TWO PROOFS IN COMBINATORIAL NUMBER THEORY

JAROSLAV NEŠETŘIL AND VOJTECH RÖDL

ABSTRACT. The aim of this paper is to present a short combinatorial proof of a theorem of P. Erdös on multiplicative bases of integers. A solution of a problem of P. Erdös and D. J. Newman is also presented.

I. Let \( X \) be a set of positive integers. We say that \( X \) is a multiplicative base if for every positive integer \( n \) there are \( x, y \in X \) such that \( n = xy \). The following was proved by P. Erdös (see [1]).

**Theorem 1.** Let \( X \) be a multiplicative base. Then for every positive integer \( p \) there exists a positive integer \( n \) such that \( n \) can be expressed as the product of two elements of \( X \) in at least \( p \) different ways.

In the proof of Theorem 1 we shall need the well-known theorem of Ramsey: Let \( p \) be a given integer and let \( [A]^p = C_1 \cup C_2 \) be a partition of the set of all \( p \)-tuples of elements of an infinite set \( A \) into two parts. Then there exists \( i \) and an infinite set \( B \subseteq A \) such that \( [B]^p \subseteq C_i \). The set \( B \) is called homogeneous with respect to the partition \( (C_1, C_2) \).

**Proof of Theorem 1.** In the following we shall consider the integers which are products of distinct primes only. Such integers can be identified in a natural way with finite subsets of the set of all primes. Thus it suffices to prove the following

**Theorem 1'.** Let \( A \) be an infinite set. Denote by \( [A]^{<\omega} \) the set of all finite subsets of \( A \). Let \( \mathcal{A} \subseteq [A]^{<\omega} \) be a set of finite subsets of \( A \) such that the following holds:

\[
\text{For every } P \in [A]^{<\omega} \text{ there are } Q, Q' \in \mathcal{A} \text{ such that } Q \cup Q' = P \text{ and } Q \cap Q' = \emptyset.
\]

Then for every integer \( p \) there is a set \( P \) which can be expressed in at least \( p \)-different ways as a union of two disjoint elements of \( \mathcal{A} \).

Proof of Theorem 1' is a straightforward consequence of Ramsey's theorem: Let \( p \) be a given positive integer, \( p \geq 2 \). For every \( i = 1, \ldots, p - 1 \) consider a partition \( [A]^i = C_1^i \cup C_2^i \) defined by \( Q \in C_1^i \text{ iff } Q \in \mathcal{A} \). Let \( B \) be an infinite set which is homogeneous with respect to all partitions \( C_1^i, C_2^i, i = 1, \ldots, p - 1 \) (such a set clearly...
exists by iterating the Ramsey theorem. From (\*) we get that there is an \( i, 1 \leq i \leq p - 1 \), such that

\[
[B]^i \subseteq C_1^i \quad \text{and} \quad [B]^{p-i} \subseteq C_1^{p-i},
\]

and hence every \( P \in [B]^p \) can be represented as a union of at least \( \binom{p}{2} \geq p \) elements of \( A \).

\textbf{Remark.} Note that the above proof gives nothing concerning the additive version of Theorem 1. This is an old problem of P. Erdős:

\textbf{Problem.} Let \( X \) be a set of positive integers with the property that for every positive integer \( n \) there are \( x, y \in X \) such that \( n = x + y \). Is it true that for every positive integer \( p \) there exists a positive integer \( n \) such that \( n \) can be expressed as the sum of two elements of \( X \) in at least \( p \) different ways?

\textbf{II.} Let \( X \) be a set of positive integers. We say that \( X \) is a \( B_2^k \)-sequence if the number of representations of \( n \) as the sum \( x + y \), \( x, y \in X \), is at most \( k \) and for some \( n \) is exactly \( k \). The following is known as the Erdős-Newman problem:

Is it true that given a \( k \) there exists a \( B_n^k \)-sequence \( X \) such that for every partition \( X = X_1 \cup \cdots \cup X_r \) into a finite number of parts one of the parts is a \( B_n^k \)-sequence?

For certain \( k \) the affirmative solution is given in [2]. We prove here (by different methods)

\textbf{Theorem 2.} For every \( k \geq 2 \) there exists a set of integers \( X \) such that:

1. \( X \) is a \( B_n^k \)-sequence;
2. For every partition of \( X \) into a finite number of parts one of the parts is a \( B_n^k \)-sequence.

The proof is based on the existence of Ramsey graphs of a special type. Before stating this result we introduce some necessary notions. An ordered graph is a graph \((V, E)\) with a (fixed) ordering of its vertices. \( K_3 \) is the complete graph with 3 vertices (i.e. the triangle). Denote by \( L_k \) the graph \((V, E)\) defined as follows:

\[
V = \{0, 1, \ldots, k + 1\},
\]

\[
E = \{\{0, i\}; i = 1, \ldots, k\} \cup \{\{i, k + 1\}; i = 1, \ldots, k\}.
\]

The graph \( L_k \) is always considered as an ordered graph with the natural ordering of its vertices. (The graph \( L_k \) is depicted in Figure 1.) Let \((V, E)\) and \((V', E')\) be ordered graphs. We say that \((V, E)\) is contained in \((V', E')\) if \( V \subseteq V' \) and \( E \subseteq E' \) and the ordering of \( V' \) restricted to the set \( V \) coincides with that of \( V \). We shall use the following

\textbf{Lemma.} For every \( k, r \geq 2 \) there exists an ordered graph \( G_r^k = (V, E) \) with the following properties:

1. \( G_r^k \) does not contain \( L_{k+1} \) and \( K_3 \);
2. for every partition \( E = E_1 \cup \cdots \cup E_r \), one of the classes \( E_i \) contains \( L_k \).

(A proof of this Lemma is too nontrivial (and lengthy) to be included here. However it follows easily from the "partite construction" which is introduced and studied in [3].)
Proof of Theorem 2. Put \( G = \bigcup (G^k_r; \ r \geq 2) \)—the disjoint union of graphs described in the Lemma. Consider \( G = (V, E) \) as an ordered graph which contains every \( G^k_r; \ r \geq 2 \). Assume without loss of generality that the vertices of \( G \) are integers. Define the set \( X \) as the set of all sums \( \sum n \), where the summation is taken over the set \( I_{uv} \) of all positive integers \( n \) which satisfy \( u < n < v \) for an edge \( \{ u, v \} \in E \). In the sequel the sets of the form \( I_{uv} \) are called intervals. We prove that \( X \) has the desired properties:

ad 1. Observe that if \( z = x + y \) for \( x, y \in X \) and if \( z = \sum_{i \in I} e_i 3^i \) is the triadic expansion of \( z \) (i.e. \( e_i = 1 \) or \( 2 \)), then \( I \) is either an interval or union of two intervals. Moreover, if \( e_i = 2 \) for an \( i \in I \), then \( I \) is an interval and \( I_1 = \{ i; e_i = 2 \} \) is also an interval. Therefore we may distinguish three cases which can be visualized as follows:

(i) \( I \neq \emptyset \). Either:

\[
\begin{align*}
x & \quad y \\
or
\end{align*}
\]

(ii) \( I = \emptyset \), \( I \) is an interval:

\[
\begin{align*}
x & \quad y
\end{align*}
\]

(iii) \( I \) is the union of two intervals, but it is not an interval itself:

\[
\begin{align*}
x & \quad y
\end{align*}
\]

In (i) there are at most two (depicted) possibilities for \( z = x' + y', x', y' \in X \). In (ii), there are at most \( k \) possibilities for the solution \( z = x' + y' \) by assumption (1) of the Lemma on graphs \( G^k_r \) (graphs \( G^k_r \) do not contain \( L_{k+1} \)). In (iii), \( z = x + y \) is the unique solution. Therefore \( X \) is a \( B_2^{(k)} \)-sequence.

As every partition of \( X \) corresponds to a partition of the edges of the graph \( G \), the second half of the statement of Theorem 2 follows immediately from property (2) of the Lemma on the graphs \( G^k_r \).

The methods described above enable the following generalizations of Theorems 1 and 2. Let \( X \) be a set of positive integers. Let us call \( X \) the multiplicative \( j \)-base if for every positive integer \( n \) there are \( x_1, \ldots, x_j \in X \) such that \( n = x_1 \cdots x_j \).

**Theorem 1.** Let \( X \) be a multiplicative \( j \)-base. Then for every positive integer \( p \) there exists a positive integer \( n \) such that \( n \) can be expressed as the product of \( j \) elements of \( X \) in at least \( p \) different ways.
Similarly, let us say that $X$ is a $B_{j}^{(k)}$-sequence if the number of representation of $n$ as the sum $n = x_1 + x_2 + \cdots + x_i$, $i \leq j$, $x_1, x_2, \ldots, x_i \in X$, is at most $k$ and for some $n$ exactly $k$. P. Erdős asked whether an analogy of Theorem 2 can be proved for $B_{j}^{(k)}$-sequences. If we use a suitable modification of graphs $L_k$, Theorem 2 can be strengthened as follows:

**Theorem II.** For every $k \geq 2$ and $j \geq 2$ there exists a set of integers $X$ such that

1. $X$ is a $B_{j}^{(k)}$ sequence;
2. for every partition of $X$ into a finite number of parts one of the parts is a $B_{j}^{(k)}$-sequence.

The proof is analogous to the above proof of Theorem 2 with the difference that instead of graphs $L_k$ we use graphs $L'_k = (V, E)$ defined as follows:

- $V = \{0, 1, \ldots, kj + 1\}$,
- $E = \{\{0, j \cdot i + 1\}; i = 0, \ldots, k - 1\}$
  $\cup \{\{j \cdot i + l, ji + l + 1\}; i = 0, 1, \ldots, k - 1, l = 1, 2, \ldots, j - 1\}$
  $\cup \{\{lj, kj + 1\}; l = 1, \ldots, k\}$

(see Figure 2).

**References**

2. _, Some application of Ramsey’s theorem to additive number theory, European J. Combin. 1 (1980), 43–46.