

A FINITENESS THEOREM FOR A CLASS OF EXPONENTIAL CONGRUENCES

MARIAN VĂJĂITU AND ALEXANDRU ZAHARESCU

(Communicated by William W. Adams)

ABSTRACT. For given elements $\alpha_1, \dots, \alpha_k$ and β belonging to the ring of integers \mathcal{A} of a number field we consider the set of all k -tuples (a_1, \dots, a_k) in \mathbb{N}^k for which $\sum_{i=1}^k \alpha_i \beta^{a_i}$ divides $\sum_{i=1}^k \alpha_i z^{a_i}$ for any $z \in \mathcal{A}$, and prove under some reasonable assumptions that the set of solutions is finite.

The original motivation for this work comes from a problem raised by J. L. Selfridge (see Guy [1], problem B47) who asks for what pairs (a, b) does $2^a - 2^b$ divide $n^a - n^b$ for all integers n . A related (but more difficult) problem proposed by H. Ruderman asks to show that if $2^a - 2^b$ divides $3^a - 3^b$, then $2^a - 2^b$ divides $n^a - n^b$ for all integers n . This was investigated by B. Velez in [6]. While Ruderman's problem is still open, Selfridge's problem was solved by Pomerance [2], who combined results of Schinzel [4] with Velez's work. It turns out that there are exactly 14 solutions. The problem was also solved by Sun Qi and Zhang Ming Zhi [5].

In this paper we show that the above finiteness result is a particular case of a more general phenomenon.

Let \mathcal{K} be a number field, $\mathcal{A} = \mathcal{A}_{\mathcal{K}}$ its ring of integers and $\mathcal{U} = \mathcal{U}_{\mathcal{K}}$ its group of units. Let $\alpha_1, \dots, \alpha_k$ and β be nonzero elements of \mathcal{A} . We consider the set of all k -tuples (a_1, \dots, a_k) in \mathbb{N}^k for which

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

If $k = 1$ and β is a unit, (1) holds true for any a_1 . Therefore, if we want to obtain a general finiteness result we cannot allow β to be a unit. Even with this restriction on β the above set might be infinite, as we see in the following example: $\mathcal{A} = \mathbb{Z}$, $k = 3$, $\alpha_1 = 1$, $\alpha_2 = -\beta$, $\alpha_3 = 1$. Here we have infinitely many solutions of the form $a_1 = n$, $a_2 = n - 1$, $a_3 = 0$. For these solutions the moduli $\sum_{i=1}^3 \alpha_i \beta^{a_i}$ "degenerate". The same phenomenon appears in fact also in the original problem of Selfridge, where we have degenerate solutions $a = b$. To avoid such situations, in the following we shall only consider solutions to (1) which also satisfy

$$(2) \quad \sum_{i \in S} \alpha_i \beta^{a_i} \neq 0 \quad \text{for any } S \subseteq \{1, 2, \dots, k\}.$$

Received by the editors October 17, 1995 and, in revised form, May 20, 1997 and October 28, 1997.

1991 *Mathematics Subject Classification*. Primary 11A07.

©1999 American Mathematical Society

Then we have the following

Theorem 1. *Let \mathcal{A} be the ring of integers in an algebraic number field and let $\alpha_1, \dots, \alpha_k$ and β be nonzero elements of \mathcal{A} , β not a unit. Then there are only finitely many k -tuples (a_1, \dots, a_k) in \mathbb{N}^k satisfying (1) and (2) above.*

In case $\mathcal{U}_{\mathcal{K}}$ is finite (i.e. when $\mathcal{K} = \mathbf{Q}$ or \mathcal{K} is an imaginary quadratic number field) we can strengthen the conclusion of the above result.

Theorem 2. *Let \mathcal{A} be the ring of rational integers \mathbb{Z} or the ring of integers in an imaginary quadratic number field and let $\alpha_1, \dots, \alpha_k$ be nonzero elements of \mathcal{A} . Then there are only finitely many elements β in \mathcal{A} for which there exist a_1, \dots, a_k in \mathbb{N} , not all zero, satisfying (1) and (2) above.*

An upper bound for the absolute value of those β appearing in Theorem 2 is given by $|\beta| \leq 2^k \sum_{i=1}^k |\alpha_i|$. Theorem 1 is also effective, although in order to simplify the presentation we shall not compute explicit bounds for the solutions a_1, \dots, a_k . Theorem 1 is established by combining two main estimates which are obtained by quite different means. In the first of these arguments we establish lower bounds for the norm of those moduli $\sum_{i=1}^k \alpha_i \beta^{a_i}$ which satisfy (2). The second estimate, which is of independent interest, gives an upper bound for the norm of the ideal generated by the values of a polynomial at integer points.

1. A LOWER BOUND FOR $\left| \text{Norm} \left(\sum_{i=1}^k \alpha_i \beta^{a_i} \right) \right|$

Here and throughout the paper $\text{Norm}(\cdot)$ stands for $\text{Norm}_{\mathcal{K}/\mathbf{Q}}(\cdot)$.

The relation (1) says that $\sum_{i=1}^k \alpha_i \beta^{a_i}$ divides the ideal \mathcal{J} generated by the elements of the form $\sum_{i=1}^k \alpha_i z^{a_i}$ with $z \in A$. As a consequence, $\text{Norm} \left(\sum_{i=1}^k \alpha_i \beta^{a_i} \right)$ will divide $\text{Norm}(\mathcal{J})$. Now, if we can show that with finitely many exceptions we have

$$(3) \quad \left| \text{Norm} \left(\sum_{i=1}^k \alpha_i \beta^{a_i} \right) \right| > \text{Norm}(\mathcal{J}),$$

then Theorem 1 will be proved. In order to accomplish this goal we proceed to derive a lower bound for the left hand side and an upper bound for the right hand side of (3). In this section our object is to prove the following

Proposition 1. *Let \mathcal{A} be the ring of integers in an algebraic number field and let $\alpha_1, \dots, \alpha_k$ and β be nonzero elements of \mathcal{A} , β not a unit. Then there exists a constant $c = c(\alpha_1, \dots, \alpha_k, \beta, \mathcal{K}) > 0$ such that for any $(a_1, \dots, a_k) \in \mathbb{N}^k$ satisfying (2) we have*

$$(4) \quad \left| \text{Norm} \left(\sum_{i=1}^k \alpha_i \beta^{a_i} \right) \right| \geq c |\text{Norm}(\beta)|^{\max\{a_1, \dots, a_k\}}.$$

In order to prove this result we first establish the following

Lemma 1. *Let $\alpha_1, \dots, \alpha_k$ and β be nonzero complex numbers, $|\beta| \neq 1$. Then there exists a constant $c = c(\alpha_1, \dots, \alpha_k, \beta) > 0$ such that for any $(a_1, \dots, a_k) \in \mathbb{N}^k$ satisfying (2) we have*

$$(5) \quad \left| \sum_{i=1}^k \alpha_i \beta^{a_i} \right| \geq c \max\{|\beta|^{a_1}, \dots, |\beta|^{a_k}\}.$$

Remark 1. The statement would be false without the assumption $|\beta| \neq 1$. To see this, let $k = 2$, $\alpha_1 = 1$, $\alpha_2 = -1$ and $\beta = e^{2\pi i\theta}$ with $\theta \in \mathbb{R}$, θ irrational. Then one can take $a_2 = 0$ and use Dirichlet’s theorem to find an increasing sequence of a_1 ’s for which the left hand side of (5) decays at least as fast as $\frac{1}{a_1}$. Fortunately, we will not have to deal with this case in the sequel.

To derive Proposition 1 from Lemma 1 we apply (5) to $\sigma(\alpha_1), \dots, \sigma(\alpha_k), \sigma(\beta)$ for any embedding σ of K into \mathbb{C} .

The hypothesis (of Proposition 1) that “ β is not a unit” implies that $|\sigma(\beta)| \neq 1$ (which is needed for the hypothesis of Lemma 1). To see this note that if $|\sigma(\beta)| = 1$, then $\sigma(\beta)\overline{\sigma(\beta)} = 1$ and applying σ^{-1} to this gives $\beta\bar{\beta} = 1$, which implies that β is a unit, contradicting our hypothesis.

By multiplying the corresponding inequalities for all the σ we get

$$(6) \quad \left| \text{Norm} \left(\sum_{i=1}^k \alpha_i \beta^{a_i} \right) \right| \geq \prod_{\sigma} c(\sigma(\alpha_1), \dots, \sigma(\beta)) \prod_{\sigma} \max\{|\sigma(\beta)|^{a_1}, \dots, |\sigma(\beta)|^{a_k}\},$$

and we are done since the last product in (6) is not smaller than $|N(\beta)|^{\max\{a_1, \dots, a_k\}}$.

Proof of Lemma 1. Observe that the case $|\beta| < 1$ reduces to the case $|\beta| > 1$. For, it is enough to write the left hand side of (5) in terms of $\frac{1}{\beta}$, and then to multiply the inequality by an appropriate power of β .

Hence, let us suppose that $|\beta| > 1$. Dividing (5) through by $|\beta|^{\max\{a_1, \dots, a_k\}}$ and taking $b_i := \max\{a_1, \dots, a_k\} - a_i$ for each i , Lemma 1 states that if b_1, \dots, b_k are natural numbers, one of which is 0, then $|\sum_{i=1}^k \alpha_i \beta^{-b_i}| \geq c > 0$. If this is false, then there would exist an infinite sequence of natural numbers $\{b_{1,m}, \dots, b_{k,m}\}_{m \geq 0}$, with $\min_i b_{i,m} = 0$ for each m , such that

$$D_m := \sum_{i=1}^k \alpha_i \beta^{-b_{i,m}} \rightarrow 0, m \rightarrow \infty.$$

Now let I be the largest subset of $\{1, 2, \dots, k\}$ for which there exist natural numbers γ_i for each $i \in I$, and an infinite sequence of integers M , such that $b_{i,m} = \gamma_i$ for each $i \in I, m \in M$. Evidently nonempty such sets I must exist as there must be some integer i and some infinite subsequence of integers m with each $b_{i,m} = 0$ (since there is some such integer $i \in \{1, 2, \dots, k\}$ for every integer m).

Now, since I is the largest such set, we have $b_{i,m} \rightarrow \infty$ for each $i \notin I, m \in M$. Thus

$$D_m \rightarrow \sum_{i \in I} \alpha_i \beta^{-\gamma_i}, m \rightarrow \infty, m \in M.$$

However this is not 0 by (2), giving a contradiction.

2. AN UPPER BOUND FOR $\text{Norm}(\mathcal{J})$

Let \mathcal{A} be the ring of integers in an algebraic number field \mathcal{K} . Let $g(x) \in \mathcal{A}[x]$, $g(x) = \sum_{i=1}^k \alpha_i x^{a_i}$, where $\alpha_1 \neq 0$, $a_1 > a_2 > \dots > a_k$, $a = \max(a_1, 3)$, $\Delta = \prod_{i=2}^k (a_1 - a_i)$, and denote by $\mathcal{J} = \mathcal{J}(g)$ the ideal of \mathcal{A} generated by the set

$\{g(z): z \in \mathcal{A}\}$. Then we have the following

Proposition 2. *There are constants $c_1, c_2, c_3, c_4 > 0$, depending on k and \mathcal{K} only, such that*

$$Norm(\mathcal{J}) \leq c_1 |Norm(\alpha_1)|^{c_2} \exp\left(c_3 a^{\frac{c_4}{\log \log a}}\right).$$

The proof is based on Lemmas 2 and 3 below. From Lemma 2 one gets a bound for the norm of any prime ideal \mathcal{P} which divides \mathcal{J} . Then Lemma 3 gives a bound for the power of \mathcal{P} which enters into \mathcal{J} .

Lemma 2. *Let $\alpha_1, \dots, \alpha_k, a_1, \dots, a_k, g(x), \Delta$ and \mathcal{J} be as in Proposition 2, and let \mathcal{P} be a prime dividing \mathcal{J} . Then at least one of the following holds true:*

- (7) (i) \mathcal{P} divides α_1 ,
- (8) (ii) $Norm(\mathcal{P}) - 1$ divides Δ .

Proof. \mathcal{A}/\mathcal{P} is a finite field with $N(\mathcal{P}) = q = p^d$ elements, say. Since \mathcal{P} divides \mathcal{J} we know that for any z in \mathcal{A} $g(z)$ lies in \mathcal{P} . Let $r_i = 0$ if $a_i = 0$, and otherwise let r_i be the least positive residue of $a_i \pmod{q-1}$. Define $h(x) := \sum_{i=1}^k \alpha_i x^{r_i}$. For every $y \in \mathcal{A}/\mathcal{P}$ we have $y^q = y$, so that each $y^{r_i} = y^{a_i}$, and thus $h(y) = g(y) = 0$. Now, $h(x) (= \sum_{j=0}^q h_j x^j)$ has degree $< q$, and q distinct roots, and thus must vanish modulo \mathcal{P} . Thus for any l , we have $\sum_{i=1, a_i \equiv l \pmod{q-1}}^k \alpha_i = \sum_{j=0, j \equiv l \pmod{q-1}}^q h_j = 0$ in \mathcal{A}/\mathcal{P} . In particular, $\sum_{i=1, a_i \equiv a_1 \pmod{q-1}}^k \alpha_i \equiv 0 \pmod{\mathcal{P}}$. If there is some $i > 1$ with $a_i \equiv a_1 \pmod{q-1}$, then $q-1$ divides $a_i - a_1$ which divides Δ ; if there is no such i , then, from the line above, \mathcal{P} divides α_1 . This concludes the proof of the lemma.

Let $\alpha_1, \dots, \alpha_k, a_1, \dots, a_k, g(x)$ and Δ be as above. Let p be a prime number and \mathcal{P} a prime ideal of \mathcal{A} which lies over p . We denote by $e(\mathcal{P})$ the ramification index of \mathcal{P} and by $v_{\mathcal{P}}(z)$ the exponent of \mathcal{P} which enters in z , where z is any element or ideal of \mathcal{A} . Let $\tilde{\mathcal{J}} = \tilde{\mathcal{J}}(g)$ be the ideal generated by the set $\{g(z): z \in \mathcal{A} \setminus \mathcal{P}\}$. We have

Lemma 3.

$$(9) \quad v_{\mathcal{P}}(\tilde{\mathcal{J}}) \leq \left(1 + \frac{1}{Norm(\mathcal{P}) - 1}\right)^{k-1} \left(v_{\mathcal{P}}(\alpha_1 \Delta) + Norm(\mathcal{P})\right) - Norm(\mathcal{P}).$$

Proof. We proceed by induction. The result is clear if $k = 1$. In this case $\tilde{\mathcal{J}}$ is principal, generated by α_1 , and (9) becomes an equality. Let us take a general k . We want to reduce the number of terms in $g(x)$ to be able to use the induction hypothesis. To accomplish this the idea is to divide $g(x)$ by x^{a_k} and then take its derivative. Observe that $(\alpha_1 \Delta)$ is left unchanged by these operations. While the first operation produces no loss in (9), the second one might decrease its left hand side. We intend to show that the loss is not too big.

Let z be an arbitrary element in $\mathcal{A} \setminus \mathcal{P}$. We need to give a lower bound for $v_{\mathcal{P}}(f'(z))$, where $f(x) = g(x) x^{-a_k}$. At this point we fix a positive integer r whose value will be made explicit later. Further, we choose a positive integer m which we want to be as small as possible, satisfying the following property:

For any $y \in \mathcal{P}^m$ all the terms with $n > r$ in the Taylor expansion $f(z+y) = f(z) + f'(z)y + \dots + \frac{f^{(n)}(z)y^n}{n!} + \dots$ satisfy $v_{\mathcal{P}}\left(\frac{f^{(n)}(z)y^n}{n!}\right) \geq v_{\mathcal{P}}(\tilde{\mathcal{J}})$. Here $f(z) = \sum_i \alpha_i z^{b_i}$

(where $b_i = a_i - a_k$), and so one has $v_{\mathcal{P}}\left(\frac{f^{(n)}(z)}{n!}\right) \geq 0$. Therefore it is enough to choose an m such that for any $n > r$ we have

$$m n \geq v_{\mathcal{P}}(\tilde{\mathcal{J}}).$$

To insure this, we take m to be the smallest integer greater than or equal to $\frac{v_{\mathcal{P}}(\tilde{\mathcal{J}})}{r+1}$.

Now let y_1, \dots, y_r be distinct elements in \mathcal{P}^m . We consider the above Taylor expansions for y_1, \dots, y_r and put them in the form

$$\begin{cases} f'(z) y_1 + \dots + \frac{f^{(r)}(z) y_1^r}{r!} = t_1 \\ \vdots \\ f'(z) y_r + \dots + \frac{f^{(r)}(z) y_r^r}{r!} = t_r. \end{cases}$$

From our choice of m and the inequality $v_{\mathcal{P}}(f(z)) \geq v_{\mathcal{P}}(\tilde{\mathcal{J}})$ it follows that t_1, \dots, t_r satisfy $v_{\mathcal{P}}(t_j) \geq v_{\mathcal{P}}(\tilde{\mathcal{J}})$ for $j = 1, \dots, r$.

We treat this as a Vandermonde linear system in unknowns $f'(z), \dots, \frac{f^{(r)}(z)}{r!}$ and get from Cramer's rule

$$(10) \quad f'(z) = \frac{\begin{vmatrix} t_1 & y_1^2 & \dots & y_1^r \\ \vdots & \vdots & \dots & \vdots \\ t_r & y_r^2 & \dots & y_r^r \end{vmatrix}}{\prod_{i=1}^r y_i \prod_{1 \leq i < j \leq r} (y_j - y_i)}.$$

Here we do not want the denominator to be divisible by a high power of \mathcal{P} and for this reason we assume in what follows that the y_i 's lie in $\mathcal{P}^m \setminus \mathcal{P}^{m+1}$ and that their images in $\mathcal{P}^m / \mathcal{P}^{m+1}$ are distinct. Therefore we restrict the possible values of r to the set $\{1, \dots, Norm(\mathcal{P}) - 1\}$ and then the existence of such y_i 's is assured. Under these assumptions the exponent of \mathcal{P} in the denominator in (10) equals $mr + m \frac{r(r-1)}{2} = \frac{mr(r+1)}{2}$. On the other hand, in the numerator one can select \mathcal{P} to the power $v_{\mathcal{P}}(\tilde{\mathcal{J}})$ from the first column, \mathcal{P}^{2m} from the second column, and so on until we select \mathcal{P}^{rm} from the last column, which makes a total exponent of $v_{\mathcal{P}}(\tilde{\mathcal{J}}) + m \left(\frac{r(r+1)}{2} - 1\right)$. Thus

$$v_{\mathcal{P}}(f'(z)) \geq v_{\mathcal{P}}(\tilde{\mathcal{J}}) - m = \left[\frac{r}{r+1} v_{\mathcal{P}}(\tilde{\mathcal{J}})\right].$$

We now see that here we want r be as large as possible. Hence we take $r = Norm(\mathcal{P}) - 1$ and conclude that if $\tilde{\mathcal{J}}(f')$ denotes the ideal generated by the set $\{f'(z) : z \in \mathcal{A} \setminus \mathcal{P}\}$, then

$$v_{\mathcal{P}}(\tilde{\mathcal{J}}(f')) \geq \left[\left(1 - \frac{1}{Norm(\mathcal{P})}\right) v_{\mathcal{P}}(\tilde{\mathcal{J}}(g))\right].$$

From the induction hypothesis we get

$$v_{\mathcal{P}}(\tilde{\mathcal{J}}(f')) \leq \left(1 + \frac{1}{Norm(\mathcal{P}) - 1}\right)^{k-2} \left(v_{\mathcal{P}}(\alpha_1 \Delta) + Norm(\mathcal{P})\right) - Norm(\mathcal{P}).$$

On combining these estimates one derives immediately the required bound for $v_{\mathcal{P}}(\tilde{\mathcal{J}})$, which concludes the proof of the lemma.

Since $\mathcal{J}(g)$ divides $\tilde{\mathcal{J}}(g)$ one has the following

Corollary 1. *The inequality (9) holds true with $\tilde{\mathcal{J}}$ replaced by \mathcal{J} .*

We now take advantage of the fact that the right hand side of (9) as a function of \mathcal{P} , with \mathcal{K} , k and g fixed, is bounded: the coefficient of $v_{\mathcal{P}}(\alpha_1 \Delta)$ is bounded by 2^{k-1} and moreover the function $h(x) = \left(1 + \frac{1}{x-1}\right)^{k-1} x - x$ is bounded as $x \rightarrow \infty$. Taking these into account we infer the following

Corollary 2. *There are integers $c_5, c_6 > 0$ depending only on k and \mathcal{K} such that with the above notations we have $v_{\mathcal{P}}(\mathcal{J}) \leq c_6 v_{\mathcal{P}}(\alpha_1 \Delta)$ for any \mathcal{P} for which $v_{\mathcal{P}}(\mathcal{J}) \geq c_5$.*

Proof of Proposition 2. Let us decompose $\mathcal{J} = \mathcal{J}_1 \mathcal{J}_2$ where \mathcal{J}_1 contains those primes \mathcal{P} for which $v_{\mathcal{P}}(\mathcal{J}) < c_5$ and \mathcal{J}_2 those primes \mathcal{P} for which $v_{\mathcal{P}}(\mathcal{J}) \geq c_5$.

Then Corollary 2 shows that \mathcal{J}_2 divides $(\alpha_1 \Delta)^{c_6}$. As a consequence

$$\text{Norm}(\mathcal{J}_2) \leq |\text{Norm}(\alpha_1 \Delta)|^{c_6} = |\text{Norm}(\alpha_1)|^{c_6} |\Delta|^{c_6 [\mathcal{K}: \mathbb{Q}]}$$

Since $|\Delta| \leq a^{k-1} = \exp((k-1) \log a)$ and $\log a \leq \frac{c_4}{a^{\log \log a}}$ uniformly in a for c_4 large enough, one clearly has a bound of the required type for $\text{Norm}(\mathcal{J}_2)$. Now let $\mathcal{J}_0 = \prod_{\mathcal{P} | \mathcal{J}_1} \mathcal{P}$.

Since \mathcal{J}_1 divides $\mathcal{J}_0^{c_5}$ one has $\text{Norm}(\mathcal{J}_1) \leq (\text{Norm}(\mathcal{J}_0))^{c_5}$. Therefore we are done if we can provide a bound of the required type for \mathcal{J}_0 . In order to do this we first remove from \mathcal{J}_0 all the divisors of 2 (if there are any). Their product is “swallowed” by the constant c_1 anyway. We also remove from \mathcal{J}_0 any divisor of α_1 . Their product divides α_1 and then its norm is bounded by $|\text{Norm}(\alpha_1)|$.

Hence we are left with a square free divisor of \mathcal{J} , call it \mathcal{J}_3 , which is relatively prime to $2\alpha_1$. Now Lemma 2 implies that for any prime divisor \mathcal{P} of \mathcal{J}_3 , $\text{Norm}(\mathcal{P}) - 1$ divides Δ . One cannot derive from this that their product still divides Δ since the numbers $\text{Norm}(\mathcal{P}) - 1$ are by no means relatively prime. However, the fact that any positive divisor of Δ equals $\text{Norm}(\mathcal{P}) - 1$ for at most $[\mathcal{K}: \mathbb{Q}]$ prime ideals \mathcal{P} shows that $\prod_{\mathcal{P} | \mathcal{J}_3} (\text{Norm}(\mathcal{P}) - 1)$ divides $(\prod_{d | \Delta} d)^{[\mathcal{K}: \mathbb{Q}]}$, which equals $\Delta^{\frac{1}{2} [\mathcal{K}: \mathbb{Q}] \sigma_0(\Delta)}$, where $\sigma_0(\Delta)$ denotes the number of divisors of Δ .

For $\sigma_0(\Delta)$ one has the upper bound (see Ramanujan [3])

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

for any $\epsilon > 0$. At the same time observe that since $\text{Norm}(\mathcal{P}) \geq 3$ if \mathcal{P} divides \mathcal{J}_3 , one has crude inequalities of the type $\text{Norm}(\mathcal{P}) < (\text{Norm}(\mathcal{P}) - 1)^2$, therefore

$$\text{Norm}(\mathcal{J}_3) < \left(\prod_{\mathcal{P} | \mathcal{J}_3} (\text{Norm}(\mathcal{P}) - 1) \right)^2$$

When the above inequalities are combined we find a bound of required type for $\text{Norm}(\mathcal{J}_3)$. This concludes the proof of Proposition 2.

3. PROOF OF THEOREMS 1 AND 2

Proof of Theorem 1. Let (a_1, \dots, a_k) satisfy (1) and (2) with $a = \max\{a_1, \dots, a_k\}$, $a \geq 3$. We consider the polynomial $g(x) = \sum_{i=1}^k \alpha_i x^{a_i}$. Here some of the a_i 's might be equal but the corresponding coefficients cannot cancel in view of (2). In

particular $\deg(g(x)) = a$ and the leading coefficient α equals $\sum_{a_i=a} \alpha_i$. Now (1) says that $g(\beta)$ divides $\mathcal{J}(g)$. From (3), Proposition 1 and Proposition 2 one derives

$$(11) \quad c(\alpha_1, \dots, \alpha_k, \beta, \mathcal{K}) |Norm(\beta)|^a \leq c_1 |Norm(\alpha)|^{c_2} \exp\left(c_3 a \frac{c_4}{\log \log a}\right).$$

Since $|Norm(\beta)| > 1$ (11) clearly gives us an upper bound for a . Therefore the set of solutions (a_1, \dots, a_k) is finite, which concludes the proof of Theorem 1.

Proof of Theorem 2. We proceed by induction on k . The case $k = 1$ is clear. Let $k \geq 2$ and assume the result true for $1, 2, \dots, k - 1$. Fix $\alpha_1, \dots, \alpha_k$ in \mathcal{A} and let β be such that (1) and (2) are satisfied for nonnegative integers a_1, \dots, a_k not all zero. Two cases may appear:

(I) There exist $i, j \in \{1, \dots, k\}$, $i \neq j$, such that $a_i = a_j$. Then the numbers $a_1, \dots, a_{j-1}, a_{j+1}, \dots, a_k$ will satisfy (1) and (2) in which one keeps the same β and replaces the k -tuple $(\alpha_1, \dots, \alpha_k)$ by the $(k - 1)$ -tuple $(\alpha_1, \dots, \alpha_{i-1}, \alpha_i + \alpha_j, \dots, \alpha_{j-1}, \alpha_{j+1}, \dots, \alpha_k)$.

Therefore, by the induction hypothesis it follows that there are only finitely many β for which the above can happen.

(II) The numbers a_1, \dots, a_k are distinct. Suppose $a_1 > \dots > a_k$. We consider the polynomial $f(x) = \sum_{i=1}^k \alpha_i x^{a_i}$ and its relation with the following nonzero Vandermonde determinant:

$$\begin{vmatrix} 1 & \dots & 1 \\ 2^{a_1} & \dots & 2^{a_k} \\ \vdots & \vdots & \vdots \\ 2^{(k-1)a_1} & \dots & 2^{(k-1)a_k} \end{vmatrix}.$$

We add its columns multiplied by $\alpha_1, \dots, \alpha_k$ and obtain a new column that doesn't vanish and has $f(1), f(2), \dots, f(2^{k-1})$ as entries. Thus $f(r) \neq 0$ for some $r \in \{1, 2, \dots, 2^{k-1}\}$. We have

$$(12) \quad |f(r)| \leq \sum_{i=1}^k |\alpha_i| 2^{(k-1)a_i} < 2^{(k-1)a_1} \sum_{i=1}^k |\alpha_i|.$$

On the other hand, if $|\beta| \geq \frac{2^{\sum_{2 \leq i \leq k} |\alpha_i|}}{|\alpha_1|}$, then

$$\left| \sum_{2 \leq i \leq k} \alpha_i \beta^{a_i} \right| \leq \sum_{2 \leq i \leq k} |\alpha_i| |\beta|^{a_i} \leq \frac{|\alpha_1| |\beta|^{a_1}}{2}$$

and this implies

$$(13) \quad |f(\beta)| \geq \frac{|\alpha_1| |\beta|^{a_1}}{2}.$$

The rings \mathcal{A} under consideration have the property that the absolute value of any nonzero element of \mathcal{A} is ≥ 1 . Therefore the divisibility $f(\beta) | f(r)$ implies the inequality $|f(\beta)| \leq |f(r)|$. But the right hand side in (13) is larger than that of (12) if $|\beta|$ is large enough, for example if $|\beta| > 2^k \sum_{i=1}^k |\alpha_i| \geq \frac{2^k \sum_{i=1}^k |\alpha_i|}{|\alpha_1|}$, and this completes the proof of Theorem 2.

We note that in the above proof one can replace “2” in the Vandermonde determinant by any element of \mathcal{A} that is not a root of unity.

ACKNOWLEDGEMENT

We thank the referee for the numerous suggestions in improving the presentation of this paper.

REFERENCES

- [1] R. Guy, *Unsolved problems in Number Theory*, Springer-Verlag, New York-Berlin, (1981), (second edition 1994). MR **83k**:10002; MR **96e**:11002
- [2] C. Pomerance, *Amer. Math. Monthly* **84** (1977), 59–60.
- [3] S. Ramanujan, *Highly composite numbers*, *Proc. London Math. Soc.* (2) **14** (1915).
- [4] A. Schinzel, *On primitive prime factors of $a^n - b^n$* , *Proc. Cambridge Philos. Soc.* **58** (1962), 555–562. MR **26**:1280
- [5] Sun, Qi and Zhang Ming Zhi, *Pairs where $2^a - 2^b$ divides $n^a - n^b$ for all n* , *Proc. Amer. Math. Soc.* **93** (1985), 218–220. MR **86c**:11004
- [6] B. Velez, *Amer. Math. Monthly* **83** (1976), 288–289.

INSTITUTE OF MATHEMATICS OF THE ROMANIAN ACADEMY, P.O.Box 1-764, 70700 BUCHAREST, ROMANIA

E-mail address: `mvajaitu@stoilow.imar.ro`

MASSACHUSETTS INSTITUTE OF TECHNOLOGY, DEPARTMENT OF MATHEMATICS, 77 MASSACHUSETTS AVENUE, CAMBRIDGE, MASSACHUSETTS 02139

E-mail address: `azah@math.mit.edu`

Current address: Department of Mathematics and Statistics, McGill University, Burnside Hall, 805 Sherbrooke Street West, Montreal, Quebec, Canada H3A 2K6