag{3.7}$$

Multiplying the inequalities (3.7) for all the embeddings σ of K into $\mathbb{C}$, we derive

$$\begin{aligned} |\mathrm{Norm}(S)| &\ge \left(\prod_\sigma c_\sigma \right) \prod_\sigma \prod_{j=1}^{n} \max\left\{ |\sigma(\beta_j)|^{a_{j1}}, \dots, |\sigma(\beta_j)|^{a_{jk_j}} \right\} \\ &\ge \left(\prod_\sigma c_\sigma \right) \prod_{j=1}^{n} |\mathrm{Norm}(\beta_j)|^{a_{j1}}. \end{aligned} \tag{3.8}$$

By combining (3.8) with (3.6) we obtain

$$\left(\prod_\sigma c_\sigma \right) \prod_{j=1}^{n} |\mathrm{Norm}(\beta_j)|^{a_{j1}} \le l_3 \,|\mathrm{Norm}(\alpha_{1,\dots,1})|^{l_4} \exp\left(l_5 a^{\frac{l_6}{\log\log a}} \right). \tag{3.9}$$

Since $|\mathrm{Norm}(\beta_j)| > 1$ for $1 \le j \le n$, from (3.9) one clearly obtains an upper bound for a, which is also an upper bound for each of the numbers a_{j1} with $1 \le j \le n$. It follows that there are only finitely many solutions $(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ to our problem, and this completes the proof of the theorem. □

4. Proof of Theorem 2

Proof. We prove the theorem by induction on n. For $n = 1$ the statement reduces to Theorem 2 from [7]. Let $n > 1$ and assume that the statement holds true for $n-1$. As in the proof of Theorem 1, we now use induction on k_1. Let $k_1 = 1$, and choose $\beta_1, \ldots, \beta_n \in \mathbf{A}$ for which there exists $(\mathbf{a}_1, \ldots, \mathbf{a}_n) \in \mathbb{N}^{k_1} \times \cdots \mathbb{N}^{k_n}$ with $\mathbf{a}_j \neq (0, \ldots, 0)$ for $1 \leq j \leq n$, such that (1.5) and (1.6) are satisfied. Then (1.5) reduces to (3.1), which further implies (3.2) on the one hand, and on the other hand it implies that $\beta_1^{a_{11}}$ divides 1. Since $a_{11} \geq 1$, it follows that β_1 is a unit in $\mathbf{A}$. The group of units of $\mathbf{A}$ is finite, so there are only finitely many choices for β_1. Also, from (3.2) it follows by the induction hypothesis that there are only finitely many $(n-1)$-tuples $(\beta_2, \ldots, \beta_n)$ with the required properties. This proves the statement of the theorem in case $k_1 = 1$. Let now $k_1 > 1$ and assume that the statement holds for $k_1 - 1$. Again we order the components of $\mathbf{a}_1$ according to their size, say $a_{11} \geq a_{12} \geq \cdots \geq a_{1k_1}$. If at least one of these inequalities is an equality, then we may use the induction hypothesis to obtain the desired result. Thus we may assume in what follows that $a_{11} > a_{12} > \cdots > a_{1k_1}$. As in the proof of Theorem 1, we continue the reasoning by using induction on k_2, then on $k_3, \ldots$, and lastly on k_n. In the end we are left with the case when $k_1 > 1, \ldots, k_n > 1$ and one has the inequalities $a_{j1} > a_{j2} > \cdots > a_{jk_j} \geq 0$ for $1 \leq j \leq n$. We need to show that there are only finitely many n-tuples $(\beta_1, \ldots, \beta_n)$ for which there exist tuples $\mathbf{a}_j = (a_{j1}, \ldots, a_{jk_j})$, $1 \leq j \leq n$ as above, satisfying (1.5) and (1.6). Let

$$f(X_1, \ldots, X_n) = \sum_{\substack{1 \leq i_1 \leq k_1 \\ \cdots\cdots \\ 1 \leq i_n \leq k_n}} \alpha_{i_1, \ldots, i_n} X_1^{a_{1i_1}} \cdots X_n^{a_{ni_n}}.$$

We claim that there exists an n-tuple $(r_1, \ldots, r_n)$ with $r_i \in \{1, 2, \ldots, 2^{k_i - 1}\}$, $i = 1, \ldots, n$ such that $f(r_1, \ldots, r_n) \neq 0$. This holds true for $n = 1$. For, in this case f reduces to $f(X_1) = \sum_{1 \leq i_1 \leq k_1} \alpha_{i_1} X_1^{a_{1i_1}}$.

Consider the nonzero Vandermonde determinant

$$\begin{vmatrix} 1 & \dots & 1 \\ 2^{a_{11}} & \dots & 2^{a_{1k_1}} \\ \vdots & \vdots & \vdots \\ 2^{(k_1-1)a_{11}} & \dots & 2^{(k_1-1)a_{1k_1}} \end{vmatrix}.$$

We add its columns multiplied by $\alpha_1, \dots, \alpha_{k_1}$ and obtain a new column that does not vanish and has $f(1), f(2), \dots, f(2^{k_1-1})$ as entries. Thus $f(r) \neq 0$ for some $r \in \{1, 2, \dots, 2^{k_1-1}\}$. Assume now that the above statement holds true for $n-1$ and suppose that $f(r_1, \dots, r_n) = 0$ for any $(r_1, \dots, r_n) \in \{1, 2, \dots, 2^{k_1-1}\} \times \cdots \times \{1, 2, \dots, 2^{k_n-1}\}$. Fix $(r_1, \dots, r_{n-1})$. Then for any $r_n \in \{1, 2, \dots, 2^{k_n-1}\}$,

$$h(r_n) := f(r_1, \dots, r_{n-1}, r_n) = \sum_{1 \leq i_n \leq k_n} A_{i_n} r_n^{a_{ni_n}} = 0,$$

where

$$A_{i_n} = \sum_{\substack{1 \leq i_1 \leq k_1 \\ \cdots\cdots \\ 1 \leq i_{n-1} \leq k_{n-1}}} \alpha_{i_1, \dots, i_n} r_1^{a_{1i_1}} \cdots r_{n-1}^{a_{n-1 i_{n-1}}}.$$

We now apply the case $n = 1$ to $h(r_n)$. It follows that for each $(r_1, \dots, r_{n-1}) \in \{1, 2, \dots, 2^{k_1-1}\} \times \cdots \times \{1, 2, \dots, 2^{k_n-1}\}$,

$$A_{i_n}(r_1, \dots, r_{n-1}) = \sum_{\substack{1 \leq i_1 \leq k_1 \\ \cdots\cdots \\ 1 \leq i_{n-1} \leq k_{n-1}}} \alpha_{i_1, \dots, i_n} r_1^{a_{1i_1}} \cdots r_{n-1}^{a_{n-1 i_{n-1}}} = 0.$$

This contradicts the induction hypothesis. Hence $f(r_1, \dots, r_n) \neq 0$ for some $(r_1, \dots, r_n) \in \{1, 2, \dots, 2^{k_1-1}\} \times \cdots \times \{1, 2, \dots, 2^{k_n-1}\}$, which proves the claim. Next, let us remark that since $f(\beta_1, \dots, \beta_n)$ divides $f(r_1, \dots, r_n)$ and since in the ring $\mathbf{A}$ under consideration the absolute value of any nonzero element of $\mathbf{A}$ is ≥ 1, we have $|f(\beta_1, \dots, \beta_n)| \leq |f(r_1, \dots, r_n)|$. Note that the condition (1.6) implies that

$$\sum_{1 \leq i_l \leq k_l} \alpha_{1, \dots, 1, i_l, 1, \dots, 1} \beta_l^{a_{li_l}} \neq 0$$

for any $l = 1, \dots, n$. It is clear that

$$\begin{aligned} |f(r_1, \dots, r_n)| &\leq \sum_{\substack{1\leq i_1\leq k_1\\ \cdots\cdots \\ 1\leq i_n\leq k_n}} |\alpha_{i_1,\dots,i_n}||r_1|^{a_{1i_1}} \cdots |r_n|^{a_{ni_n}} \\ &\leq 2^{k_1a_{11}+\cdots+k_na_{n1}} \sum_{\substack{1\leq i_1\leq k_1\\ \cdots\cdots \\ 1\leq i_n\leq k_n}} |\alpha_{i_1,\dots,i_n}|. \end{aligned} \tag{4.1}$$

On the other hand if for all $i = 1, \dots, n$,

$$|\beta_i| \geq \frac{2}{|\alpha_{1,\dots,1}|} \sum_{\substack{1\leq i_1\leq k_1\\ \cdots\cdots \\ 1\leq i_n\leq k_n \\ (i_1,\dots,i_n)\neq(1,\dots,1)}} |\alpha_{i_1,\dots,i_n}|,$$

then

$$|f(\beta_1, \dots, \beta_n)| \geq |\alpha_{1,\dots,1}||\beta_1|^{a_{11}} \cdots |\beta_n|^{a_{n1}} - \sum_{\substack{1\leq i_1\leq k_1\\ \cdots\cdots \\ 1\leq i_n\leq k_n \\ (i_1,\dots,i_n)\neq(1,\dots,1)}} |\alpha_{i_1,\dots,i_n}||\beta_1|^{a_{1i_1}} \cdots |\beta_n|^{a_{ni_n}} \tag{4.2}$$

$$\geq |\alpha_{1,\dots,1}||\beta_1|^{a_{11}} \cdots |\beta_n|^{a_{n1}} - \frac{|\beta_1|^{a_{11}} \cdots |\beta_n|^{a_{n1}}}{|\beta_i|} \sum_{\substack{1\leq i_1\leq k_1\\ \cdots\cdots \\ 1\leq i_n\leq k_n \\ (i_1,\dots,i_n)\neq(1,\dots,1)}} |\alpha_{i_1,\dots,i_n}|$$

$$\geq \frac{|\alpha_{1,\dots,1}||\beta_1|^{a_{11}} \cdots |\beta_n|^{a_{n1}}}{2}. \tag{4.3}$$

Note that if

$$|\beta_i| > 2^{\max\{k_1,\dots,k_n\}} \sum_{\substack{1\leq i_1\leq k_1\\ \cdots\cdots \\ 1\leq i_n\leq k_n}} |\alpha_{i_1,\dots,i_n}| \geq \frac{2}{|\alpha_{1,\dots,1}|} \sum_{\substack{1\leq i_1\leq k_1\\ \cdots\cdots \\ 1\leq i_n\leq k_n \\ (i_1,\dots,i_n)\neq(1,\dots,1)}} |\alpha_{i_1,\dots,i_n}|$$

for all $i = 1, \dots, n$, then the bound from (4.2) becomes larger than the bound from (4.1), and we obtain a contradiction. Hence $|\beta_i| \leq 2^{\max\{k_1,\dots,k_n\}} \sum_{\substack{1\leq i_1\leq k_1\\ \cdots\cdots \\ 1\leq i_n\leq k_n}} |\alpha_{i_1,\dots,i_n}|$ for some $i = 1, \dots, n$. To make a choice, we assume that this happens for $i = n$. Let

$$M = 2^{\max\{k_1,\ldots,k_n\}} \sum_{\substack{1\le i_1\le k_1 \\ \cdots\cdots \\ i\le i_n\le k_n}} |\alpha_{i_1,\ldots,i_n}|.$$

Thus $|\beta_n| < M$. Note that there are only finitely many elements in $\mathbf{A}$ of absolute value less than M. Next, we provide for each $i = 1, \ldots, n$ an upper bound for $|\beta_i|$. Fix β_n and let

$$f_n(\beta_1, \ldots, \beta_{n-1}) := f(\beta_1, \ldots, \beta_n).$$

Then

$$f_n(\beta_1, \ldots, \beta_{n-1}) = \sum_{\substack{1\le i_1\le k_1 \\ \cdots\cdots \\ 1\le i_{n-1}\le k_{n-1}}} A_{i_1,\ldots,i_{n-1}} \beta_1^{a_{1i_1}} \cdots \beta_{n-1}^{a_{n-1 i_{n-1}}},$$

where $A_{i_1,\ldots,i_{n-1}} = \sum_{1\le i_n\le k_n} \alpha_{i_1,\ldots,i_n} \beta_n^{a_{ni_n}} \in \mathbf{A}$. By replacing $\alpha_{i_1,\ldots,i_n}$ by $A_{i_1,\ldots,i_{n-1}}$ in the above argument, we deduce that there exists a number $M_1(\beta_n)$ depending on β_n, such that not all the numbers $|\beta_1|, \ldots, |\beta_{n-1}|$ are larger than $M_1(\beta_n)$. Let $M_1 = \max\{M_1(\beta_n) : |\beta_n| < M\}$. Thus at least one of the numbers $|\beta_1|, \ldots, |\beta_{n-1}|$ is less than M_1. Without any loss of generality we may assume that $|\beta_{n-1}| < M_1$. We now fix β_n, β_{n-1}, and let $f_{n-1}(\beta_1, \ldots, \beta_{n-2}) := f(\beta_1, \ldots, \beta_n)$. Then it follows that there exists $M_2(\beta_n, \beta_{n-1})$ such that not all the numbers $|\beta_1|, \ldots, |\beta_{n-2}|$ are larger than $M_2(\beta_n, \beta_{n-1})$. Let

$$M_2 = \max\{M_2(\beta_n, \beta_{n-1}) : |\beta_n| < M,\ |\beta_{n-1}| < M_1\}.$$

Then at least one of $|\beta_1|, \ldots, |\beta_{n-2}|$ is less than M_2. Without any loss of generality we may assume that $|\beta_{n-2}| < M_2$. By repeating the same argument, we conclude that there are M, M_1, M_2, ..., $M_{n-1} > 0$ such that any solution $(\beta_1, \ldots, \beta_n)$ satisfies the inequalities $|\beta_n| < M$, $|\beta_{n-1}| < M_1, \ldots, |\beta_1| < M_{n-1}$. We conclude that there are only finitely many n-tuples $(\beta_1, \ldots, \beta_n)$ satisfying the conditions from the statement of the theorem. □

References

[1] R. Guy, *Unsolved problems in number theory*, Springer-Verlag, NY. -Berlin, 1981, (2nd edition 1994).

[2] C. Pomerance, *Problem E2468*, Proposed by H. Ruderman, Amer. Math. Monthly **84** (1977), 59–60.

[3] S. Ramanujan, *Highly composite numbers*, Proc. London Math. Soc. **14** (1915), no. 2, 347–409.

[4] A. Schinzel, *On primitive prime factors of $a^n - b^n$*, Proc. Camb. Philos. Soc. **58** (1962), 555-562.

[5] Q. Sun and M. Zhang, *Pairs where $2^a - 2^b$ divides $n^a - n^b$ for all n*, Proc. Amer. Math. Soc. **93** (1985), 218–220.

[6] W. Y. Velez, *Problem E2468*, Proposed by H. Ruderman, Amer. Math. Monthly **83** (1976), 288–289.

[7] M. Vajaitu and A. Zaharescu, *A finiteness theorem for a class of exponential congruences*, Proc. Amer. Math. Soc. **127** (1999), 2225–2232.

Geumlan Choi and Alexandru Zaharescu
Mathematics Department
University of Illinois
1409 West Green Street
Urbana - Champaign, Illinois 61801, USA.
E-mail: g-choi1@math.uiuc.edu
zaharesc@math.uiuc.edu