



ИТОГИ НАУКИ И ТЕХНИКИ.  
Современная математика и ее приложения.  
Тематические обзоры.  
Том 204 (2022). С. 27–36  
DOI: 10.36535/0233-6723-2022-204-27-36

УДК 511.348

## МУЛЬТИПОТЕНТНЫЕ МНОЖЕСТВА В ОДНОРОДНЫХ КОММУТАТИВНЫХ МОНОИДАХ

© 2022 г. Ю. П. ВИРЧЕНКО

**Аннотация.** Введено понятие о  $k$ -потентных множествах в моноидах,  $k \in \mathbb{N}$ , установлены их простейшие свойства. Выделен класс однородных моноидов, обладающих набором образующих элементов. Найдены простейшие необходимые условия того, чтобы фиксированное множество в таком моноиде было  $k$ -потентным. При наличии коммутативности в моноидах установлен изоморфизм каждого из них моноиду  $\mathbb{N}_+^{\mathfrak{J}}$  с соответствующим ему множеством меток  $\mathfrak{J}$ . Для коммутативных однородных моноидов, обладающих множеством образующих, доказаны необходимые и достаточные условия  $k$ -потентности их подмножеств. Описано приложение этого результата к анализу так называемой бинарной проблемы Гольдбаха в аналитической теории чисел.

**Ключевые слова:** коммутативность, моноид, мультипотентное множество, однородность, простое число, цикл.

## MULTIPOTENT SETS IN HOMOGENEOUS COMMUTATIVE MONOIDS

© 2022 Yu. P. VIRCHENKO

**ABSTRACT.** In this paper, we introduce the concept of  $k$ -potent sets in monoids,  $k \in \mathbb{N}$ , establish their simplest properties, and indicate a class of homogeneous monoids with a set of generating elements. We find simple necessary conditions of the  $k$ -potency of a fixed set in such a monoid. For commutative monoids, we establish an isomorphism between them and the monoid  $\mathbb{N}_+^{\mathfrak{J}}$  with the corresponding label set  $\mathfrak{J}$ . For commutative homogeneous monoids with sets of generators, we prove necessary and sufficient conditions for the  $k$ -potency of their subsets. Finally, we apply this result to the binary Goldbach problem in analytic number theory.

**Keywords and phrases:** commutativity, monoid, multipotent set, homogeneity, prime number, cycle.

**AMS Subject Classification:** 06F05, 20M14, 11P32

**1. Введение.** Понятие о мультипотентных, в частности, квадратентных множествах в моноидах возникает, естественным образом, как обобщение представления о множествах, которые являются объектом изучения в некоторых задачах теории чисел, связанных с суммами чисел со специальными свойствами. Таковыми являются, например, задача о представлении чисел из  $\mathbb{N}$  в виде сумм  $n$ -х степеней фиксированного числа натуральных чисел — так называемая проблема Варинга (см. [8]) — или задача о представлении всех нечетных чисел в виде сумм трех простых чисел — проблема Гольдбаха (см. [7]). Замечательно, что при алгебраическом анализе указанных задач оказывается важным только лишь то, что на изучаемом множестве  $\mathfrak{A}$  элементов задана бинарная алгебраическая ассоциативная операция коммутативной композиции, которую будем в дальнейшем обозначать знаком  $+$ , так что для любых двух элементов  $x \in \mathfrak{A}$ ,  $y \in \mathfrak{A}$  определен элемент  $x + y \in \mathfrak{A}$ . Задание ассоциативной операции превращает множество  $\mathfrak{A}$  в *полугруппу*,

в частности, коммутативную. В связи с таким положением, настоящая работа посвящена описанию общей абстрактной постановки и выработки подхода к решению указанных выше и родственных им задач.

Пусть  $\mathfrak{A}$  — полугруппа с единицей  $e$ , в общем случае, некоммутативная, т.е.  $\mathfrak{A}$  является моноидом<sup>1</sup> (см. [1]). Операцию композиции обозначим посредством  $*$ . В соответствии с этим, степень  $d$  любого элемента  $x \in \mathfrak{A}$  будем обозначать посредством  $x_*^d$ . Наличие единицы не ограничивает общности рассмотрения, так как любую полугруппу  $\mathfrak{A}$ , при отсутствии в ней единицы, всегда можно дополнить новым элементом  $e$ , который обладает свойствами единицы, т.е. для любого элемента  $x \in \mathfrak{A}$  имеет место  $x * e = e * x = x$ , при этом расширив таблицу умножения в  $\mathfrak{A}$ .

Определим на основе операции  $*$  в моноиде  $\mathfrak{A}$  аналогичную операцию на классе  $P(\mathfrak{A}) = \{\mathfrak{B} \subset \mathfrak{A} : \mathfrak{B} \neq \emptyset\}$  всех непустых подмножеств из  $\mathfrak{A}$ . Пусть  $\mathfrak{B}_j \subset \mathfrak{A}$ ,  $j = 1, 2$  — любая пара подмножеств из  $\mathfrak{A}$ . Определим подмножество

$$\mathfrak{B}_1 * \mathfrak{B}_2 = \{x \in \mathfrak{B} : x = y_1 * y_2, y_j \in \mathfrak{B}_j, j = 1, 2\} \subset \mathfrak{A}. \quad (1)$$

Отображение  $\mathfrak{A} \times \mathfrak{A} \mapsto \mathfrak{A}$ , которое паре  $\langle \mathfrak{B}_1, \mathfrak{B}_2 \rangle$  ставит в соответствие множество (1), определяет на классе  $P(\mathfrak{A})$  бинарную ассоциативную и коммутативную операцию и тем самым превращает этот класс в коммутативный моноид, единицей которого служит одноэлементное подмножество  $\{e\}$ . На основе операции  $*$  на классе  $P(\mathfrak{A})$  вводится понятие о степени  $d \in \mathbb{N}$  любого подмножества  $\mathfrak{B} \subset \mathfrak{A}$ , которую будем обозначать, так же как и выше, посредством  $\mathfrak{B}_*^d$ . Именно, для любого  $d \in \mathbb{N}$  положим  $\mathfrak{B}_*^{d+1} = \mathfrak{B}_*^d * \mathfrak{B}$ ,  $d \in \mathbb{N}$  и, посредством этого соотношения, определим, индуктивным образом, множества  $\mathfrak{B}_*^d$ ,  $d \in \mathbb{N}$ .

Введем теперь базовое понятие  $k$ -потентного множества.

**Определение 1.** Подмножество  $\mathfrak{B}$  моноида  $\mathfrak{A}$  будем называть мультипотентным порядка  $k \in \mathbb{N}$  ( $k$ -потентным), если имеет место равенство

$$\mathfrak{B}_*^k = \mathfrak{A}.$$

В частности, при  $k = 2$  такое множество  $\mathfrak{B}$  будем называть *квадратопотентным*. Для него имеет место

$$\mathfrak{B}_*^2 = \{x \in \mathfrak{A} : x = y * z, y, z \in \mathfrak{B}\} = \mathfrak{A}. \quad (2)$$

Основной задачей развиваемой далее теории мультипотентных множеств является установление признаков, на основе которых можно было бы судить, является ли  $k$ -потентным заданное подмножество  $\mathfrak{B} \subset \mathfrak{A}$ .

**2. Моноиды.** Пусть  $\mathfrak{B}$  — подмоноид моноида  $\mathfrak{A}$ , т.е. такое подмножество  $\mathfrak{B} \subset \mathfrak{A}$ , которое замкнуто относительно операции  $*$ , так что для любой пары подмножеств  $\mathfrak{B}_j \subset \mathfrak{B}$ ,  $j = 1, 2$ , имеет место  $\mathfrak{B}_1 * \mathfrak{B}_2 \subset \mathfrak{B}$ .

**Определение 2.** Пусть  $\mathfrak{C} \subset \mathfrak{A}$ . Подмоноид  $M(\mathfrak{C})$  называется минимальным по отношению к  $\mathfrak{C}$ , если любой подмоноид  $\mathfrak{B}$ , содержащий  $\mathfrak{C}$ , обязательно содержит  $M(\mathfrak{C})$ .

Множество  $\mathfrak{C}$  будем называть *порождающим* минимальный моноид  $M(\mathfrak{C})$ . В частности, если  $\mathfrak{C} \subset \mathfrak{A}$  и  $M(\mathfrak{C}) = \mathfrak{A}$ , то  $\mathfrak{C}$  порождает моноид  $\mathfrak{A}$ .

**Теорема 1.** Для любого моноида  $\mathfrak{A}$  и любого множества  $\mathfrak{C} \subset \mathfrak{A}$  существует единственный минимальный моноид  $M(\mathfrak{C}) \subset \mathfrak{A}$ .

*Доказательство.* Рассмотрим множество

$$\mathfrak{B} = \bigcup_{d=0}^{\infty} \mathfrak{C}_*^d, \quad \mathfrak{C}_*^0 = \{e\}.$$

Пусть  $x_j$ ,  $j = 1, \dots, d$  — набор любых отличных от  $e$  элементов моноида, не обязательно различных между собой. Тогда элемент  $x_1 * \dots * x_d \in \mathfrak{B}_*^d$  и, точно так же, согласно определению моноида,

<sup>1</sup>По поводу общих свойств полугрупп см., например, [3, 6].

он принадлежит любому моноиду, содержащему элементы  $x_j$ ,  $j = 1, \dots, d$ . Следовательно, любой такой элемент принадлежит  $M(\mathfrak{C})$  и поэтому, ввиду произвольности  $d \in \mathbb{N}$ ,  $M(\mathfrak{C}) \supset \mathfrak{B}$ .

С другой стороны,  $\mathfrak{B}$  является моноидом ввиду замкнутости этого множества относительно операции  $*$ . В самом деле, если  $y_j \in \mathfrak{B}$ ;  $j = 1, 2$ , то существуют такие числа  $d_1 \in \mathbb{N}_+$  и  $d_2 \in \mathbb{N}_+$ , что  $y_j \in \mathfrak{B}_*^{d_j}$ ;  $j = 1, 2$ . Тогда существуют такие последовательности  $\langle x_1^{(j)}, \dots, x_{d_j}^{(j)} \rangle$  элементов из  $\mathfrak{C}$ , что  $y_j = x_1^{(j)} \dots x_{d_j}^{(j)}$ ,  $j = 1, 2$ . Отсюда следует, что

$$y_1 * y_2 = x_1^{(1)} * \dots * x_{d_1}^{(1)} * x_1^{(2)} * \dots * x_{d_2}^{(2)} \in \mathfrak{B}_*^{d_1} * \mathfrak{B}_*^{d_2} = \mathfrak{B}_*^{d_1+d_2},$$

т.е.  $y_1 * y_2 \in \mathfrak{B}$ .

Так как  $\mathfrak{B}$  — моноид, содержащий  $\mathfrak{C}$ , то  $\mathfrak{B} \supset M(\mathfrak{C})$ . Из полученных двух противоположных включений следует, что  $\mathfrak{B} = M(\mathfrak{C})$ .  $\square$

**Следствие 1.** Минимальный моноид  $M(\mathfrak{C})$ , порожденный множеством  $\mathfrak{C} \subset \mathfrak{A}$ , состоит из всех произведений  $x = x_1 * x_2 * \dots * x_l$ , составляемых из компонент последовательностей  $\langle x_1, x_2, \dots, x_l \rangle$ , где  $x_j \in \mathfrak{C}$ ,  $j = 1, \dots, l$ ,  $l \in \mathbb{N}$ . Если моноид  $\mathfrak{A}$  коммутативен, то элементы  $x$  моноида  $M(\mathfrak{C})$  определяются множеством пар  $\{\langle y_j, m_j \rangle; j = 1, \dots, d\}$ , где  $x_j$  — различные элементы из  $\mathfrak{C}$ ,  $m_j \in \mathbb{N}$ ,  $j = 1, \dots, d$  и каждый из них представим в виде  $m_1 y_1 + \dots + m_d y_d$ ,  $m_1 + \dots + m_d = l$  с  $m_j y_j \equiv (y_j)_+^{m_j}$ ,  $j = 1, \dots, d$ .

**Определение 3.** Если для моноида  $\mathfrak{A}$  найдется такое порождающее его множество  $\mathfrak{B}_0$ , которое не содержит в себе никакого другого множества, порождающего моноид  $\mathfrak{A}$ , то множество  $\mathfrak{B}_0$  называется системой образующих элементов моноида  $\mathfrak{A}$ , а его элементы — образующими моноида.

**Замечание 1.** Для заданного моноида  $\mathfrak{A}$  система образующих не обязана существовать.

**Замечание 2.** Если для элемента  $x$  моноида  $\mathfrak{A}$  определен обратный ему элемент  $y$  такой, что  $x * y = e$  (в частности, такое положение имеет место, если  $\mathfrak{A}$  является группой с операцией  $*$ ), и если  $x \in \mathfrak{B}_0$ , то с точки зрения Определения 3  $x^{-1}$  может входить в  $\mathfrak{B}_0$  как независимый элемент.

Если множество  $\mathfrak{A}$  конечно, то соответствующий моноид с операцией  $*$  будем называть конечным. В противном случае бесконечным. Приведем пример простейшего конечного моноида.

**Пример 1.** Моноид  $\mathfrak{A} = \{0, 1, 2, \dots, d-1\}$ ,  $d \geq 2$ , с операцией  $*$  сложения по модулю  $d$  и единичным элементом  $e = 0$ . Этот моноид конечен, коммутативен и имеет один образующий элемент  $x = 1$ .

Заметим, что в случае, когда моноид  $\mathfrak{A}$  обладает множеством образующих, и он является минимальным для некоторого множества  $\mathfrak{C} \subset \mathfrak{A}$ ,  $M(\mathfrak{C}) = \mathfrak{A}$ , совсем не обязательно, что образующие принадлежат  $\mathfrak{C}$ . В моноиде примера 1 при  $d = 6$  множество  $\mathfrak{C} = \{2, 3\}$  его порождает, но содержит образующий элемент моноида — число 1.

**Определение 4.** Будем говорить, что моноид  $\mathfrak{A}$  содержит цикл, если в нем существует такой элемент  $a$ , для которого имеются последовательности  $\langle x_1, \dots, x_m \rangle$  и  $\langle y_1, \dots, y_n \rangle$  такие, что выполняется равенство  $x_1 * \dots * x_m * a * y_1 * \dots * y_n = a$ .

Моноид примера 1 содержит цикл, у которого  $a = e = 0$ ,  $d = n$  и  $y_j = 1$ ,  $j = 1, \dots, n$ , так как  $1_+^n = \underbrace{(1 + \dots + 1)}_n \bmod n = 0$  и  $x_i = 0$ ,  $i = 1, \dots, m$ .

Легко видеть, что в конечных моноидах всегда имеется цикл, так как взяв произвольный элемент  $z$  конечного моноида  $\mathfrak{A}$  и построив последовательность  $\langle z_*^l; l = 1, \dots, n \rangle$ , ввиду конечности  $\mathfrak{A}$ , для любого элемента  $z_*^m \equiv a$ , при достаточно большом  $n > m$ , что выполняется  $a * z_*^{n-m} = a$ .

Заметим также, что если моноид  $\mathfrak{A}$  с операцией  $*$  для какого-то элемента  $x$  имеет обратный элемент  $x^{-1}$ ,  $e = x * x^{-1}$  и, в частности, если моноид является группой относительно этой операции, то он, тривиальным образом, содержит цикл  $x = x * x^{-1} * x$ .

В настоящей работе будем рассматривать моноиды, у которых отсутствуют циклы.

**Определение 5.** Если в моноиде  $\mathfrak{A}$  отсутствуют циклы, то такой моноид назовем направленным.

**Теорема 2.** Если моноид  $\mathfrak{A}$  направленный и обладает набором  $\mathfrak{B}_0$  образующих его элементов, то этот набор определен однозначным образом.

*Доказательство.* Положим имеются два набора  $\mathfrak{B}_0$  и  $\mathfrak{B}'_0$  образующих элементов так, что их симметрическая разность не пуста  $(\mathfrak{B}'_0 \setminus \mathfrak{B}_0) \cup (\mathfrak{B}_0 \setminus \mathfrak{B}'_0) \neq \emptyset$ . Положим, для определенности, что  $x \in \mathfrak{B}_0 \setminus \mathfrak{B}'_0 \neq \emptyset$ . Тогда этот элемент представим в виде композиции образующих набора  $\mathfrak{B}'_0$ :

$$x = x'_1 * \dots * x'_l, \quad x'_j \in \mathfrak{B}'_0, \quad j = 1, \dots, l.$$

В свою очередь, каждая из образующих  $x'_j$  представима в виде композиции образующих элементов из набора  $\mathfrak{B}_0$ :

$$x'_j = x_{k_1^{(j)}} * \dots * x_{k_{m_j}^{(j)}}; \quad x_{k_s^{(j)}} \in \mathfrak{B}_0, \quad s = 1, \dots, m_j; \quad j = 1, \dots, l.$$

Отсюда следует, что

$$x = (x_{k_1^{(1)}} * \dots * x_{k_{l_1}^{(1)}}) * \dots * (x_{k_1^{(l)}} * \dots * x_{k_{m_l}^{(l)}}). \quad (3)$$

Если в последовательности сомножителей присутствует элемент  $x$ , как один из образующих элементов моноида  $\mathfrak{A}$ , то это означает, что в  $\mathfrak{A}$  имеется цикл и это противоречит направленности моноида. Если же в этой последовательности элемент  $x$  отсутствует, то это противоречит тому, что он входит в набор образующих элементов, так как ввиду представления в виде (3) его можно исключить из набора  $\mathfrak{B}_0$ .  $\square$

Целью настоящей работы является изучение направленных и, следовательно, бесконечных моноидов. Приведем примеры таких моноидов. Имея в виду предмет настоящей работы, все моноиды в приводимых ниже примерах коммутативны.

В примерах 2–5 числовое множество  $\mathfrak{A}$  имеют счетную мощность. Это, во-первых, направленные моноиды, связанные с натуральными числами.

**Пример 2.** Моноид  $\mathfrak{A} = \mathbb{N} \cup \{0\} = \mathbb{N}_+ = \{0, 1, 2, 3, \dots\}$  с операцией сложения натуральных чисел. Он имеет одну образующую  $1 \in \mathbb{N}_+$ . Единицей моноида является  $\{0\}$ .

**Пример 3.** Моноид  $\mathbb{N} = \{1, 2, 3, \dots\}$  с операцией умножения натуральных чисел. Используя основную теорему арифметики [2], заключаем, что он имеет бесконечный набор образующих, которые представляются множеством простых натуральных чисел  $\mathfrak{P}$ .

Следующие примеры связаны с рациональными числами.

**Пример 4.** Направленный моноид  $\mathfrak{A} = \mathbb{Q} = \{p/q \in \mathbb{Q} : p \in \mathbb{N}, q \in \mathbb{N}\}$ , состоящий из положительных рациональных чисел. Он имеет бесконечный набор образующих, который состоит из всех дробей  $p/q$ , у которых числитель и знаменатель являются не равными друг другу простыми числами.

**Пример 5.** Моноид  $\mathbb{Q}_+ = \mathbb{Q} \cup \{0\}$  с операцией сложения рациональных чисел. Он является направленным, но не обладает множеством образующих. Последнее связано с тем, что любое множество  $\mathfrak{B}$  дробей  $p/q \in \mathbb{Q}_+$ , которое могло бы быть множеством образующих, и любого интервала  $(0, s^{-1})$ ,  $s \in \mathbb{N}$ , можно сузить, ограничив его только дробями из  $\mathfrak{B} \cap (0, s^{-1})$ .

Моноиды, связанные с положительными действительными числами, которые имеют мощность континуума.

**Пример 6.** Моноиды с множествами  $\mathfrak{A} = (0, \infty)$  и  $\mathfrak{A} = [0, \infty)$  с операциями умножения и сложения действительных чисел, соответственно. Они не имеют множества образующих по причине, указанной в предыдущем примере.

Дальнейшие примеры направленных моноидов, в конструкции которых используются числовые множества, строятся на основе каждого из моноидов, указанных в примерах 2–6, посредством построения их декартовых степеней, кратность которых (показатель декартовой степени) может

быть как конечной, так и бесконечной. В последнем случае кратность декартовой степени может иметь любое бесконечное кардинальное число. При этом операция композиции в конструируемых моноидах получается в виде покомпонентного применения операции композиции в моноидах, входящих в состав декартовой степени. Легко видеть, что для всех таких моноидов реализуется точно такая же ситуация с точки зрения существования в них множества образующих.

**3. Минимальные  $k$ -потентные множества.** Прежде всего, отметим справедливость простейших утверждений, связывающих операцию композиции в моноиде с булевыми операциями.

**Лемма 1.** *Для любых подмножеств  $\mathfrak{B}_j$ ,  $j = 1, 2$ ;  $\mathfrak{C}$  моноида  $\mathfrak{A}$  имеют место равенства*

$$(\mathfrak{B}_1 \cup \mathfrak{B}_2) * \mathfrak{C} = (\mathfrak{B}_1 * \mathfrak{C}) \cup (\mathfrak{B}_2 * \mathfrak{C}), \quad (\mathfrak{B}_1 \cap \mathfrak{B}_2) * \mathfrak{C} = (\mathfrak{B}_1 * \mathfrak{C}) \cap (\mathfrak{B}_2 * \mathfrak{C}). \quad (4)$$

*Доказательство.* Положив, что  $x \in \mathfrak{B}_1 \cup \mathfrak{B}_2$  и  $y \in \mathfrak{C}$ , т.е.  $x * y \in (\mathfrak{B}_1 \cup \mathfrak{B}_2) * \mathfrak{C}$ , где, не ограничивая общности,  $x \in \mathfrak{B}_1$ , получим, что  $x * y \in \mathfrak{B}_1 * \mathfrak{C}$  и, следовательно,  $x * y \in (\mathfrak{B}_1 * \mathfrak{C}) \cup (\mathfrak{B}_2 * \mathfrak{C})$ . Таким образом, ввиду произвольности  $x$  и  $y$ ,  $(\mathfrak{B}_1 \cup \mathfrak{B}_2) * \mathfrak{C} \subset (\mathfrak{B}_1 * \mathfrak{C}) \cup (\mathfrak{B}_2 * \mathfrak{C})$ . Обратное включение доказывается аналогично и поэтому выполняется первое из равенств (4).

Пусть теперь  $x \in \mathfrak{B}_1 \cap \mathfrak{B}_2$  и, как и ранее,  $y \in \mathfrak{C}$ . Тогда  $x \in \mathfrak{B}_1$  и  $x \in \mathfrak{B}_2$ . Поэтому  $x * y \in \mathfrak{B}_1 * \mathfrak{C}$  и, одновременно,  $x * y \in \mathfrak{B}_2 * \mathfrak{C}$ . Следовательно,  $x * y \in (\mathfrak{B}_1 * \mathfrak{C}) \cap (\mathfrak{B}_2 * \mathfrak{C})$ . Ввиду произвольности элементов  $x$  и  $y$  имеет место включение  $(\mathfrak{B}_1 \cap \mathfrak{B}_2) * \mathfrak{C} \subset (\mathfrak{B}_1 * \mathfrak{C}) \cap (\mathfrak{B}_2 * \mathfrak{C})$ . Обратное включение доказывается аналогично и поэтому выполняется второе равенство в (4).  $\square$

Индукцией по числу компонент, входящих, соответственно, в объединение и пересечение подмножеств моноида  $\mathfrak{A}$ , используя формулы (4), убеждаемся в справедливости следующих равенств.

**Следствие 2.** *Для любого семейства множеств  $\mathfrak{B}_j \subset \mathfrak{A}$ ,  $j \in \Sigma$ , и любого множества  $\mathfrak{C} \subset \mathfrak{A}$  имеют место равенства*

$$\left( \bigcup_{j \in \Sigma} \mathfrak{B}_j \right) * \mathfrak{C} = \bigcup_{j \in \Sigma} (\mathfrak{B}_j * \mathfrak{C}), \quad \left( \bigcap_{j \in \Sigma} \mathfrak{B}_j \right) * \mathfrak{C} = \bigcap_{j \in \Sigma} (\mathfrak{B}_j * \mathfrak{C}). \quad (5)$$

Из формул (5) получаем следующее утверждение.

**Следствие 3.** *Для любых семейств множеств  $\mathfrak{B}_j \subset \mathfrak{A}$ ,  $j \in \Sigma$  и  $\mathfrak{C}_k \subset \mathfrak{A}$ ,  $k \in \Gamma$  имеют место равенства*

$$\left( \bigcup_{j \in \Sigma} \mathfrak{B}_j \right) * \left( \bigcup_{k \in \Gamma} \mathfrak{C}_k \right) = \bigcup_{j \in \Sigma, k \in \Gamma} (\mathfrak{B}_j * \mathfrak{C}_k), \quad \left( \bigcap_{j \in \Sigma} \mathfrak{B}_j \right) * \left( \bigcap_{k \in \Gamma} \mathfrak{C}_k \right) = \bigcap_{j \in \Sigma, k \in \Gamma} (\mathfrak{B}_j * \mathfrak{C}_k). \quad (6)$$

Обратимся к изучению мультипотентных множеств в направленных моноидах.

**Определение 6.**  $k$ -потентное подмножество  $\mathfrak{B}_\infty$  моноида  $\mathfrak{A}$  будем называть минимальным, если оно не содержит в себе собственного подмножества  $\mathfrak{B}$ , которое является мультипотентным порядка  $k$  для моноида  $\mathfrak{A}$ .

Очевидно, что в силу данного определения любое  $k$ -потентное множество одновременно является  $l$ -потентным при любом  $l > k$ .

В отличие от понятия системы образующих элементов моноида, которая может отсутствовать, понятие минимального  $k$ -потентного множества обладает универсальностью, так как справедлива следующая теорема.

**Теорема 3.** *В любом моноиде  $\mathfrak{A}$ , для любого множества  $\mathfrak{B} \subset \mathfrak{A}$  и при любом значении  $k \in \mathbb{N}$  имеется по крайней мере одно минимальное  $k$ -потентное множество  $\mathfrak{B}_\infty$ , содержащее  $\mathfrak{B}$ .*

*Доказательство.* Зафиксируем число  $k \in \mathbb{N}$ . Множество  $\mathfrak{A}$  является тривиальным образом  $k$ -потентным, так как  $\mathfrak{A} * \mathfrak{A} = \mathfrak{A}$  и оно содержит  $\mathfrak{B}$ . Допустим, что оно не является минимальным. Тогда существует сужающаяся последовательность  $\langle \mathfrak{B}_n; n \in \mathbb{N} \rangle$   $k$ -потентных множеств,

$\mathfrak{B}_{n+1} \subset \mathfrak{B}_n$ ,  $(\mathfrak{B}_n)_*^k = \mathfrak{A}$ , каждое из которых содержит  $\mathfrak{B}$ , но не является минимальным. Рассмотрим теоретико-множественный предел

$$\mathfrak{B}_\infty = \lim_{n \rightarrow \infty} \mathfrak{B}_n = \bigcap_{n=1}^{\infty} \mathfrak{B}_n.$$

Это множество непусто, оно содержит множество  $\mathfrak{B}$  и является  $k$ -потентным, так как

$$(\mathfrak{B}_\infty)_*^k = \left( \lim_{n \rightarrow \infty} \mathfrak{B}_n \right)_*^k = \lim_{n \rightarrow \infty} (\mathfrak{B}_n)_*^k = \left( \lim_{n \rightarrow \infty} \mathfrak{A} \right)_*^k = \mathfrak{A}. \quad \square$$

**Замечание 3.** При любом  $k \in \mathbb{N}$  минимальное  $k$ -потентное множество, вообще говоря, не единственно.

Допустим, что моноид  $\mathfrak{A}$  направленный. Тогда справедлива следующая теорема.

**Теорема 4.** Любое  $k$ -потентное множество  $\mathfrak{B}$  в направленном моноиде содержит единицу  $e$  моноида.

*Доказательство.* Допустим, что утверждение теоремы не имеет места. Тогда, так как  $\mathfrak{B}_*^k = \mathfrak{A}$  и  $e \in \mathfrak{A}$ , то должны существовать такие элементы  $x_j \in \mathfrak{B}$ ,  $j = 1, \dots, k$ , для которых  $x_1 * \dots * x_k = e$ . Однако ввиду направленности моноида  $\mathfrak{A}$ , т.е. отсутствия в нем циклов, это равенство может иметь место только в случае, когда  $x_j = e$ ,  $j = 1, \dots, k$ .  $\square$

Далее будем предполагать, что моноид  $\mathfrak{A}$ , наряду с направленностью, обладает системой образующих  $\mathfrak{B}_0$ . Тогда справедливо следующее утверждение.

**Теорема 5.** Для любого направленного моноида  $\mathfrak{A}$ , обладающего системой образующих  $\mathfrak{B}_0$ , при любом  $k \in \mathbb{N}$ , каждое  $k$ -потентное множество  $\mathfrak{B}$  содержит  $\mathfrak{B}_0$ .

*Доказательство.* Допустим противное, что в системе  $\mathfrak{B}_0$  образующих элементов моноида  $\mathfrak{A}$  имеется такой элемент  $x$ , который не содержится в  $\mathfrak{B}$ . Тогда, так как  $\mathfrak{B}$  является  $k$ -потентным, то в этом множестве найдется такая последовательность  $\langle y_1, \dots, y_k \rangle$ ,  $y_j \in \mathfrak{B}$ ,  $j = 1, \dots, k$ , что имеет место равенство  $y_1 * \dots * y_k = x$ . Следовательно, так как каждый из элементов  $y_j$  представим в виде композиции  $y_j = x_{k_1^{(j)}} * \dots * x_{k_{m_j}^{(j)}}$ , где ее компонентами  $x_{k_l^{(j)}}$ ,  $l = 1, \dots, m_j$ , являются образующие элементы моноида  $\mathfrak{A}$ ,  $j = 1, \dots, k$ . Подстановка этих разложений элементов  $y_j$ ,  $j = 1, \dots, k$ , в композицию  $y_1 * \dots * y_k = x$  дает представление образующего элемента  $x$  в виде произведения, в состав которого входят только образующие элементы из  $\mathfrak{B}_0$ .

Может реализоваться только один из двух случаев:

- (i) в списке всех компонент последовательностей  $\langle x_{k_1^{(j)}}, \dots, x_{k_{m_j}^{(j)}} \rangle$ ,  $j = 1, \dots, k$ , отсутствует образующий элемент  $x$ ;
- (ii) среди всех компонент последовательностей  $\langle x_{k_1^{(j)}}, \dots, x_{k_{m_j}^{(j)}} \rangle$ ,  $j = 1, \dots, k$ , присутствует элемент  $x$ .

Если имеет место положение (i), то элемент  $x$  не может входить в систему образующих элементов  $\mathfrak{B}_0$  ввиду минимальности ее выбора. Пусть имеет место положение (ii) и  $l$  — номер последнего элемента из числа тех, которые входят в состав композиции  $x = y_1 * \dots * y_k$  и в композиции которого присутствует образующий элемент  $x$ , а  $k_s^{(l)}$  — номер такого элемента в композиции элемента  $y_l$ , что  $x_{k_s^{(l)}}^{(l)} = x$ , так что он представляет последнее вхождение этого образующего элемента в композицию  $y_l = x_{k_1^{(j)}} * \dots * x_{k_{m_j}^{(j)}}$ . Тогда в композиции  $x = y_1 * \dots * y_k$  имеется цикл

$$(y_1 * \dots * y_{l-1} * x_{k_1^{(l)}} * \dots * x_{k_{s-1}^{(l)}}) * x * (x_{k_{s+1}^{(l)}} * \dots * x_{k_{m_l}^{(l)}} * y_{l+1} * \dots * y_k) = x. \quad \square$$

В заключение раздела введем следующее понятие.

**Определение 7.** Направленный моноид  $\mathfrak{A}$ , обладающий набором  $\mathfrak{B}_0$  образующих его элементов, назовем однородным, если имеет место  $(\mathfrak{B}_0)_*^m \cap (\mathfrak{B}_0)_*^n = \emptyset$  при  $n \neq m$ .

**4. Коммутативные моноиды.** В этом разделе рассмотрим более подробно коммутативные однородные моноиды  $\mathfrak{A}$ , которые обладают множеством образующих  $x_j$ ,  $j \in \mathfrak{J}$ , где множество  $\mathfrak{J}$  либо конечно и содержит  $d$  элементов, либо оно бесконечно и обладает  $\text{card}(\mathfrak{J}) = \aleph_s$ ,  $s \in \mathbb{N}_+$ . В связи с этим будем обозначать мощность множества образующих элементов посредством  $d$ , которое либо конечно и принадлежит  $\mathbb{N}$ , либо бесконечно и  $d = \aleph_s$ ,  $s \in \mathbb{N}$ . Операцию композиции в таких моноидах будем обозначать посредством знака  $+$ .

Рассмотрим далее коммутативный моноид  $\mathbb{N}_+^d$ , где операцией композиции является покомпонентное сложение, так что каждый элемент  $\mathbf{a}$  моноида представим в виде

$$\mathbf{a} = \sum_{i \in \mathfrak{J}} m_i x_i \quad (7)$$

с  $m_i \in \mathbb{N}_+$ , где  $\Delta(\mathbf{a}) \subset \mathfrak{J}$  — множество номеров  $i$ , для которых  $m_i \neq 0$  конечно и  $x_i = \langle \delta_{ij}; j \in \mathfrak{J} \rangle$ ,  $i \in \mathfrak{J}$  — множество образующих.

Для любых двух элементов  $\mathbf{a}$  и

$$\mathbf{b} = \sum_{j \in \mathfrak{J}} n_j x_j$$

с  $n_j \in \mathbb{N}_+$ ,  $j \in \mathfrak{J}$  их композиция представляется элементом

$$\mathbf{a} + \mathbf{b} = \sum_{i \in \mathfrak{J}} (m_i + n_i) x_i.$$

**Теорема 6.** Если моноид  $\mathfrak{A}$  обладает набором образующих  $\{x_j; j \in \mathfrak{J}\}$ , коммутативен и однороден, то он изоморфен моноиду  $\mathbb{N}_+^{\mathfrak{J}}$ . При этом единица  $\mathbf{e}$  моноида отображается в  $\mathbf{0} \in \mathbb{N}_+^{\mathfrak{J}}$  и множество образующих  $\mathfrak{B}_0 = \{x_j; j \in \mathfrak{J}\}$  моноида  $\mathfrak{A}$  отображается в множество  $\{\langle \delta_{ij}; j \in \mathfrak{J} \rangle; i \in \mathfrak{J}\}$ .

*Доказательство.* Сопоставим единице  $\mathbf{e} \in \mathfrak{A}$  элемент  $\mathbf{0} \in \mathbb{N}_+^{\mathfrak{J}}$  и образующим  $x_i$  элементам — векторы  $\langle \delta_{ij}; j \in \mathfrak{J} \rangle$ ,  $i \in \mathfrak{J}$  множества  $\mathbb{N}_+^{\mathfrak{J}}$ . Тогда первое утверждение теоремы следует из представления каждого из элементов коммутативного моноида, указанного в следствии теоремы 1. Ввиду отсутствия циклов в моноиде  $\mathfrak{A}$ ,  $\mathbf{e}$  отображение в  $\mathbf{0} \in \mathbb{N}_+^{\mathfrak{J}}$  однозначно.

Принимая во внимание утверждение теоремы 2, замечаем, что множество образующих элементов в однородном моноиде  $\mathfrak{A}$  единственно, и его отображение в моноид  $\mathbb{N}_+^{\mathfrak{J}}$  определено однозначным образом, с точностью до перестановки в нумерации элементов в  $\{x_j; j \in \mathfrak{J}\}$ .  $\square$

Нашей дальнейшей задачей является найти необходимые и достаточные условия  $k$ -потентности множеств  $\mathfrak{B}$  в коммутативном однородном моноиде. Ввиду теоремы 6 достаточно исследовать моноиды  $\mathbb{N}_+^{\mathfrak{J}}$ .

Любой элемент  $\mathbf{a} = \langle m_i \in \mathbb{N}_+; i \in \mathfrak{J} \rangle \in \mathbb{N}_+^{\mathfrak{J}}$  представляется в виде

$$\mathbf{a} = \sum_{i \in \mathfrak{J}} m_i x_i. \quad (8)$$

Если  $\mathfrak{B}$  —  $k$ -потентное множество в  $\mathfrak{A}$ , то для элемента  $\mathbf{a}$  найдется такой набор элементов  $\mathbf{b}_1, \dots, \mathbf{b}_k$ , что имеет место

$$\mathbf{a} = \sum_{l=1}^k \mathbf{b}_l.$$

Каждый элемент из этого набора имеет представление, аналогичное (8),

$$\mathbf{b}_l = \sum_{j \in \mathfrak{J}} n_j^{(l)} x_j, \quad (9)$$

где  $\langle n_j^{(l)} \in \mathbb{N}; j \in \mathfrak{J} \rangle$  и для каждого  $l = 1, \dots, k$  множество тех номеров  $j$ , для которых  $n_j^{(l)} \neq 0$  конечно.

Таким образом, для любого элемента  $\mathbf{a} \in \mathfrak{A}$  из  $k$ -потентного множества  $\mathfrak{B}$  в моноиде  $\mathfrak{A}$  должно иметь место представление

$$\mathbf{a} = \sum_{j \in \mathfrak{J}} m_j \mathbf{x}_j = \sum_{l=1}^k \sum_{j \in \mathfrak{J}} n_j^{(l)} \mathbf{x}_j = \sum_{j \in \mathfrak{J}} \mathbf{x}_j \sum_{l=1}^k n_j^{(l)}.$$

Ввиду однозначности разложения (8), это означает, что для любого набора натуральных чисел  $\langle m_j; j \in \mathfrak{J} \rangle$ , среди которых имеется только лишь конечное множество  $\Delta(\mathbf{a})$  отличных от нуля, должна быть разрешима в натуральных числах система уравнений

$$m_j = \sum_{l=1}^k n_j^{(l)}, \quad j \in \Delta(\mathbf{a}), \quad (10)$$

где  $\langle n_j^{(l)}; j \in \mathfrak{J} \rangle \in \mathbb{N}_+^{\mathfrak{J}}$ ,  $l = 1, \dots, k$ . Таким образом, справедлива следующая теорема.

**Теорема 7.** *Необходимым и достаточным условием того, чтобы множество  $\mathfrak{B} \subset \mathbb{N}_+^{\mathfrak{J}}$  было  $k$ -потентным, является наличие в нем таких элементов, представляемых в виде (9), для которых разрешима система уравнений (10).*

Теперь докажем утверждение, относящееся к моноидам, у которых  $\mathfrak{J} \equiv I_d = \{1, \dots, d\}$  конечно. Оно имеет важное значение для приложений изложенной выше теории. Введем функцию, характеризующую распределение элементов в любом подмножестве  $\mathfrak{B} \subset \mathbb{N}_+^d$ :

$$\varphi_{\mathfrak{B}}(x_1, \dots, x_d) = |\{\mathbf{x} \in \mathfrak{B} : \mathbf{x} = \langle n_1, \dots, n_d \rangle \in \mathbb{N}_+^d; n_j \leq x_j, j = 1, \dots, d\}|, \quad \langle x_1, \dots, x_d \rangle \in \mathbb{R}_+^d.$$

Эта функция распределения не убывает.

**Лемма 2.** *Пусть*

$$\varphi_{\mathfrak{C}}(x_1, \dots, x_d) = |\{\mathbf{x} \in \mathfrak{C} : \mathbf{x} = \langle n_1, \dots, n_d \rangle \in \mathbb{N}_+^d; n_j \leq x_j, j = 1, \dots, d\}|, \quad \langle x_1, \dots, x_d \rangle \in \mathbb{R}_+^d$$

— функция распределения некоторого множества  $\mathfrak{C}$ . Тогда

$$\varphi_{\mathfrak{C}}^{(j)}(n_1, \dots, n_d) = \varphi_{\mathfrak{C}}(n_1, \dots, n_j, \dots, n_d) - \varphi_{\mathfrak{C}}(n_1, n_2, \dots, n_j - 1, \dots, n_d) \in \{0, 1\}$$

для любого  $j = 1, \dots, d$ . Для того чтобы элемент  $\langle n_1, \dots, n_d \rangle \in \mathbb{N}_+^d$  принадлежал множеству  $\mathfrak{C}$  необходимо и достаточно, чтобы при любом  $j = 1, \dots, d$  имело место равенство

$$\varphi_{\mathfrak{C}}^{(j)}(n_1, \dots, n_d) = 1. \quad (11)$$

*Доказательство.* В доказательстве нуждается только последнее утверждение. Если имеет место (11), то это означает одноэлементность множества  $\{\mathbf{x} \in \mathfrak{C} : \mathbf{x} = \langle n'_1, \dots, n'_d \rangle \in \mathbb{N}_+^d; n'_l \leq n_l, l \neq j; n'_j = n_j\}$  при любом  $j = 1, \dots, d$ , так как при всех  $j = 1, \dots, d$  имеет место

$$\begin{aligned} 1 &= |\{\mathbf{x} \in \mathfrak{C} : \mathbf{x} = \langle n'_1, \dots, n'_d \rangle \in \mathbb{N}_+^d; n'_l \leq n_l, l = 1, \dots, d\}| - \\ &\quad - |\{\mathbf{x} \in \mathfrak{C} : \mathbf{x} = \langle n'_1, \dots, n'_d \rangle \in \mathbb{N}_+^d; n'_l \leq n_l - \delta_{jl}, l = 1, \dots, d\}| = \\ &\quad = |\{\mathbf{x} \in \mathfrak{C} : \mathbf{x} = \langle n'_1, \dots, n'_d \rangle \in \mathbb{N}_+^d; n'_l \leq n_l, l = 1, \dots, d\} \setminus \\ &\quad \setminus \{\mathbf{x} \in \mathfrak{C} : \mathbf{x} = \langle n'_1, \dots, n'_d \rangle \in \mathbb{N}_+^d; n'_l \leq n_l - \delta_{jl}, l = 1, \dots, d\}| = \\ &\quad = |\{\mathbf{x} \in \mathfrak{C} : \mathbf{x} = \langle n'_1, \dots, n'_d \rangle \in \mathbb{N}_+^d; n'_l \leq n_l, l \neq j; n'_j = n_j\}|. \end{aligned}$$

Совокупность таких равенств с  $j = 1, \dots, d$  эквивалентна соотношению

$$\begin{aligned} 1 &= \left| \bigcap_{j=1}^d \{\mathbf{x} \in \mathfrak{C} : \mathbf{x} = \langle n'_1, \dots, n'_d \rangle \in \mathbb{N}_+^d; n'_l \leq n_l, l \neq j; n'_j = n_j\} \right| = \\ &= |\{\mathbf{x} \in \mathfrak{C} : \mathbf{x} = \langle n_1, \dots, n_d \rangle \in \mathbb{N}_+^d\}|. \quad \square \end{aligned}$$



**Теорема 8.** Для того чтобы множество  $\mathfrak{B}$  было  $k$ -потентным, необходимо и достаточно, чтобы для любого элемента  $\langle m_1, \dots, m_d \rangle \in \mathbb{N}_+^d$  одновременно выполнялись все неравенства

$$\sum_{\substack{\langle n_j^{(1)}, \dots, n_j^{(k)} \rangle: \\ n_j^{(1)} + \dots + n_j^{(k)} = m_j}} \prod_{l=1}^k \varphi^{(j)}(n_1^{(l)}, \dots, n_d^{(l)}) \geq 1, \quad j = 1, \dots, d$$

и имело место  $\varphi(0, \dots, 0) = 1$ .

*Доказательство.* Теорема следует из теоремы 7 и леммы 2, примененных для каждого  $j = 1, \dots, d$ .  $\square$

В частности, при  $k = 2$ ,  $d = 1$  из теоремы 8 получаем следующее утверждение.

**Теорема 9.** Для квадратентности множества  $\mathfrak{B} \subset \mathbb{N}_+$  необходимо и достаточно, чтобы для его функции распределения  $\varphi(x)$  имело место  $\varphi(0) = 1$  и выполнялось неравенство

$$\sum_{n=1}^m [\varphi(n) - \varphi(n-1)] \cdot [\varphi(m-n) - \varphi(m-n-1)] \geq 1 \quad (12)$$

при всех  $m \in \mathbb{N}$ .

**5. Приложение к проблеме Гольдбаха.** В 1742 году в переписке между К. Гольдбахом и Л. Эйлером была высказана следующая гипотеза: *Каждое чётное число, большее двух, можно представить в виде суммы двух простых чисел.* Эта гипотеза получила название «бинарной проблемы Гольдбаха» (или проблемы Эйлера). Покажем, каким образом эта проблема может быть сформулирована в терминах моноида  $\mathbb{N}_+$ . (В такой формулировке единица включается в множество простых чисел).

Обозначим посредством  $\mathfrak{P}$  множество всех простых чисел в указанном смысле. Нужно доказать, что каждое четное число  $2(m+1)$ ,  $m \in \mathbb{N}_+$ , представимо в виде суммы двух простых  $2(m+1) = p + q$ ,  $p, q \in \mathfrak{P}$ . Каждое простое число, большее 2, о которых идет речь в формулировке проблемы, нечетно. Таким образом, для этих чисел  $p = 2r + 1$ ,  $q = 2s + 1$ ;  $r, s \in \mathbb{N}$  и  $r + s = m$ . Обратно, если  $r, s \in \mathbb{N}_+$ , то  $p + q = 2(r + s + 1) = 2(m + 1)$ ,  $r + s + 1 \equiv m + 1$ ,  $m \in \mathbb{N}$ .

Добавим к этим числам  $p = q = 1$ , для которых  $r, s = 0$ , что соответствует добавлению числа  $p + q = 2(m + 1)$  с  $m = 0$ , для которого утверждение бинарной гипотезы Гольдбаха тривиально. В связи с этим определим множество  $\mathfrak{B}$  равенством

$$\mathfrak{B} = \{t \in \mathbb{N}_+ : 2t + 1 \in \mathfrak{P}\} \cup \{0\}.$$

Отсюда следует, что бинарная гипотеза Гольдбаха эквивалентна утверждению о том, что множество  $\mathfrak{B}$  в моноиде  $\mathbb{N}_+$  должно обладать свойством  $\mathfrak{B} + \mathfrak{B} = \mathbb{N}$ , т.е. быть мультипотентным с показателем  $k = 2$ .

Рассмотрим используемую в теории чисел функцию (см., например, [4, 5])

$$\psi(x) \equiv |\{p \in \mathfrak{P} : p \leq x\}|, \quad x \in \mathbb{R}_+.$$

Тогда, используя определение множества  $\mathfrak{B}$ , имеем

$$\psi(x) = |\{l \in \mathbb{N} : 2l + 1 \in \mathfrak{P}, 2l + 1 \leq x\}| = |\{l \in \mathbb{N} : 2l + 1 \in \mathfrak{P}, l \leq (x-1)/2\}|,$$

т.е.

$$|\{l \in \mathfrak{B} : l \leq x\}| = |\{l \in \mathbb{N} : 2l + 1 \in \mathfrak{P}, l \leq x\}| \equiv \psi(2x + 1).$$

Полагая  $\varphi_{\mathfrak{B}}(x) = \psi(2x + 1)$ , на основании следствия теоремы 8 получаем следующее утверждение.

**Теорема 10.** Для того чтобы множество  $\mathfrak{B}$  было квадрапотентным, необходимо и достаточно, чтобы для любого  $m \in \mathbb{N}$  имело место неравенство

$$S(m) \equiv \sum_{n=1}^m [\psi(2n + 1) - \psi(2n - 1)] \cdot [\psi(2(m - n) + 1) - \psi(2(m - n) - 1)] \geq 1. \quad (13)$$

**6. Заключение.** В работе введено понятие мультипотентности множеств в моноидах, которое, при наличии однородности и коммутативности в таких алгебраических структурах, оказывается полезным при анализе задач аддитивной теории чисел, связанных с представлениями натуральных чисел в виде сумм чисел, обладающих специальными свойствами. Выявлены самые общие свойства мультипотентных множеств и представлена формулировка в терминах таких множеств с показателем  $k = 2$  известной бинарной проблемы Гольдбаха. Ключевым результатом работы, позволяющим анализировать задачи указанного выше типа, является теорема 8. В частности, ее применение в случае  $k = 2$  позволило несколько по-иному подойти к анализу бинарной проблемы Гольдбаха.

#### СПИСОК ЛИТЕРАТУРЫ

1. Бурбаки Н. Элементы математики. Алгебра. Часть 1. Алгебраические структуры. Линейная и полилинейная алгебра. — М.: Физматлит, 1962.
2. Виноградов И. М. Основы теории чисел. — М.-Л.: Гостехиздат, 1952.
3. Ляпин Е. С. Полугруппы. — М.: Физматлит, 1960.
4. Прахар К. П. Распределение простых чисел. — М.: Мир, 1967.
5. Чандрасекхаран К. Введение в аналитическую теорию чисел. — М.: Мир, 1974.
6. Шеврин Л. Н. Полугруппы// в кн.: Справочная математическая библиотека. Общая алгебра. Т. 2.. — М.: Наука, 1991. — С. 11–191.
7. Goldbach C. Lettre XLIII// in: Correspondance mathematique et physique de quelques celebres geometres du XVIII-eme siecle (Band 1). — St. Petersburg, 1743. — P. 125–129.
8. Waring E. Meditationes Algebraicae. — Cambridge, 1770.

Вирченко Юрий Петрович

Белгородский государственный национальный исследовательский университет

E-mail: virch@bsu.edu.ru