Czechoslovak Mathematical Journal

Vladimír Puš

On multiplicative bases in abelian groups

Czechoslovak Mathematical Journal, Vol. 41 (1991), No. 2, 282–287

Persistent URL: http://dml.cz/dmlcz/102461

Czechoslovak Mathematical Journal, 41 (116) 1991, Praha

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 $x = m_1 . m_2 . \ldots . m_k$, where $m_i \in M$ for $i = 1, 2, \ldots, k$. (Two expressions $x = m_1 . \ldots . m_k$ and $x = m'_1 . \ldots . m'_k$ 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 if $f_{M,k}(x) > 0$ 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. Erdös 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. Erdös 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 $y = x . z$.

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 $x = y . j$.

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 $x_1 \,.\, x_2 \,.\, \ldots \,.\, x_k$ of the elements of F. Further we put $\prod \emptyset = 1$, 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 $\prod F = x_1 \,.\, x_2$ 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 $k \geqq 2$.*

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 $k \geqq 2$.

In the present paper we show that, in contrast with Theorem 1, for infinite Abelian groups with the property that every equation $x^r = a$, $r \geqq 2$, 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 $m \leqq n$, then $[m, n]$ denotes the set of all integers x such that $m \leqq x \leqq n$.

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

(1) $\quad |X| = \varkappa$ *is a regular cardinal and*

(2) $\quad |\{x;\, x^r = a\}| < \varkappa$ *for every* $a \in X$ *and* $r \in [2, 2k]$.

Then for every function $f: X \to \varkappa \setminus \{0\}$ 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′):

(2′) $\quad |\{x;\, x^p = a\}| < \varkappa$ for every $a \in X$ and for every prime number $p \in [2, 2k]$.

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

(0) $\quad M_0 = \emptyset$,

(1) $M_\beta \subseteq M_\alpha$ for $\beta < \alpha$,

(2) $|M_\alpha| < \varkappa$,

(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_α, and

(4) every element x_β for $\beta \geqq \alpha$ can be expressed in at most one way as a product of k elements (not necessarily distinct) of M_α.

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

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

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

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

$$\lambda + f_{M_\alpha,k}(x_\alpha) = f(x_\alpha) .$$

(Clearly $f_{M_\alpha,k}(x_\alpha) \in \{0, 1\}$ by (4).) If $\lambda = 0$ then we put $M_{\alpha+1} = M_\alpha$. Let us suppose that $\lambda > 0$. First we construct a set $\{a_{\mu,j}; \mu < \lambda \,\&\, j \in [1, k-1]\}$ satisfying the following condition (C):

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

(Since $|M_\alpha| < \varkappa$ and $\lambda < \varkappa$, we have $|M_\alpha \cup \{a_{\nu,l}; (\nu, l) \lessdot (\mu, j)\}| < \varkappa$ and thus $a_{\mu,j}$'s can be constructed by recursion because all equations $x^r . c = d$ have less than $\varkappa$ solutions and the number of equations is less than $\varkappa$.)

Let us notice that (C) implies in particular that $a_{\mu,j}$'s do not belong to M_α and are pairwise distinct.

Finally, we define $a_{\mu,k}$ to be an arbitrary (but fixed) solution of the equation $x . a_{\mu,1} . a_{\mu,2} . \ldots . a_{\mu,k-1} = x_\alpha$, and put $M_{\alpha+1} = M_\alpha \cup \{a_{\mu,j}; \mu < \lambda \,\&\, j \in [1, k]\}$.

Clearly, the set $M_{\alpha+1}$ satisfies (1) and (2). Let us verify (3). For every $x \in X$ we put $x^0 = 1$ where 1 is the identity element. Suppose that

(6) $$m_1 . \ldots . m_r . \Big(\prod_{j=1}^{k} a_{\mu_1,j}^{p_1,j}\Big) . \ldots . \Big(\prod_{j=1}^{k} a_{\mu_t,j}^{p_t,j}\Big) =$$
$$= n_1 . \ldots . n_s . \Big(\prod_{j=1}^{k} a_{\mu_1,j}^{q_1,j}\Big) . \ldots . \Big(\prod_{j=1}^{k} a_{\mu_t,j}^{q_t,j}\Big)$$

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

$$(7) \qquad (m_1 \cdot \ldots \cdot m_r \cdot (\prod_{j=1}^{k-1} a_{\mu_1,j}^{p_{1,j}-p_{1,k}}) \cdot \ldots \cdot (\prod_{j=1}^{k-1} a_{\mu_t,j}^{p_{t,j}-p_{t,k}} \cdot x_\alpha^{\sum_{i=1}^{t} p_{i,k}} =$$

$$= n_1 \cdot \ldots \cdot n_s \cdot (\prod_{j=1}^{k-1} a_{\mu_1,j}^{q_{1,j}-q_{1,k}}) \cdot \ldots \cdot (\prod_{j=1}^{k-1} a_{\mu_t,j}^{q_{t,j}-q_{t,k}}) \cdot x_\alpha^{\sum_{i=1}^{t} q_{i,k}} .$$

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 $r + \sum_{i,j} p_{i,j} \geqq k$, 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 $m_1 \cdot \ldots \cdot m_r = n_1 \cdot \ldots \cdot n_s$. By the induction hypothesis, the expressions $m_1 \cdot \ldots \cdot m_r$ and $n_1 \cdot \ldots \cdot n_s$ are identical, thus the expressions on the left and on the right hand side of (6) are identical, too. This concludes the proof that $M_{\alpha+1}$ satisfies condition (3).

Condition (4) follows from the following two lemmas.

Lemma 1. *If*

$$(8) \qquad m_1 \cdot \ldots \cdot m_k = n_1 \cdot \ldots \cdot n_s \cdot (\prod_{j=1}^{k} a_{\mu_1,j}^{p_{1,j}}) \cdot \ldots \cdot (\prod_{j=1}^{k} a_{\mu_t,j}^{p_{t,j}}) ,$$

where $m_1, \ldots, m_k \in M_\alpha$, $n_1, \ldots, n_s \in M_\alpha$, $\mu_1, \ldots, \mu_t$ *are pairwise distinct,* $p_{i,j} \geqq 0$, $s + \sum_{i,j} p_{i,j} = k$ *and* $s < k$, *then* $m_1 \cdot \ldots \cdot m_k = x_\alpha$.

Lemma 2. *Suppose that*

$$(9) \qquad m_1 \cdot \ldots \cdot m_r \cdot (\prod_{j=1}^{k} a_{\mu_1,j}^{p_{1,j}}) \cdot \ldots \cdot (\prod_{j=1}^{k} a_{\mu_t,j}^{p_{t,j}}) =$$

$$= n_1 \cdot \ldots \cdot n_s \cdot (\prod_{j=1}^{k} a_{\mu_1,j}^{q_{1,j}}) \cdot \ldots \cdot (\prod_{j=1}^{k} a_{\mu_t,j}^{q_{t,j}}) ,$$

where $m_1, \ldots, m_r \in M_\alpha$, $n_1, \ldots, n_s \in M_\alpha$, $\mu_1, \ldots, \mu_t$ *are pairwise distinct,* $p_{i,j} \geqq 0$, $q_{i,j} \geqq 0$, $r + \sum_{i,j} p_{i,j} = s + \sum_{i,j} q_{i,j} = k$ *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* $a_{\mu,1} \cdot \ldots \cdot a_{\mu,k} = a_{\nu,1} \cdot \ldots \cdot a_{\nu,k}$, *where* $\mu, \nu < \lambda$ *and* $\mu \neq \nu$.

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

$$m_1 \cdot \ldots \cdot m_k = n_1 \cdot \ldots \cdot n_s \cdot (\prod_{j=1}^{k-1} a_{\mu_1,j}^{p_{1,j}-p_{1,k}}) \cdot \ldots \cdot (\prod_{j=1}^{k-1} a_{\mu_t,j}^{p_{t,j}-p_{t,k}}) \cdot x_\alpha^{\sum_{i=1}^{t} p_{i,k}} .$$

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 $m_1 \ldots . m_k = x_\alpha$.

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

$$m_1 \ldots . m_r = n_1 \ldots . n_s . \tag{10}$$

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 $c_i \leqq 0$ for every $i \neq i_0$. In particular, the expression on the left had 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

$$\prod_{j=1}^{k} a_{\mu_{i_1},j} = \prod_{j=1}^{k} a_{\mu_{i_0},j}$$

where $i_1 \neq i_0$.

Finally, we show that the chain $\{M_\alpha\}_{\alpha<\varkappa}$ just constructed satisfies condition (5). This follows from the following lemma.

Lemma 3. *If* $x_\beta = m_1 \ldots . m_k$, *where* $m_i \in \bigcup_{\alpha<\varkappa} M_\alpha$, *then* $m_i \in M_{\beta+1}$ *for every* $i \in [1, k]$.

Proof of Lemma 3. Suppose that $x_\beta = m_1 \ldots . m_k$ where $m_i \in \bigcup_{\alpha<\varkappa} M_\alpha$. 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 $M_\beta \subsetneqq M_\delta$. 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_δ, 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 $\varkappa < |X|$ such that $|\{x;\ x^r = a\}| \leqq \varkappa$ for every $a \in X$ and $r \in [2, 2k]$.

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

Example 1. (α) The semigroup $(\mathbb{N}, \cdot)$ has property $E(k)$ for every $k \geqq 2$.

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

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

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

References

[1] *P. Erdös:* On the multiplicative representation of integers, Israel J. Math. *2* (1964), 251—261.

[2] *P. Erdös, P. Turán:* On a problem of Sidon in additive number theory, and on some related problems, J. London Math. Soc. *16* (1941), 212—215.

[3] *M. B. Nathanson:* Multiplicative representation of integers, Israel J. Math. *57* (1987), 129—136.

[4] *J. Nešetřil, V. Rödl:* Two proofs in combinatorial number theory, Proc. Amer. Math. Soc. *93*, (1985), 185—188.

[5] *V. Puš:* Combinatorial properties of products of graphs, Czech. Math. J. *41* (1991), 269—277.

[6] *V. Puš:* On multiplicative bases in commutative semigroups (to appear to Europ. J. Combinatorics).

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