Vladimír Puš
On multiplicative bases in abelian groups


Persistent URL: [http://dml.cz/dmlcz/102461](http://dml.cz/dmlcz/102461)

**Terms of use:**

© Institute of Mathematics AS CR, 1991

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these _Terms of use._

This document has been digitized, optimized for electronic delivery and stamped with digital signature within the project _DML-CZ: The Czech Digital Mathematics Library_ [http://dml.cz](http://dml.cz)
ON MULTIPLICATIVE BASES IN ABELIAN GROUPS

VLADIMÍR Puš, Praha

(Received May 11, 1989)

1. INTRODUCTION

Suppose that $S = (X, \cdot)$ is a commutative semigroup, $M$ is a subset of $X$ and $k \geq 2$ is an integer. Denote by Card the class of all cardinals and define the function $f_{M,k}: X \to \text{Card}$ as follows: $f_{M,k}(x)$ is the number of expressions of $x$ in the form $x = m_1 \cdot m_2 \cdot \ldots \cdot m_k$, where $m_i \in M$ for $i = 1, 2, \ldots, k$. (Two expressions $x = m_1 \cdot \ldots \cdot m_k$ and $x = m'_1 \cdot \ldots \cdot m'_k$ of $x$ as a product of $k$, not necessarily distinct, elements of $M$ are considered to be identical iff they differ only in the order of members.

We say that $M$ is an asymptotic multiplicative basis of order $k$ iff $f_{M,k}(x) > 0$ for all but finitely many $x \in X$.

Let $k \geq 2$ be an integer. We say that a commutative semigroup $S = (X, \cdot)$ has property $E(k)$ if for every asymptotic multiplicative basis $M \subseteq X$ of order $k$ and for every positive integer $p$ there exists $x \in X$ such that $f_{M,k}(x) > p$.

In [2], P. Erdős and P. Turán set the following conjecture: The semigroup $(\mathbb{N}, +)$ of all positive integers with the usual addition has property $E(2)$.

This conjecture is still open, nonetheless, some semigroups fulfilling property $E(2)$ are known at this time. Namely, in [1], P. Erdős proved that the semigroup $(\mathbb{N}, \cdot)$ of all positive integers with the usual multiplication has property $E(2)$. A very simple proof of this result based on the theorem of Ramsey was given by Nešetřil and Rödl in [4]. Moreover, in [4] it is proved that the semigroup $(\mathbb{N}, \cdot)$ has property $E(k)$ for every $k \geq 2$.

In [3], M. B. Nathanson gave some generalizations of results from [4] and proved among other that the semigroup $(\mathbb{N}, \text{LCM})$, where LCM is the least common multiple, has property $E(k)$ for every $k \geq 2$. Other generalizations of results from [4] are given in [5] and in [6]. Let us state some of these generalizations.

**Definition 1.** Let $S = (X, \cdot)$ be a commutative semigroup.

We say that $x$ is a divisor of $y$, where $x, y \in X$, if there is an element $z \in X$ such that $y = x \cdot z$.

We say that $j \in X$ is a unit in $S$ if $j$ is a divisor of the identity element in $S$.

We say that elements $x, y, \in X$ are associated, and we write $x \sim y$, if there is a unit $j$ such that $x = y \cdot j$.

282
Let $S = (X, \cdot)$ be a commutative semigroup and let $F = \{x_1, x_2, \ldots, x_k\}$ be a finite subset of $X$. We denote by $\prod F$ the product $x_1 \cdot x_2 \cdot \ldots \cdot x_k$ of the elements of $F$. Further we put $\prod 0 = 1$, where 1 is the identity element.

**Definition 2.** We say that a set $P \subseteq X$ is a prime set if it contains no unit, if no two different elements of $P$ are associated and if for every finite (non-empty) set $F \subseteq P$ the following condition holds: if $\prod F = x_1 \cdot x_2$ then there exist sets $F_1, F_2 \subseteq F$ (possibly empty) such that $F_1 \cup F_2 = F, x_1 \sim \prod F_1$ and $x_2 \sim \prod F_2$.

**Definition 3.** The commutative semigroup is said to be a prime semigroup if it contains an infinite prime set and if it has only finitely many units.

The following theorem is proved in [6] (see also [5]).

**Theorem 1.** Every prime semigroup has property $E(k)$ for every $k \geq 2$.

Let us notice that all the results mentioned above can be proved as corollaries of Theorem 1. In paper [5], Theorem 1 is used to prove that the direct, cartesian and strong products of finite simple graphs possess property $E(k)$ for every $k \geq 2$.

In the present paper we show that, in contrast with Theorem 1, for infinite Abelian groups with the property that every equation $x^r = a$, $r \geq 2$, has only finitely many solutions, the behaviour of the functions $f_{M,k}$ is in substance in no way restricted.

Let us remark that in Abelian groups every element is a unit and thus no Abelian group contains a non-empty prime set.

## 2. RESULTS

**Notation.** The cardinality of a set $X$ will be denoted by $|X|$. If $m, n$ are integers and $m \leq n$, then $[m, n]$ denotes the set of all integers $x$ such that $m \leq x \leq n$.

**Theorem 2.** Let $k \geq 2$ be an integer. Suppose that $G = (X, \cdot)$ is an infinite Abelian group such that:

1. $|X| = \kappa$ is a regular cardinal and
2. $|\{x; x^r = a\}| < \kappa$ for every $a \in X$ and $r \in [2, 2k]$.

Then for every function $f: X \to \kappa \setminus \{0\}$ there is a set $M \subseteq X$ such that $f_{M,k} = f$.

**Remark 1.** Condition (2) is clearly equivalent to the following condition (2'):

\[ |\{x; x^p = a\}| < \kappa \quad \text{for every } a \in X \text{ and for every prime number } p \in [2, 2k]. \]

**Proof of Theorem 2.** Let us denote $X = \{x_\alpha; \alpha < \kappa\}$. We construct by recursion a chain of sets $M_\alpha$, $\alpha < \kappa$, such that for every $\alpha < \kappa$ the following conditions (0)-(4) hold:

1. $M_0 = \emptyset$,
(1) \(M_\beta \subseteq M_\alpha\) for \(\beta < \alpha\),
(2) \(|M_\alpha| < \alpha\),
(3) every element \(x \in X\) can be expressed in at most one way as a product of less than \(k\) elements (not necessarily distinct) of \(M_\alpha\), and
(4) every element \(x_\beta\) for \(\beta \geq \alpha\) can be expressed in at most one way as a product of \(k\) elements (not necessarily distinct) of \(M_\alpha\).

Moreover, we perform the construction of the chain \(\{M_\alpha; \alpha < \kappa\}\) in such a way that the union of the chain satisfies the following condition (5).

(5) every element \(x_\beta\) for \(\beta < \kappa\) can be expressed exactly in \(f(x_\beta)\) ways in the form \(m_1 \cdot m_2 \cdots m_k\), where \(m_i \in \bigcup_{\alpha < \kappa} M_\alpha\) (i.e. \(f_{M_\alpha}(x_\beta) = f(x_\beta)\) for \(M = \bigcup_{\alpha < \kappa} M_\alpha\)).

Let us define \(M_0 = \emptyset\) and \(M_\kappa = \bigcup_{\beta < \kappa} M_\beta\) provided \(\kappa\) is a limit ordinal. (Clearly, if the sets \(M_\beta\), \(\beta < \kappa\), satisfy conditions (0)-(4) then \(M_\kappa\) satisfies these conditions, too. Let us remark that (2) follows from the regularity of \(\kappa\).)

Now, let the set \(M_\alpha\) satisfying conditions (0)-(4) be constructed; we construct \(M_{\alpha + 1}\). Denote by \(\lambda\) the unique cardinal number such that

\[\lambda + f_{M_\alpha, k}(x_\alpha) = f(x_\alpha)\]

(C) \(a_{\mu, j}\) is not a solution of any equation \(x^r \cdot c = d\), where \(r \in \{1, 2k\}\) and \(c, d\) are products of at most \(2k^2\) elements (not necessarily distinct) of the set \(M_\alpha \cup \{a_{\mu, j}; (v, l) < (\mu, j)\} \cup \{x_\alpha\}\), where \(<\) is some (e.g. lexicographic) well-ordering of the set \(\lambda \times \{1, 2k\}\).

(6) \(m_1 \cdots m_r \cdot \left(\prod_{j=1}^{k} a_{\mu_1, j}^{p_1, j}\right) \cdots \left(\prod_{j=1}^{k} a_{\mu_1, j}^{p_1, j}\right) = \)

\[n_1 \cdots n_s \cdot \left(\prod_{j=1}^{k} a_{\mu_1, j}^{q_1, j}\right) \cdots \left(\prod_{j=1}^{k} a_{\mu_1, j}^{q_1, j}\right)\]

284
are two products of elements of $M_{a+1}$, where $m_1, \ldots, m_r \in M_a$, $n_1, \ldots, n_s \in M_a$, $\mu_1, \ldots, \mu_t$ are pairwise distinct, $p_{i,j} \geq 0$, $q_{i,j} \geq 0$, $r + \sum_{i,j} p_{i,j} < k$ and $s + \sum_{i,j} q_{i,j} < k$. Substituting $a_{\mu,k} = (\mu_{i,1} \ldots \mu_{i,k-1})^{-1} \cdot x_a$, where $i = 1, \ldots, t$, we obtain

\begin{equation}
(m_1 \ldots m_r \cdot (\prod_{j=1}^{k-1} a_{\mu_{i,j}^{-p_{i,j}}}) \ldots (\prod_{j=1}^{k-1} a_{\mu_{t,j}^{-p_{t,j}}}) \cdot x_a^s)^{\sum_{i,j} p_{i,k}} = n_1 \ldots n_s \cdot (\prod_{j=1}^{k-1} a_{\mu_{l,j}^{-q_{l,j}}}) \ldots (\prod_{j=1}^{k-1} a_{\mu_{l,j}^{-q_{l,j}}}) \cdot x_a^s \sum_{i,j} q_{i,k}.
\end{equation}

It follows from this (according to the construction of $a_{\mu,j}$'s) that, for every $i \in [1, t]$ and $j \in [1, k - 1]$, $p_{i,j} - p_{i,k} = q_{i,j} - q_{i,k}$, i.e. $p_{i,j} - q_{i,j} = p_{i,k} - q_{i,k}$. In other words, for fixed $i$, the numbers $p_{i,j} - q_{i,j}$ do not depend on $j$ and thus there is a number $c_i$ such that $p_{i,j} - q_{i,j} = c_i$ for every $j \in [1, k]$. Suppose that $c_i > 0$ for some $i$. Then $p_{i,j} = q_{i,j} + c_i > 0$ for every $j \in [1, k]$ and thus $r + \sum_{i,j} p_{i,j} \geq k$, a contradiction. Similarly $c_i < 0$ leads to a contradiction, thus $c_i = 0$ for every $i$.

We find that $p_{i,j} = q_{i,j}$ for all $i, j$. Now (6) implies that $m_1 \ldots m_r = n_1 \ldots n_s$. By the induction hypothesis, the expressions $m_1 \ldots m_r$ and $n_1 \ldots n_s$ are identical, thus the expressions on the left and on the right hand side of (6) are identical, too.

This concludes the proof that $M_{a+1}$ satisfies condition (3).

Condition (4) follows from the following two lemmas.

**Lemma 1.** If

\begin{equation}
m_1 \ldots m_k = n_1 \ldots n_s \cdot \left(\prod_{j=1}^{k} a_{\mu_{i,j}^{-p_{i,j}}}ight) \ldots \left(\prod_{j=1}^{k} a_{\mu_{t,j}^{-p_{t,j}}}ight),
\end{equation}

where $m_1, \ldots, m_k \in M_a$, $n_1, \ldots, n_s \in M_a$, $\mu_1, \ldots, \mu_t$ are pairwise distinct, $p_{i,j} \geq 0$, $s + \sum_{i,j} p_{i,j} = k$ and $s < k$, then $m_1 \ldots m_k = x_a$.

**Lemma 2.** Suppose that

\begin{equation}
m_1 \ldots m_r \cdot \left(\prod_{j=1}^{k} a_{\mu_{i,j}^{-p_{i,j}}}ight) \ldots \left(\prod_{j=1}^{k} a_{\mu_{t,j}^{-p_{t,j}}}ight) =
\end{equation}

\begin{equation}
n_1 \ldots n_s \cdot \left(\prod_{j=1}^{k} a_{\mu_{i,j}^{-q_{i,j}}}ight) \ldots \left(\prod_{j=1}^{k} a_{\mu_{t,j}^{-q_{t,j}}}ight),
\end{equation}

where $m_1, \ldots, m_r \in M_a$, $n_1, \ldots, n_s \in M_a$, $\mu_1, \ldots, \mu_t$ are pairwise distinct, $p_{i,j} \geq 0$, $q_{i,j} \geq 0$, $r + \sum_{i,j} p_{i,j} = s + \sum_{i,j} q_{i,j} = k$ and $r, s < k$. Then the expressions on the left and on the right hand side of (9) are either identical or (9) is an equation of the form $a_{\mu,1} \ldots a_{\mu,k} = a_{v,1} \ldots a_{v,k}$, where $\mu, v < \lambda$ and $\mu \neq v$.

**Proof of Lemma 1.** Substituting $(a_{\mu_{i,1}} \ldots a_{\mu_{i,k-1}})^{-1} \cdot x_a$ for $a_{\mu_{i,k}}$, where $i = 1, \ldots, t$, equation (8) converts into the form

\begin{equation}
m_1 \ldots m_k = n_1 \ldots n_s \cdot \left(\prod_{j=1}^{k-1} a_{\mu_{i,j}^{-p_{i,j}}}ight) \ldots \left(\prod_{j=1}^{k-1} a_{\mu_{t,j}^{-p_{t,j}}}ight) \cdot x_a^s \sum_{i,j} p_{i,k}.
\end{equation}
It follows from this (with regard to the construction of \( a_{\mu,j} \)'s) that \( p_{i,j} - p_{i,k} = 0 \) for every \( i \in [1, t] \) and \( j \in [1, k - 1] \). Thus, \( k \cdot \sum_{i} p_{i,k} = \sum_{i,j} p_{i,j} \). Since moreover \( \sum_{i,j} p_{i,j} = k - s > 0 \), we infer that there exists \( i_0 \in [1, t] \) such that \( p_{i_0,k} > 0 \). But then \( p_{i_0,j} > 0 \) for every \( j \in [1, k] \) and since \( s + \sum_{i,j} p_{i,j} = k \), equation (8) has the form \( m_1 \ldots m_k = \prod_{j=1}^{k} a_{\mu_{i_0,j}} \). We conclude that \( m_1 \ldots m_k = x_s \).

**Proof of Lemma 2.** Let us convert (9) into (7). Analogously as in the proof of (3) we infer that for every \( i \in [1, t] \) there is a number \( c_i \) such that
\[
p_{i,j} - q_{i,j} = c_i \quad \text{for every} \quad j \in [1, k] .
\]
We distinguish three cases.

Case (A). Let \( c_i = 0 \) for every \( i \in [1, t] \). Then \( p_{i,j} = q_{i,j} \) for every \( i \) and \( j \), and (9) implies that
\[
m_1 \ldots m_r = n_1 \ldots n_s .
\]
By (3), the expressions on the left and on the right hand side of (10) are identical and so the expressions on the left and on the right hand side of (9) are identical, too.

Case (B). Suppose that there exists \( i_0 \in [1, t] \) such that \( c_{i_0} > 0 \). Then \( p_{i_0,j} = c_{i_0} + q_{i_0,j} > 0 \) for every \( j \in [1, k] \). It follows from this and from the assumptions of Lemma 2 that \( r = 0 \), \( p_{i_0,j} = 1 \) for every \( j \), \( q_{i_0,j} = 0 \) for every \( j \), \( p_{i,j} = 0 \) for every \( j \) and \( i \neq i_0 \), and \( c_i \leq 0 \) for every \( i \neq i_0 \). In particular, the expression on the left hand side of (9) is
\[
a_{\mu_{i_0,1}} \ldots a_{\mu_{i_0,k}} .
\]
Further, there exists \( i_1 \neq i_0 \) such that \( c_{i_1} < 0 \). Otherwise \( c_i = 0 \) for every \( i \neq i_0 \), i.e. \( q_{i,j} = p_{i,j} = 0 \) for every \( j \) and \( i \neq i_0 \), and so \( q_{i,j} = 0 \) for every \( i, j \). This implies that \( s = s + \sum_{i,j} q_{i,j} = k \), a contradiction. Similarly as above, the assumption \( c_{i_1} < 0 \) implies that the right hand side of (9) is
\[
a_{\mu_{i_1,1}} \ldots a_{\mu_{i_1,k}} .
\]
We conclude that equation (9) has the form
\[
\prod_{j=1}^{k} a_{\mu_{i_0,j}} = \prod_{j=1}^{k} a_{\mu_{i_1,j}}
\]
where \( i_0 \neq i_1 \).

Case (C). Suppose that there exists \( i_0 \in [1, t] \) such that \( c_{i_0} < 0 \). Similarly as in Case (B) we infer that equation (9) has the form
\[
\prod_{j=1}^{k} a_{\mu_{i_0,j}} = \prod_{j=1}^{k} a_{\mu_{i_1,j}}
\]
where \( i_1 \neq i_0 \).
Finally, we show that the chain \( \{M_a\}_{a \leq \kappa} \) just constructed satisfies condition (5). This follows from the following lemma.

**Lemma 3.** If \( x_\delta = m_1 \ldots m_k \), where \( m_i \in \bigcup_{a \leq \kappa} M_a \), then \( x_i \in M_{\beta+1} \) for every \( i \in [1, k] \).

**Proof of Lemma 3.** Suppose that \( x_\delta = m_1 \ldots m_k \) where \( m_i \in \bigcup_{a \leq \kappa} M_a \). Put \( \gamma = \min \{ \alpha; \{ m_1, \ldots, m_k \} \subseteq M_\alpha \} \). Clearly \( \gamma = \delta + 1 \) is a successor ordinal. Our purpose is to show that \( M_\beta \supseteq M_\delta \). Let us suppose on the contrary that \( M_\beta \not\supseteq M_\delta \). Then \( M_{\beta+1} \subseteq M_\delta \). Since \( f(x_\beta) > 0 \), there are \( n_1, \ldots, n_k \in M_{\beta+1} \) such that \( x_\beta = n_1 \ldots n_k \). By Lemma 1 applied to the set \( M_\delta \), the equation \( n_1 \ldots n_k = m_1 \ldots m_k \) implies that \( n_1 \ldots n_k = x_\delta \). Thus \( x_\delta = x_\beta \) and \( \delta = \beta \), a contradiction.

According to Lemma 3, condition (5) follows from the construction of the set \( M_{\beta+1} \), (4) and Lemma 2.

**Remark 2.** Conditions (1) and (2) in Theorem 2 can be clearly replaced by the following two conditions:

(1*) \( |X| \) is a singular cardinal and

(2*) there is a cardinal \( \kappa < |X| \) such that \( |\{ x; x^r = a \}| \leq \kappa \) for every \( a \in X \) and \( r \in [2, 2k] \).

Finally, we give some examples which illustrate the previous results.

**Example 1.** (a) The semigroup \((\mathbb{N}, \cdot)\) has property \( E(k) \) for every \( k \geq 2 \).

(b) Let \( S = (\mathbb{Q}, \cdot) \) where \( \mathbb{Q} \) is the set of all positive quotients. Then for every function \( f: \mathbb{Q} \to \mathbb{N} \) there is a set \( M \subseteq \mathbb{Q} \) such that \( f_M = f \).

**Example 2.** (a) Let \( S = (\mathbb{Z}, +) \) where \( \mathbb{Z} \) is the set of all integers. Then for every function \( f: \mathbb{Z} \to \mathbb{N} \) there is a set \( M \subseteq \mathbb{Q} \) such that \( f_M = f \).

(b) An old problem of P. Erdös: Is it true that the semigroup \((\mathbb{N}, +)\) has property \( E(2) \)?

**References**


*Author's address:* 150 00 Praha 5, Lovčenská 11, Czechoslovakia.