THE PROUHET-TARRY-ESCOTT PROBLEM, INDECOMPOSABILITY OF POLYNOMIALS AND DIOPHANTINE EQUATIONS

L. HAJDU, Á. PAPP, AND R. TIJDEMAN

Abstract. In this paper we show how the subjects mentioned in the title are related. First we study the structure of partitions of $A \subseteq \{1, \dots, n\}$ in k-sets such that the first $k-1$ symmetric polynomials of the elements of the k-sets coincide. Then we apply this result to derive a decomposability result for the polynomial $f_A(x) := \prod_{x \in A}(x-a)$. Finally we prove two theorems on the structure of the solutions (x, y) of the Diophantine equation $f_A(x) = P(y)$ where $P(y) \in \mathbb{Q}[y]$ and on shifted power values of $f_A(x)$.

1. Introduction

The Prouhet-Tarry-Escott problem, shortly PTE, asks to describe disjoint pairs A and B of sets of integers such that their first k power sum symmetric polynomials are equal (cf. [17]). For example, if

$$A = \{2, 3, 7\} \quad \text{and} \quad B = \{1, 5, 6\}$$

then we can take $k = 2$, since we have

$$2 + 3 + 7 = 1 + 5 + 6 \quad \text{and} \quad 2^2 + 3^2 + 7^2 = 1^2 + 5^2 + 6^2. \tag{1}$$

In this paper we connect the PTE problem, and the question for which polynomials $f(x), g(x) \in \mathbb{Z}[x]$ the equation $f(x) = g(y)$ has infinitely many solutions $(x, y) \in \mathbb{Z}^2$ if the zeros of f are simple and form (almost) an arithmetical progression. Both problems have attracted a lot of attention. Already at this point we mention that the latter

2010 *Mathematics Subject Classification.* 11P05, 11B75, 11D41.

Key words and phrases. Partitions of $\{1, \dots, n\}$, symmetric polynomials, the Prouhet-Tarry-Escott problem, products of consecutive integers, indecomposability of polynomials, polynomial values.

Research of L.H. supported in part by the NKFIH grants 115479, 128088, and 130909, and the projects EFOP-3.6.1-16-2016-00022 and EFOP-3.6.2-16-2017-00015 co-financed by the European Union and the European Social Fund. Research of Á. P. was supported by the ÚNKP-20-3 New National Excellence Program of the Ministry for Innovation and Technology from the source of the National Research, Development and Innovation Fund.

question (through a deep result of Bilu and Tichy [4]) is closely related to decomposabilty of polynomials. A polynomial $f(x) \in \mathbb{Q}[x]$ is decomposable if we can write $f(x) = h_1(h_2(x))$ with $h_1, h_2 \in \mathbb{Q}[x]$, in a nontrivial way. (Later we shall give the precise notion.) For example,

$$f(x) = (x-1)(x-2)(x-3)(x-5)(x-6)(x-7)$$

is decomposable, since as one can readily check we have $f(x) = h_1(h_2(x))$ with

$$(2)\quad h_1(x) = (x-2\cdot3\cdot7)(x-1\cdot5\cdot6),\ h_2(x) = (x-2)(x-3)(x-7)+2\cdot3\cdot7.$$

The similarity of (1) and (2) is not a coincidence; in this paper we show the general connections between these properties. In Sections 1 and 2, we outline the studied problems, the established link and the results we obtain. The proofs of our theorems are given in Sections 3-5.

The starting point of our study was a question of Benne de Weger. There is an extensive literature on binomial coefficients which are equal or differ by a small or fixed constant (see e.g. [12, 23, 25] and the references there). In the latter paper the authors study the related Diophantine equation

$$\binom{f_1(x)}{k} + \binom{x}{2} = \binom{f_2(x)}{2},$$

in polynomials $f_1, f_2 \in \mathbb{Q}[x]$ with $\deg f_1 = 2$, $\deg f_2 = k$. Benne de Weger remarked that this equation leads to the following problem (private communication).

Problem 1. *Let $k \geq 1$. Describe the values of k for which it is possible to partition the set $\{1, \dots, 2k+1\}$ into a singleton A_0 and two sets A_1 and A_2 with $k = |A_1| = |A_2|$, such that the symmetric polynomials $\sigma_1, \dots, \sigma_{k-1}$ of the elements of A_1 and of A_2 coincide.*

This is the PTE-problem for $n = 2k+1$. De Weger added that he had solutions for $k = 1, 2, 3$ and had proved that there are none for $4 \leq k \leq 14$. A solution for $k = 3$ is $A = \{2, 3, 7\}$, $B = \{1, 5, 6\}$. Indeed we have

$$2+3+7 = 1+5+6,$$

and, by (2),

$$2\cdot3+2\cdot7+3\cdot7 = \frac{(2+3+7)^2-(2^2+3^2+7^2)}{2} = \\ = \frac{(1+5+6)^2-(1^2+5^2+6^2)}{2} = 1\cdot5+1\cdot6+5\cdot6.$$

Problem 1 was solved independently by Aart Blokhuis (private communication) and by the third author of the present paper (see Corollary 3.1).

In this paper we study the following more general problem.

Problem 2. *Let r be a fixed non-negative integer. Describe those positive integers n for which the set $\{1, \dots, n\}$ can be partitioned into sets $A_0, A_1, \dots, A_t$ with $t \geq 2$, $|A_0| = r$ and*

$$k := |A_1| = \dots = |A_t| \geq 2$$

such that all the symmetric polynomials $\sigma_1, \dots, \sigma_{k-1}$ of the elements of the A_i $(i = 1, \dots, t)$ coincide.

The problem asks: is it possible to omit a 'few' elements from the set $\{1, \dots, n\}$ such that the remaining set can be split into t subsets which have pairwise the PTE-property? Observe that Problem 1 is the special case $r = 1$, $t = 2$.

In Theorem 2.1 we show that if r is small enough with respect to n, then only $k = 2$ is possible and $A_1, A_2, \dots, A_t$ are symmetric. We call a set $A = \{a_1, \dots, a_k\} \subset \mathbb{R}$ with $a_1 < \dots < a_k$ symmetric if the sums $a_i + a_{k+1-i}$ $(i = 1, \dots, k)$ are all equal. It is obvious that such a symmetry implies a PTE-structure.

Next we establish a new link between PTE-problems and the indecomposability of certain polynomials. We recall some standard notions. Let K be a field and $f \in K[x]$. Then f is called decomposable (or composite) over K if there exists $h_1, h_2 \in K[x]$ such that

$$f(x) = h_1(h_2(x)) \quad (h_1, h_2 \in K[x],\ \deg h_1 > 1, \deg h_2 > 1).$$

Otherwise f is called indecomposable. If $f(x) = h_1(h_2(x))$ and $\lambda(x) \in K[x]$ is a linear polynomial, then $f(x) = h_3(h_4(x))$ with $h_3(x) = h_1(\lambda^{-1}(x))$ and $h_4(x) = \lambda(h_2(x))$ is another decomposition of $f(x)$. In the sequel we do not distinguish between such equivalent decompositions. Further, we consider the polynomials $f(x), f(\lambda(x))$, as well as the polynomials $f(x), \lambda(f(x))$ to be equivalent. There is a vast literature on (in)decomposability of polynomials (see e.g. [2, 4, 5, 7, 10, 11, 18] and the references there). In Theorem 2.2 we show that the studied variant of the PTE problem is equivalent to asking for the indecomposability of certain polynomials.

Using this connection, we show in Corollary 2.1 for given integers $n > r \geq 0$ with r small enough with respect to n that if for $A \subseteq \{1, \dots, n\}$ with $|A| = n - r$ the polynomial

$$f_{A,c,d}(x) := \prod_{a \in A} (x - c - ad), \quad c, d \in \mathbb{Q},\ d \neq 0 \tag{3}$$

is decomposable over $\mathbb{Q}$ as $h_1(h_2(x))$, then h_1 and h_2 can be given explicitly. Note that the polynomial $f_{A,c,d}(x)$ represents the product with terms of an arithmetic progression of length n with r terms missing. For example, if

$$f_A(x) := f_{A,0,1}(x) = (x-1)(x-2)(x-3)(x-4)(x-6)(x-7)(x-8)(x-9)$$

is decomposable as $h_1(h_2(x))$, then, apart from equivalence,

$$h_2(x) = x^2 - 10x,\ h_1(x) = (x+9)(x+16)(x+21)(x+24).$$

Next, using the above results, we establish a finiteness theorem for the number of times that a polynomial $f_{A,c,d}$ of the form (3) assumes a value which is also assumed by a given polynomial P with rational coefficients. Related problems are investigated in the papers [2, 3, 15, 26] for consecutive integers and in [14] for arithmetic progressions with at most one term missing. Generalizing and extending many of the above mentioned results, in Theorem 2.3 we provide a finiteness result for the number of values of $f_{A,c,d}$ also taken by another polynomial $P(x) \in \mathbb{Q}[x]$. This result, similarly to the above mentioned ones, is ineffective.

Finally, we consider shifted power values (i.e. values of the shape $ay^\ell + b$) of $f_{A,c,d}$. Related problems have been investigated by many authors. We recall some important results. (For a more detailed survey see e.g. the introduction of [14].) A celebrated result of Erdős and Selfridge [9] says that the product of two or more consecutive positive integers is never a perfect power. Papers of Erdős [8] and Győry [13] give similar results for binomial coefficients. A recent result of Bennett and Siksek [1] states that if the number k of terms of the arithmetic progression is fixed and large enough, then there are only finitely many instances that the product yields a perfect power. For results with $r = 1$ (just one term missing), see e.g. [19, 20] (for consecutive integers) and [21] (for general arithmetic progressions). In the equation $f_{A,c,d}(x) = ay^\ell + b$ we give an effective upper bound for the exponent ℓ and for the integer values x, y for which this equation holds, in Theorem 2.4. This result implies for example that for every integer $n \geq 24$ and rational numbers a, b with $a \neq 0$ there exists an effectively computable number C such that the equation $f_A(x) = ay^\ell + b$ with $A \subset \{1, 2, \dots, n\}$, $|A| = n-2$ implies $\max(|x|, |y|, \ell) < C$.

Our results make a step forward towards the solution of the problem how much one can ‘mutilate’ an arithmetic progression such that the corresponding product of terms still can take only finitely many values of a given polynomial, or shifted power values.

2. Results

In connection with Problem 2 we prove the following result.

Theorem 2.1. *Let n, r be non-negative integers with*

$$n > 2r^{3/2} + 5r + 8. \tag{4}$$

Then every decomposition of $\{1, \dots, n\}$ as in Problem 2 has the following structure. Putting $A := \{1, \dots, n\} \setminus A_0$ with $r = |A_0|$, we have $k = 2$, and all classes $A_i = \left\{a_1^{(i)}, a_2^{(i)}\right\}$ $(i = 1, \dots, t)$ are symmetric with respect to

$$\bar{a} := \frac{1}{n-r} \sum_{a \in A} a \tag{5}$$

that is,

$$a_1^{(i)} + a_2^{(i)} = 2\bar{a} \quad (i = 1, \dots, t).$$

Remark 1. Theorem 2.1 yields a complete answer to Problem 2 for every $n > 2r^{3/2} + 5r + 8$. On the other hand, for any r and n with $n - r$ even, if $A = \{1, \dots, n\} \setminus A_0$ is symmetric with respect to $\bar{a}$ (i.e. $a \in A$ implies that $2\bar{a} - a \in A$), then we have a partition as in Problem 2 with $k = 2$.

Remark 2. The following extension of Theorem 2.1 is also valid. Let $b_1, \dots, b_n$ be a non-constant arithmetic progression in $\mathbb{Q}$. Put $B = \{b_1, \dots, b_n\}$ and suppose that $B_0, B_1, \dots, B_t$ is a partition of B such that $r := |B_0|$, $k := |B_1| = \dots = |B_t|$, $n > 2r^{3/2} + 5r + 8$ and for all $i = 1, \dots, t$ the symmetric polynomials $\sigma_1, \dots, \sigma_{k-1}$ of the elements of B_i $(i = 1, \dots, t)$ are the same. Then $k = 2$ and writing $B_i = \{b_1^{(i)}, b_2^{(i)}\}$ $(i = 1, \dots, t)$ we have

$$b_1^{(i)} + b_2^{(i)} = b_1^{(j)} + b_2^{(j)} \quad (1 \le i, j \le t).$$

Indeed, writing $b_s = c + da_s$ with $a_s \in A \setminus A_0$ and $c, d \in \mathbb{Q}$, $d \neq 0$, it can be easily seen by induction on n that c can be taken to be zero. Then clearly, we may take $d = 1$, and the claim follows.

The next result establishes a link between partitions as in Problem 2 and decomposability of certain polynomials.

Theorem 2.2. *Let n be a positive integer and r a non-negative integer. Then there exists a partition $A_0, A_1, \dots, A_t$ of $\{1, \dots, n\}$ as in Problem 2 if and only if there exists an $A \subseteq \{1, \dots, n\}$ with $|A| = n - r$ such that the polynomial*

$$f_A(x) = \prod_{a \in A} (x - a) \tag{6}$$

is decomposable over $\mathbb{Q}$. In particular, if $A_0, A_1, \ldots, A_t$ is a partition of the required type, then $f_A(x) = h_1(h_2(x))$ with $A = \{1, \ldots, n\} \setminus A_0$ and

$$h_2(x) = \prod_{a \in A_1} (x - a) - \prod_{a \in A_1} (-a)$$

and

$$h_1(x) = \left(x + \prod_{a \in A_1} (-a) \right) \cdots \left(x + \prod_{a \in A_t} (-a) \right).$$

Remark 3. From the proof of the theorem it will be clear that in fact h_2 is independent of which A_i we use in its definition.

As a simple consequence of Theorems 2.1 and 2.2 we obtain the following statement.

Corollary 2.1. *Let $A \subseteq \{1, \ldots, n\}$ with $|A| = n - r$ where n and r are integers with $r \geq 0$ and $n > 2r^{3/2} + 5r + 8$. Further, let $c, d \in \mathbb{Q}$ with $d \neq 0$. Then the polynomial*

$$f_{A,c,d}(x) = \prod_{a \in A} (x - c - ad) \tag{7}$$

is decomposable over $\mathbb{Q}$ if and only if $n - r$ is even and A is symmetric with respect to

$$\bar{a} := \frac{1}{n - r} \sum_{a \in A} a,$$

when (up to equivalence) the only decomposition of $f_{A,c,d}(x)$ is given by $f_{A,c,d}(x) = \varphi^*((\frac{x-c}{d} - \bar{a})^2)$ with

$$\varphi^*(x) = d^{n-r} h_1 \left(x - \bar{a}^2 \right). \tag{8}$$

Here h_1 is the polynomial defined in Theorem 2.2 corresponding to the partition $A_1, \ldots, A_t$ of A with $|A_1| = |A_2| = \cdots = |A_t| = 2$.

Next we apply our results to the equation $f_{A,c,d}(x) = P(y)$ where P is a given polynomial. The first theorem of this type is general, but ineffective: it only guarantees the finiteness of the number of integral solutions.

Theorem 2.3. *Let $A \subseteq \{1, \ldots, n\}$ with $|A| = n - r$ for integers $r \geq 0$ and $n > 2r^{3/2} + 5r + 8$ and let $c, d \in \mathbb{Q}$ with $d \neq 0$. Let $f_{A,c,d}(x)$ be as in (7) and let $P(y) \in \mathbb{Q}[y]$ with $\deg P \geq 2$. Then the equation*

$$f_{A,c,d}(x) = P(y) \tag{9}$$

has only finitely many integer solutions x, y, unless we are in one of the following cases:

(i) $P(y) = f_{A,c,d}(T(y))$, *where* T *is an arbitrary non-constant polynomial with rational coefficients,*
(ii) $P(y) = \varphi^*(Q(y))$, *where* φ^* *is given by* (8) *and* Q *is a non-constant polynomial with rational coefficients having at most two roots of odd multiplicities.*

Remark 4. In cases (i) and (ii) one can easily give examples where equation (9) has infinitely many integer solutions x, y.

If the right hand side of (9) is of the shape $ay^\ell + b$ where ℓ is also unknown, then we can give an effective result.

Theorem 2.4. *Let* $A \subseteq \{1, \dots, n\}$ *with* $|A| = n-r$ *with integers* $r \geq 0$ *and* $n > 2r^{3/2} + 5r + 8$ *and let* $c, d \in \mathbb{Q}$ *with* $d \neq 0$. *Let* $f_{A,c,d}(x)$ *be given by* (7) *and let* $a, b \in \mathbb{Q}$ *with* $a \neq 0$. *Then all solutions of the equation*

$$f_{A,c,d}(x) = ay^\ell + b \tag{10}$$

in integers x, y, ℓ *with* $\ell \geq 2$ *satisfy* $\max(|x|, |y|, \ell) < C$ *for some effectively computable constant* C *depending only on* a, b, c, d, n. *Here we use the convention that for* $|y| \leq 1$ *we have* $\ell \leq 3$.

3. Proofs of results of Prouhet-Tarry-Escott type

Proof of Theorem 2.1. Throughout the proof, we shall use the earlier notation: $r = |A_0|$ stands for the number of 'missing elements' from $\{1, \dots, n\}$, $A_0, A_1, \dots, A_t$ form a partition of $\{1, \dots, n\}$ with the prescribed properties and

$$k = |A_1| = \dots = |A_t|.$$

In particular, we have $n - r = tk$. Observe that (4) implies that $n - 1 > 2(r-1)^{3/2} + 5(r-1) + 8$ for $r > 0$. Therefore, by induction on r, we may assume without loss of generality that $n \in A$.

We shall frequently use the identity

$$\sum_{i=j}^{I} \binom{i}{j} = \binom{I+1}{j+1},$$

valid for all $j \geq 0$. Also, we shall make use of the fact that it follows from the conditions of the theorem by induction on h that

$$\sum_{a \in A_i} \binom{a+\ell}{h} = \sum_{a \in A_j} \binom{a+\ell}{h} \quad \text{for } h = 0, 1, \dots, k-1 \text{ and all } i, j. \tag{11}$$

As we shall see, our choice of ℓ will depend on the parity of k.

Suppose first k is odd. Then $k \geq 3$. We choose $\ell = -r-2$ in (11) and let

$$f(x) = \binom{x-r-2}{k-1}.$$

Since $\deg f = k-1$, by our assumptions we have

$$\sum_{a \in A_i} f(a) = \sum_{a \in A_j} f(a) \quad (1 \leq i, j \leq t).$$

Recall that $A = A_1 \cup \cdots \cup A_t$ and $n \in A$. Observe that

$$f(1) = \binom{k+r-1}{k-1},\ f(2) = \binom{k+r-2}{k-1}, \dots, f(r+1) = \binom{k-1}{k-1}.$$

Thus we have

$$\sum_{a \in A} f(a) \leq \sum_{i=k-1}^{n-r-2} \binom{i}{k-1} + \sum_{i=k-1}^{k+r-1} \binom{i}{k-1} = \binom{n-r-1}{k} + \binom{k+r}{k}.$$

Hence for any j with $1 \leq j \leq t$ we get

(12)

$$\sum_{a \in A_j} f(a) \leq \frac{\binom{n-r-1}{k} + \binom{k+r}{k}}{t} = \frac{n-r-1}{n-r}\binom{n-r-2}{k-1} + \frac{k}{n-r}\binom{k+r}{k}.$$

On the other hand, assuming without loss of generality that $n \in A_1$, we also have

$$\sum_{a \in A_1} f(a) \geq \binom{n-r-2}{k-1}. \tag{13}$$

Combining (12) and (13), we obtain

$$k\binom{k+r}{k} \geq \binom{n-r-2}{k-1}.$$

Since $k \geq 3$, we can rewrite this inequality as

$$(r+1)(r+2)(r+3)\prod_{i=1}^{k-3}(r+3+i) \geq$$

$$\geq (n-r-2)(n-r-3)\prod_{i=1}^{k-3}(n-r-k-1+i).$$

We show that it is impossible. On the one hand, in view of $k \leq (n-r)/2$ and (4), we have

$$n-r-k-1+i > r+3+i \quad (i = 1, \dots, k-3).$$

On the other hand, we get from (4) that

$$(r+1)(r+2)(r+3) < (n-r-2)(n-r-3). \tag{14}$$

This yields a contradiction, which proves our claim for k odd.

Suppose k is even and $k \geq 4$. Here we choose $\ell = -2r-2$ in (11) and let

$$f(x) = \binom{x-2r-2}{k-1}.$$

Since $\deg f = k-1$, by our assumptions we have

$$\sum_{a \in A_i} f(a) = \sum_{a \in A_j} f(a) \quad (1 \leq i, j \leq t).$$

Observe that the negative values of f are

$$f(1) = -\binom{k+2r-1}{k-1},\ f(2) = -\binom{k+2r-2}{k-1}, \ldots, f(2r+1) = -\binom{k-1}{k-1}.$$

Thus we have

$$\sum_{a \in A, f(a)<0} |f(a)| \leq \sum_{i=k-1}^{k+2r-1} \binom{i}{k-1} = \binom{k+2r}{k}. \tag{15}$$

Furthermore,

$$\sum_{a \in A, f(a) \geq 0} f(a) \leq \sum_{i=2r+2}^{n} \binom{i-2r-2}{k-1} = \sum_{j=0}^{n-2r-2} \binom{j}{k-1} = \binom{n-2r-1}{k}.$$

Hence for any j with $1 \leq j \leq t$ we get

$$\sum_{a \in A_j} f(a) \leq \frac{\binom{n-2r-1}{k}}{t} = \frac{n-2r-1}{n-r} \binom{n-2r-2}{k-1}. \tag{16}$$

On the other hand, assuming without loss of generality that $n \in A_1$, we also have, by (15),

$$\sum_{a \in A_1} f(a) \geq \binom{n-2r-2}{k-1} - \binom{k+2r}{k}. \tag{17}$$

Combining (16) and (17), we obtain

$$(n-r)\binom{k+2r}{k} \geq (r+1)\binom{n-2r-2}{k-1}.$$

Since $k \geq 4$, we can rewrite this inequality as

$$(n-r)(2r+1)(2r+2)(2r+3)(2r+4)\prod_{i=1}^{k-4}(2r+4+i) \geq$$

$$\geq k(r+1)(n-2r-2)(n-2r-3)(n-2r-4)\prod_{i=1}^{k-4}(n-2r-k-1+i).$$

We show that it is impossible. In view of $k \leq (n-r)/2$ and (4), we have

$$n-2r-k-1+i > 2r+4+i \quad (i=1,\dots,k-4).$$

On using $k \geq 4$ and writing $m = n-2r$ it follows that

$$(m+r)(2r+1)(2r+3)(r+2) > (m-2)(m-3)(m-4). \tag{18}$$

Since (4) implies $m > 2r^{3/2}+3r+8$, this yields a contradiction.

Finally, let $k=2$. Then we have $t=(n-r)/2$; in particular, $n-r$ is even. That is, we have pairs of elements of A having the same sum. Obviously, this is possible only if we take the largest number with the smallest one, and so on, so the pairs are symmetric with respect to $\bar{a}$. □

Corollary 3.1. *The only solution of Problem* 1 *with* $k>2$ *is for* $n=7$.

Proof. We apply the proof of Theorem 2.1 with $r=1$ and $t=2$. It follows that $k=2$ if $n>15$. On the other hand, n has to be odd and if $k>2$, then $n \geq 7$. Hence it remains to check the odd values of n between 7 and 15.

If $n = 15, 13, 11$ or 9, then $k=(n-1)/2$ and we apply (11) with $h=k-1, \ell=-3$. If $n \neq 9$, then the largest coefficient $\binom{2k-2}{k-1}$ is larger than the sum of the absolute values of the other $2k$ binomial coefficients. Hence the sums in (11) cannot be equal. If $n=9$, the largest binomial coefficient, $\binom{6}{3}=20$, is equal to the sum of the absolute values of the other terms. It follows that $9,1,2 \in A_1$ and $8,7,6 \in A_2$. However, when applying (11) with $h=1, \ell=-3$ we see that the sum of the elements in A_2 exceeds that of A_1 for all possible choices of the remaining elements 3, 4 and 5.

If $n=7$, choose $A_0=\{4\}, A_1=\{2,3,7\}, A_2=\{1,5,6\}$. This is the only valid choice. □

Remark 5. Remark 2 implies that the symmetric polynomials σ_1, σ_2 of $1,2,6$ and of $0,4,5$, and also of $3,5,13$ and of $1,9,11$, coincide too.

4. Proofs of results on indecomposability

Proof of Theorem 2.2. Let $A_0, A_1, \ldots, A_t$ be a partition as stated in Problem 2. Put $A = \{1, \ldots, n\} \setminus A_0$ and let f_A, h_1, h_2 be as in the theorem. We want to show that $f_A(x) = h_1(h_2(x))$. If two polynomials of degree $n-r$ have the same values at $n-r+1$ points, then they coincide. It is clear that $f_A(0) = h_1(h_2(0)) = \prod_{a\in A}(-a)$ and that both $f_A(x)$ and $h_1(h_2(x))$ have all $a \in A_1$ as roots. In view of

$$\prod_{a\in A_1}(x-a) - \prod_{a\in A_1}(-a) = \prod_{a\in A_i}(x-a) - \prod_{a\in A_i}(-a)$$

for $2 \le i \le t$, we see that every $a \in A$ is both a root of $f_A(x)$ and of $h_1(h_2(x))$. Thus $f_A(x)$ and $h_1(h_2(x))$ assume the same value at $n-r+1$ points, hence $f_A = h_1(h_2)$. This proves the "only if" statement and the second statement of the theorem.

To prove the "if" statement, let $A \subseteq \{1, \ldots, n\}$ with $|A| = n-r$, and suppose that $h_1(h_2)$ is a decomposition of f_A with $h_1, h_2 \in \mathbb{Q}[x]$. Clearly, we may assume that both h_1 and h_2 are monic polynomials. Set $h_1(x) = (x-\alpha_1)\ldots(x-\alpha_t)$ with $\alpha_1, \ldots, \alpha_t \in \mathbb{C}$. Observe that these roots are pairwise distinct. Then

$$\prod_{a\in A}(x-a) = h_1(h_2(x)) = (h_2(x)-\alpha_1)\cdots(h_2(x)-\alpha_t).$$

Let A_i consist of the roots of the polynomial $h_2(x) - \alpha_i$ $(i = 1, \ldots, t)$. Then all the symmetric polynomials of the elements of A_i for $i = 1, \ldots, t$ coincide. So putting $A_0 = \{1, \ldots, n\} \setminus A$, the sets $A_0, A_1, \ldots, A_t$ form a partition as in Problem 2. □

Proof of Corollary 2.1. Clearly, by

$$f_{A,c,d}(x) = d^{n-r}\prod_{a\in A}\left(\frac{x-c}{d} - a\right) = d^{n-r} f_A\left(\frac{x-c}{d}\right),$$

$f_{A,c,d}$ and f_A are equivalent and therefore have equivalent decompositions. It follows from Theorems 2.2 and 2.1 that $f_{A,c,d}$ is decomposable if and only if $n-r$ is even, each partition set A_i has two elements, $a_1^{(i)}$ and $a_2^{(i)}$ for $i = 1, \ldots, t$, say, the set A is symmetric with respect to $\bar{a}$ and (5) holds.

To get the specific decomposition observe that

$$(x-a_1^{(i)})(x-a_2^{(i)}) - a_1^{(i)}a_2^{(i)} = (x-\overline{a})^2 - \overline{a}^2$$

for $i = 1, \ldots, n$. Thus, using the decomposition $f_A = h_1(h_2)$ with h_1, h_2 as in Theorem 2.2, we have

$$f_{A,c,d}(x) = d^{n-r} h_1 \left(h_2 \left(\frac{x-c}{d} \right) \right) = d^{n-r} h_1 \left(\left(\frac{x-c}{d} - \overline{a} \right)^2 - \overline{a}^2 \right),$$

so choosing $\varphi^*(x) = d^{n-r} h_1(x - \overline{a}^2)$ we obtain the decomposition as given in the theorem.

To prove the uniqueness let $f_A(x) = P(Bx^2 + Cx + D)$ any decomposition of $f_A(x)$ with $P(x) \in \mathbb{Q}[x]$ and $B, C, D \in \mathbb{Q}, B \neq 0$. Without loss of generality we may assume $B = 1$. Then $f_A(x) = P\left((x + C/2)^2 + D - C^2/4\right)$. Hence the roots of f_A form a symmetric set with respect to $-C/2$, but they also form a symmetric set with respect to $\overline{a}$. Thus $C = -2\overline{a}$. This proves the uniqueness. □

5. Proofs of results on Diophantine equations

We start with the proof of Theorem 2.4. For this, we introduce some notation and state three lemmas.

Let $f(x) \in \mathbb{Z}[x]$ of degree d and height (i.e, the maximum of the absolute values of the coefficients) H, and let a be a non-zero integer. Consider the equation

$$f(x) = ay^\ell \tag{19}$$

in $x, y, \ell \in \mathbb{Z}$ with $\ell \geq 2$. The next lemma is due to Schinzel and Tijdeman [22]. Actually already Tijdeman [24] suffices.

Lemma 5.1. *Suppose that $f(x)$ has at least two different roots. Then for all solutions x, y, ℓ of (19) with $|y| > 1$ we have*

$$\ell < C_1,$$

where $C_1 = C_1(a, d, H)$ is an effectively computable constant depending only on a, d and H.

The second lemma is a result of Brindza [6]. Let S be a finite set of primes, and write $\mathbb{Z}_S$ for the set of those rational numbers whose denominators have no prime divisors outside S. For a rational number q (given in its minimal form), by its height $h(q)$ we mean the maximum of the absolute values of its denominator and numerator.

Lemma 5.2. *Let $f(x) \in \mathbb{Z}[x]$ with*

$$f(x) = a_0 \prod_{i=1}^{s} (x - \gamma_i)^{r_i},$$

where $\gamma_1, \dots, \gamma_s$ are the (distinct, complex) zeros of $f(x)$, with multiplicities $r_1, \dots, r_s$, respectively. Further, suppose that ℓ (with $\ell \geq 2$) is fixed, and write

$$t_i = \frac{\ell}{\gcd(\ell, r_i)} \qquad (i = 1, \dots, s).$$

Suppose that $(t_1, \dots, t_s)$ is not a permutation of any of the s-tuples

$$(t, 1, \dots, 1)\ (t \geq 1), \quad (2, 2, 1, \dots, 1).$$

Then for any finite set S of primes, for the solutions $x, y \in \mathbb{Z}_S$ of (19) *we have*

$$\max(h(x), h(y)) < C_2.$$

Here $C_2 = C_2(a, \ell, d, H, S)$ is an effectively computable constant depending only on a, ℓ, d, H, S.

Finally, we formulate a statement taking care of the cases $r \leq 1$.

Lemma 5.3. *Let k, j be integers with $k \geq 8$ and $1 \leq j \leq k$, and put*

$$f_{k,j}(x) = \prod_{\substack{i=1 \\ i \neq j}}^{k} (x - i).$$

Further, let $a, b \in \mathbb{Q}$ with $a \neq 0$. Then for all solutions of the equation

$$f_{k,j}(x) = a y^\ell + b$$

in integers x, y, ℓ with $\ell \geq 2$ we have $\max(|x|, |y|, \ell) < C_3$*, where C_3 is an effectively computable constant depending only on k, a, b. Here we use the convention that for $|y| \leq 1$ we have $\ell \leq 3$.*

Proof. In case of $j = 1$ or $j = k$ the statement follows from the main result of [26], while in the other cases it is a consequence of Theorem 2.2 of [14]. □

Now we are ready to give the proof of our effective result.

Proof of Theorem 2.4. Consider (10) with fixed A, c, d, a, b in integers x, y, ℓ with $\ell \geq 2$. Our proof relies on Lemmas 5.1 and 5.2, hence ultimately on the multiplicities of the roots of $f_{A,c,d}(x)$ and its shifts $f_{A,c,d}(x) - b$. Thus as by a simple rational substitution and multiplication by appropriate rationals we can transform $f_{A,c,d}(x)$ into $f_A(x)$, we may consider $f_A(x)$ in place of $f_{A,c,d}(x)$. In view of Lemma 5.3 and $n \geq 9$, we may assume $r = n - |A| \geq 2$ as well.

As all the roots of $f_A(x)$ are simple and real, the same is valid for the polynomial $f_A'(x)$, and consequently for $(f_A(x) - b)'$. Thus the polynomial $f_A(x) - b$ can have at most double roots. Since its degree is $n-r \geq 22$, the statement immediately follows from Lemmas 5.1 and 5.2, unless $\ell = 2$ and $f_A(x)$ is of the form

$$f_A(x) = p(x)(q(x))^2 + b \tag{20}$$

with some $p, q \in \mathbb{Q}[x]$ with $\deg p \leq 2$. In particular,

$$N := |A| = \deg f_A(x)$$

has the same parity as $\deg p$ has. Write $a_1 < \cdots < a_N$ for the elements of A. Taking derivatives, (20) gives

$$f'_A(x) = q(x)(p'(x)q(x) + 2p(x)q'(x)). \tag{21}$$

Let $\alpha_1, \ldots, \alpha_{N-1}$ be the roots of $f'_A(x)$. Then by Rolle's theorem these are distinct real numbers with

$$a_i < \alpha_i < a_{i+1} \quad (i = 1, \ldots, N-1).$$

We only consider the case $\deg p = 2$. In fact, it is the most complicated possibility, the other cases are simpler and can be handled similarly. Then clearly, $\deg q = N/2 - 1$, and (21) shows that the roots of $q(x)$ are among the α_i-s. Further, (20) implies that for these α_i-s we have $f_A(\alpha_i) = b$. Observe that, by (6), $f_A(\alpha_i) < 0$ for i odd, while $f_A(\alpha_i) > 0$ for i even. Altogether, we have two options:

(a) either the roots of $q(x)$ are given by $\alpha_2, \alpha_4, \ldots, \alpha_{N-2}$ (i.e. all the roots with even indices are involved),
(b) or the $N/2-1$ roots of $q(x)$ are among $\alpha_1, \alpha_3, \ldots, \alpha_{N-1}$ (that is, all the roots with odd indices with one exception are involved).

Put

$$G(x) = f_A(x-2) - f_A(x)$$

and set

$$A^* = \{a \in A \ : \ a + 2 \in A\}.$$

Observe that $|A^*| \geq N - r - 2$ and

$$G(x) = H(x) \prod_{a^* \in A^*} (x - a^*)$$

with $\deg H \leq r + 2$. Further, among the (not disjoint) quadruples

$$\{2i-2, 2i-1, 2i, 2i+1\} \quad (i = 2, \ldots, \lfloor (n-1)/2 \rfloor)$$

at least $n/2 - 2 - 2r$ are subsets of A. So by (4), there is a quadruple $2i-2, 2i-1, 2i, 2i+1$ contained in A, such that $H(x)$, and thus $G(x)$ has no root in some interval $(2i, 2i+1)$. However, then the sign of $G(x)$ does not change in this interval. If $G(x) > 0$ for $x \in (2i, 2i+1)$ then $f_A(x-2) > f_A(x)$ and choosing $x = \alpha_{2i}$ we have

$$f_A(\alpha_{2i-2}) \geq f_A(\alpha_{2i} - 2) > f_A(\alpha_{2i}).$$

Here we use that α_{2i-2} is the maximum of f_A on $(2i-2, 2i-1)$. If $G(x) < 0$ for $x \in (2i, 2i+1)$ then $f_A(x-2) < f_A(x)$ and choosing $x = \alpha_{2i-2} + 2$ the same reasoning gives

$$f_A(\alpha_{2i-2}) < f_A(\alpha_{2i-2} + 2) \leq f_A(\alpha_{2i}).$$

Hence in both cases

$$f_A(\alpha_{2i-2}) \neq f_A(\alpha_{2i}), \tag{22}$$

which shows that the option (a) above concerning the roots of $q(x)$ is not possible. On the other hand, among the quadruples

$$\{2i-1, 2i, 2i+1, 2i+2\} \quad (i = 1, \dots, \lfloor n/2 - 1 \rfloor)$$

at least $n/2 - 2r - 2$ are subsets of A. So by (4), there are three quadruples as above contained in A, such that $H(x)$, and thus $G(x)$ has no root in three distinct intervals $(2i_j + 1, 2i_j + 2)$ $(j = 1, 2, 3)$. Similarly to (22) we obtain

$$f_A(\alpha_{2i_j - 1}) \neq f_A(\alpha_{2i_j + 1}) \quad (j = 1, 2, 3),$$

which shows that the option (b) above concerning the roots of $q(x)$ is also impossible. $\square$

Now we give the proof of Theorem 2.3. For this we need some more results and notation.

Let δ be a non-zero rational number and μ be a positive integer. Then

$$D_\mu(x, \delta) := \sum_{i=0}^{\lfloor \mu/2 \rfloor} d_{\mu,i} x^{\mu - 2i} \quad \text{where } d_{\mu,i} = \frac{\mu}{\mu - i} \binom{\mu - i}{i} (-\delta)^i$$

is the μ-th Dickson polynomial. For properties of these polynomials see e.g. [16].

We shall use a deep result of Bilu and Tichy [4] concerning equations of the type

$$f(x) = g(y) \tag{23}$$

in integers x, y, where f, g are polynomials with rational coefficients. To describe this result, we introduce some notation. We say that $F, G \in \mathbb{Q}[x]$ form a standard pair over $\mathbb{Q}$ if either $(F(x), G(x))$ or $(G(x), F(x))$ appears in Table 1.

Now we recall the main result of [4], which will play a key role in the proof of Theorem 2.3.

Lemma 5.4. *Let $f(x), g(x) \in \mathbb{Q}[x]$ be non-constant polynomials. Then the following two statements are equivalent.*

Kind	Standard pair	Parameter restrictions
First	$(x^q, \alpha x^p v(x)^q)$	$0 \le p < q$, $(p,q)=1$, $p+\deg v(x) > 0$
Second	$(x^2, (\alpha x^2+\beta)v(x)^2)$	-
Third	$(D_\mu(x,\alpha^\nu), D_\nu(x,\alpha^\mu))$	$\gcd(\mu,\nu)=1$
Fourth	$(\alpha^{-\mu/2}D_\mu(x,\alpha), -\beta^{-\nu/2}D_\nu(x,\beta))$	$\gcd(\mu,\nu)=2$
Fifth	$((\alpha x^2-1)^3, 3x^4-4x^3)$	-

TABLE 1. Standard pairs. Here α, β are non-zero rational numbers, μ, ν, q are positive integers, p is a non-negative integer, $v(x) \in \mathbb{Q}[x]$ is a non-zero, but possibly constant polynomial.

(I) *Equation* (23) *has infinitely many rational solutions x, y with a bounded denominator.*

(II) *We have $f = \varphi \circ F \circ \lambda$ and $g = \varphi \circ G \circ \kappa$, where $\lambda(x), \kappa(x) \in \mathbb{Q}[x]$ are linear polynomials, $\varphi(x) \in \mathbb{Q}[x]$, and $F(x), G(x)$ form a standard pair over $\mathbb{Q}$ such that the equation $F(x) = G(y)$ has infinitely many rational solutions x, y with a bounded denominator.*

Proof of Theorem 2.3. By Lemma 5.4, if $f_{A,c,d}(x) = P(y)$ has infinitely many integer solutions then $f_{A,c,d} = \varphi \circ F \circ \lambda$ and $P = \varphi \circ G \circ \kappa$, where φ, λ, κ are rational polynomials with $\deg \lambda = \deg \kappa = 1$, and F and G form a standard pair. By Corollary 2.1, $\deg \varphi \in \{n-r, (n-r)/2, 1\}$. Observe that since the decompositions of the polynomials $f_{A,c,d}$ and f_A are equivalent, we may assume that $c = 0$ and $d = 1$, that is, it is enough to deal with $f_A(x)$. Further, since all quadratic polynomials are equivalent, in view of the case $\ell = 2$ in Theorem 2.4, we may assume without loss of generality that $\deg P \ge 3$. Finally, by the main result of [15] and by Theorem 2.1 of [14] we may assume that $r = n - |A| \ge 2$. By (4) this implies

$$\deg f_A(x) = N = n - r \ge 24. \tag{24}$$

If $\deg \varphi = n - r$ then $\deg F = 1$, and we easily get that we are in case (i) of Theorem 2.3.

Suppose $\deg \varphi = (n-r)/2$. Then we have $\deg F = 2$. By Corollary 2.1 the decomposition is given up to a linear transformation: $f_A(x) = \varphi^*((x-\overline{a})^2)$. If we have infinitely many solutions then by Lemma 5.4 we have $\varphi^*((x-\overline{a})^2) = P(y) = \varphi^*(G(y))$ for some $G(y) \in \mathbb{Q}[y]$ such that $(x-\overline{a})^2 = G(y)$ has infinitely many solutions. Lemma 5.2 implies that we must be in case (ii).

Finally, consider the case $\deg \varphi = 1$. Then $\deg F = n - r$, and we have

$$f_A(x) = aF(sx + t) + b$$

where F is a member of a standard pair. We check the possible cases.

As $\deg f_A \geq 24$, F cannot come from a standard pair of the fifth kind. Since we assumed that $\deg P \geq 3$, the polynomial F cannot belong to a standard pair of the second type, either.

Assume that F belongs to a standard pair of the first kind. Since all the zeros of $f_A(x)$ are real and simple, hence by Rolle's theorem all the roots of $f'_A(x)$ are real and simple, $F(x) = x^q$ is not possible. On the other hand, if $F(x) = x^p(v(x))^q$, then f_A is of the form

$$f_A(x) = a(s_1x + s_2)^p(v(s_1x + s_2))^q + b$$

with some $s_1, s_2 \in \mathbb{Q}$, $s_1 \neq 0$. Using again that the roots of $f'_A(x)$ are simple, we get $q \leq 2$. However, then in view of that the other term in the standard pair in question is x^q, we see that $\deg P \leq 2$, which is excluded.

Finally, assume that F belongs to a standard pair of the third or fourth kind. Then $f_A(x)$ should be a linear transform of a Dickson polynomial. More precisely, with some rationals s_1, s_2, t_1, t_2 $(s_1t_1 \neq 0)$ and non-negative integer N we can write

$$t_1 f_A(s_1x + s_2) + t_2 = D_N(x, \delta),$$

where $D_N(x, \delta)$ is the N-th Dickson polynomial, with non-zero parameter $\delta \in \mathbb{Q}$. (Here we apply the inside and outside linear transformations to f_A rather than to D_N. In fact, writing $f_A = \varphi \circ D_N \circ \lambda$, $t_1x + t_2$ and $s_1x + s_2$ are the inverses of the linear polynomials $\varphi(x)$ and $\lambda(x)$, respectively.) Observe that here $N = \deg f_A(x) = |A|$ must hold. Then, by the well-known identity (see. e.g. formula (2.2) on p. 9 of [16])

$$D_N\left(y + \frac{\delta}{y}, \delta\right) = y^N + \left(\frac{\delta}{y}\right)^N$$

we obtain

$$t_1 \prod_{a \in A}\left(s_1\left(y + \frac{\delta}{y}\right) + s_2 - a\right) + t_2 = y^N + \left(\frac{\delta}{y}\right)^N.$$

Hence as $|A| = N$,

$$\prod_{a \in A}\left(y^2 + \frac{s_2 - a}{s_1}y + \delta\right) = y^{2N} - t_2y^N + \delta^N$$

follows. Here we used by comparing the leading coefficients, that $t_1s_1^N = 1$ must hold. Write ζ, ξ for the roots of the polynomial $y^2 -$

$t_2y + \delta^N$. Clearly, ζ, ξ are algebraic numbers of degree at most two. Further, we have

$$\prod_{a\in A}\left(y^2 + \frac{s_2 - a}{s_1}y + \delta\right) = (y^N - \zeta)(y^N - \xi). \tag{25}$$

If ζ_0, ξ_0 are roots of $y^N - \zeta$ and $y^N - \xi$, respectively, then all the roots of these polynomials are given by

$$\zeta_0\varepsilon^i \quad \text{and} \quad \xi_0\varepsilon^i \quad (i = 0, 1, \ldots, N-1),$$

respectively, where ε is a primitive N-th root of unity. By (25) we see that all these roots are algebraic numbers of degrees at most two. This immediately gives that the degree of ε is at most four, hence $\varphi(N) \le 4$. We conclude that $N \le 12$. This contradicts (24). □

Acknowledgements

The authors are grateful to the Referee for the useful and helpful remarks.

References

[1] M. Bennett, S. Siksek, *A conjecture of Erdős, supersingular primes and short character sums*, Annals Math. **191** (2020), 355-392.

[2] F. Beukers, T. N. Shorey and R. Tijdeman, *Irreducibility of polynomials and arithmetic progressions with equal product of terms*, in: Number Theory in Progress (Proc. Internat. Conf. in Number Theory in Honor of A. Schinzel, Zakopane, 1997), K. Győry, H. Iwaniec and J. Urbanowicz (eds.), de Gruyter, 1999, pp. 11–26.

[3] Yu. Bilu, M. Kulkarni, B. Sury, *The Diophantine equation* $x(x+1)\ldots(x+(m-1))+r=y^n$, Acta Arith. **113** (2004), 303–308.

[4] Yu. Bilu, R. Tichy, *The Diophantine equation* $f(x) = g(y)$, Acta Arith. **95** (2000), 261–288.

[5] R. Blankertz, *A polynomial time algorithm for computing all minimal decompositions of a polynomial*, ACM Comm. Computer Algebra 48:1, Issue 187 (2014), 13-23.

[6] B. Brindza, *On S-integral solutions of the equation* $y^m = f(x)$, Acta Math. Hungar. **44** (1984), 133–139.

[7] H. Davenport, D.J. Lewis, A. Schinzel, *Equations of the form* $f(x) = g(y)$, Quart. J. Oxford Ser. (2) 12 (1961), 304-312.

[8] P. Erdős, *On a Diophantine equation*, J. London Math. Soc. **26** (1951), 176–178.

[9] P. Erdős, J. L. Selfridge, *The product of consecutive integers is never a power*, Ill. J. Math. **19** (1975), 292–301.

[10] M. Fried, *On a theorem of Ritt and related Diophantine problems*, J. Reine Angew. Math. **264** (1973), 40-55.

[11] M. Fried, *Variables separated polynomials, the genus 0 problem and moduli spaces*, Number Theory in Progress, vol. 1, Walter de Gruyter, Berlin, pp. 169-228 (1999).

[12] H. R. Gallegos-Ruiz, N. Katsipis, Sz. Tengely, M. Ulas, *On the Diophantine equation* $\binom{n}{k} = \binom{m}{l} + d$, J. Number Th. **208** (2020), 418-440.

[13] K. Győry, *On the Diophantine equation* $\binom{n}{k} = x^l$, Acta Arith. **80** (1997), 289–295.

[14] L. Hajdu, Á. Papp, *Polynomial values of products of terms from an arithmetic progression*, Monatsh. Math. **162** (2020).

[15] M. Kulkarni, B. Sury, *On the Diophantine equation* $x(x+1)(x+2)\cdots(x+(m-1)) = g(y)$, Indag. Math. **14** (2003), 35–44.

[16] R. Lidl, G. Mullen, G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics **65**, Longman Scientific & Technical, Harlow, 1993.

[17] S. Raghavendran, V.Varayanan, *The Prouhet Tarry Escott problem: A review*, MDPI, Mathematics 7 (2019), 227.

[18] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51-66.

[19] N. Saradha, T. N. Shorey, *Almost perfect powers in arithmetic progression*, Acta Arith. **99** (2001), 363–388.

[20] N. Saradha, T. N. Shorey, *Almost squares and factorizations in consecutive integers*, Compositio Math. **138** (2003), 113–124.

[21] N. Saradha, T. N. Shorey, *On the equation* $n(n+d)\cdots(n+(i_0-1)d)(n+(i_0+1)d)\cdots(n+(k-1)d) = y^l$ *with* $0 < i_0 < k-1$, Acta Arith. **129** (2007), 1–21.

[22] A. Schinzel, R. Tijdeman, *On the equation* $y^m = P(x)$, Acta Arith. **31** (1976), 199–204.

[23] T. Stoll, R. F. Tichy, *The Diophantine equation* $\alpha\binom{x}{m} + \beta\binom{y}{n} = \gamma$, Publ. Math. Debrecen **64** (2004), 155–165.

[24] R. Tijdeman, *Applications of the Gel'fond-Baker method to rational number theory*, Topics in Number Theory, Proceedings of the Conference at Debrecen 1974, Colloq. Math. Soc. János Bolyai **13**, pp. 399–416, North-Holland, Amsterdam, 1976.

[25] B. de Weger, *Equal Binomial Coefficients: Some Elementary Considerations*, J. Number Th. **63** (1997), 373–386.

[26] P.-Z. Yuan, *On a special diophantine equation* $a\binom{x}{m} = by^r + c$, Publ. Math. Debrecen **44** (1994), 137–143.

L. Hajdu
University of Debrecen, Institute of Mathematics
H-4002 Debrecen, P.O. Box 400.
and Alfréd Rényi Institute of Mathematics
H-1367 Budapest, P.O. Box 127.
Hungary
Email address: hajdul@science.unideb.hu
Email address: hajdu@renyi.hu

Á. Papp
University of Debrecen, Institute of Mathematics
H-4002 Debrecen, P.O. Box 400.
Hungary
Email address: papp.agoston@science.unideb.hu

R. Tijdeman
Mathematical Institute
Leiden University
Postbus 9512, 2300 RA Leiden, The Netherlands
Email address: tijdeman@math.leidenuniv.nl