О прогрессивном представлении периодических семейств с ограничениями на начало и шаг

Дергач П.С., Данилевская Е.Д.

В статье изучается множество $K(n) := \mathbb{N} \setminus (n, n)$, исследуется его представление в виде объединения как можно меньшего количества арифметических прогрессий с ограничением на начало или шаг. В каждом из двух случаев найдены соответствующие точные оценки.

Ключевые слова: арифметическая прогрессия, натуральный ряд, проблема минимизации, типы ограничений.

Введение

Статья написана в соавторстве Дергача П. С. с его ученицей Данилевской Е. Д. и является переработанным результатом ее дипломной выпускной работы в филиале МГУ имени М. В. Ломоносова в городе Ташкенте. Рассматривается периодическое семейство натуральных чисел $K(n) := \mathbb{N} \setminus (n, n)$, взятое из работы [1]. Необходимо представить это семейство минимальным по количеству объединением арифметических прогрессий, на которые наложены следующие типы ограничений. Либо это ограничение сверху на начало прогрессий, либо это ограничение сверху на шаг прогрессий. В обоих случаях приводится точная реализация, доставляющая соответствующий минимум. Доказывается неулучшаемость полученных оценок. Читатели, желающие познакомиться с аналогичными интересными результатами, отсылаются к статьям [3-20].

Основные определения и результаты

Множество натуральных чисел обозначаем через $\mathbb{N}$, а множество целых неотрицательных чисел — через $\mathbb{N}_0$. Множество натуральных чисел от 1 до s обозначаем через E_s. Для $a \in \mathbb{N}$, $b \in \mathbb{N}$ обозначаем

$$(a, b) := \{a + ib \mid i \in \mathbb{N}_0\}$$

и называем это множество *арифметической прогрессией с началом a и шагом b*. Для произвольного $n \in \mathbb{N}$ положим

$$K(n) := \mathbb{N} \setminus (n, n).$$

Множество арифметических прогрессий обозначаем через $\mathbb{P}$. Для произвольного $k \in \mathbb{N}$ рассматриваем множества

$$\mathbb{B}(k) := \{(a, b) \in \mathbb{P} \mid a \le k\},$$

$$\mathbb{S}(k) := \{(a, b) \in \mathbb{P} \mid b \le k\}.$$

Для $* \in \{\mathbb{B}, \mathbb{S}\}$ пишем, что

$$K(n) \in U_k(*),$$

если множество $K(n)$ можно представить конечным объединением элементов из $*(k)$. Наконец, для произвольного $n \in \mathbb{N}$ вводим обозначения

$$f_1(n) = \min_k\{K(n) \in U_k(\mathbb{B})\},$$

$$f_2(n) = \min_k\{K(n) \in U_k(\mathbb{S})\}.$$

Теорема 1. *Пусть $n \in \mathbb{N}$ и $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ — его разложение на простые множители. Тогда*

$$f_1(n) = \max_{i \in E_s} p_i^{a_i - 1}(p_i - 1).$$

Теорема 2. *Пусть $n \in \mathbb{N}$ и $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ — его разложение на простые множители. Тогда*

$$f_2(n) = \max_{i \in E_s} p_i^{a_i}.$$

Доказательство вспомогательных утверждений

Лемма 1. Критерий пересечения. *Для любых* $a, c \in \mathbb{N}_0$ *и* $b, d \in \mathbb{N}$ *верно*

$$(a, b) \cap (c, d) \neq \emptyset \Longleftrightarrow a \equiv c \ (mod \ НОД(b, d)).$$

Доказательство леммы см. в [2].

Доказательство основных утверждений

Теорема 1. *Пусть* $n \in \mathbb{N}$ *и* $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ *— его разложение на простые множители. Тогда*

$$f_1(n) = \max_{i \in E_s} p_i^{a_i - 1}(p_i - 1).$$

Доказательство.

Обозначим через h_n число $\max\limits_{i \in E_s} p_i^{a_i - 1}(p_i - 1)$ и докажем верхнюю оценку, то есть что

$$f_1(n) \leq h_n. \tag{1}$$

Для этого достаточно показать, что множество $K(n)$ можно представить конечным объединением элементов из $\mathbb{B}(h_n)$, то есть арифметических прогрессий с началом не больше h_n. Это можно сделать, например, следующим образом. Для всех

$$0 \leq i \leq a_1 - 1, \tag{2}$$

$$p_1^i \leq j \leq p_1^i(p_1 - 1) \tag{3}$$

рассматриваем прогрессии

$$(a_i^j, b_i^j) := (j, p_1^{i+1}). \tag{4}$$

Ясно, что для каждого фиксированного i из (2) объединение прогрессий (a_i^j, b_i^j) по всем j из (3) дает нам множество всех натуральных чисел, которые делятся на p_1^i, но не делятся на p_1^{i+1}. Если теперь объединить эти конструкции по всем i из (2), то получим множество всех натуральных чисел, которые не делятся на $p_1^{a_1}$, то есть множество $K(p_1^{a_1})$. При этом, начала всех использованных в (4) прогрессий не превосходят $p_1^{a_1-1}(p_1 - 1)$, а значит не превосходят и h_n. Поэтому множество $K(p_1^{a_1})$

лежит в $U_{h_n}(\mathbb{B})$. Аналогично можно показать, что при всех $i \in E_s$ множество $K(p_i^{a_i})$ лежит в $U_{h_n}(\mathbb{B})$. Для этого достаточно в приведенном выше рассуждении заменить p_1 на p_i. Значит и множество $\bigcup\limits_{i \in E_s} K(p_i^{a_i})$ лежит в $U_{h_n}(\mathbb{B})$. Осталось заметить, что

$$\bigcup_{i \in E_s} K(p_i^{a_i}) = K(p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}) = K(n).$$

Неравенство (1) доказано.

Докажем теперь нижнюю оценку, то есть что

$$f_1(n) \geq h(n). \tag{5}$$

Для этого достаточно показать, что множество $K(n)$ нельзя представить конечным объединением элементов из множества $\mathbb{B}(h_n - 1)$, то есть арифметических прогрессий с началом не больше $h_n - 1$. Это можно сделать, например, следующим образом. Будем доказывать утверждение от противного. Допустим, такое представление существует. Без ограничения общности, будем считать, что

$$h_n = p_1^{a_1 - 1}(p_1 - 1). \tag{6}$$

Обозначим через a число, которое по модулю $p_1^{a_1}$ дает остаток $h(n)$, а по модулям $p_2^{a_2}, \dots, p_s^{a_s}$ дает остаток 0, то есть делится нацело. Из китайской теоремы об остатках известно, что найдется (и при том ровно одно) такое число на промежутке E_n. Очевидно, что $a \neq n$. Значит $a \in K(n)$ и поэтому содержится хотя бы в одной из прогрессий представления. Выберем любую из них. Пусть эта прогрессия имеет начало x. Рассмотрим тогда ее подпрогрессию $(x, a - x)$. Эта подпрогрессия все еще лежит в $K(n)$ и, значит, не пересекается с прогрессией (n, n). Поэтому из леммы 1 заключаем, что

$$x \not\equiv n \ (mod \ \text{НОД}(a - x, n)).$$

Значит найдутся такие $i \in E_s$ и $j \in E_{a_i}$, для которых

$$x \not\equiv n \ (mod \ p_i^j), \ x \equiv a \ (mod \ p_i^j).$$

Однако, оба числа a и n делятся нацело на

$$p_1^{a_1 - 1} p_2^{a_2} \dots p_s^{a_s} = \frac{n}{p_1}.$$

Значит,

$$x \not\equiv n \ (mod\ p_1^{a_1}),\ x \equiv a \ (mod\ p_1^{a_1}). \tag{7}$$

Так как число a по модулю $p_1^{a_1}$ дает остаток $h(n)$, то из (7) следует, что

$$x \equiv h(n) \ (mod\ p_1^{a_1}). \tag{8}$$

Однако, каждое начало прогрессий нашего представления не превосходит $h_n - 1$ и значит

$$x < h_n. \tag{9}$$

Условия (8) и (9) противоречат друг другу. Неравенство (5) доказано. Вместе с неравенством (1) это завершает доказательство теоремы.

∎

Теорема 2. *Пусть $n \in \mathbb{N}$ и $n = p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}$ — его разложение на простые множители. Тогда*

$$f_2(n) = \max_{i \in E_s} p_i^{a_i}.$$

Доказательство.

Обозначим через r_n число $\max\limits_{i \in E_s} p_i^{a_i}$ и докажем верхнюю оценку, то есть что

$$f_2(n) \leq r_n. \tag{10}$$

Для этого достаточно показать, что множество $K(n)$ можно представить конечным объединением элементов из множества $\mathbb{S}(r_n)$, то есть арифметических прогрессий с шагом не больше r_n. Это можно сделать, например, следующим образом. Для всех

$$1 \leq i \leq p_1^{a_1} - 1 \tag{11}$$

рассматриваем прогрессии

$$(a_i, b_i) := (i, p_1^{a_1}). \tag{12}$$

Ясно, что объединение прогрессий (a_i, b_i) по всем i из (11) дает нам множество всех натуральных чисел, которые не делятся на $p_1^{a_1}$. Шаги всех использованных в (12) прогрессий равны $p_1^{a_1}$, а значит не превосходят r_n. Поэтому множество $K(p_1^{a_1})$ лежит в $U_{r_n}(\mathbb{S})$. Аналогично можно показать, что при всех $i \in E_s$ множество $K(p_i^{a_i})$ лежит в $U_{r_n}(\mathbb{S})$. Для этого достаточно в приведенном выше рассуждении заменить p_1 на p_i. Значит и множество $\bigcup\limits_{i \in E_s} K(p_i^{a_i})$ лежит в $U_{r_n}(\mathbb{S})$. Осталось заметить, что

$$\bigcup_{i \in E_s} K(p_i^{a_i}) = K(p_1^{a_1} p_2^{a_2} \dots p_s^{a_s}) = K(n).$$

Докажем теперь нижнюю оценку, то есть что

$$f_1(n) \geq h(n). \tag{13}$$

Для этого достаточно показать, что множество $K(n)$ нельзя представить конечным объединением элементов из множества $\mathbb{S}(r_n - 1)$, то есть арифметических прогрессий с шагом не больше $r_n - 1$. Это можно сделать, например, следующим образом. Будем доказывать утверждение от противного. Допустим, такое представление существует. Без ограничения общности, будем считать, что

$$r_n = p_1^{a_1}. \tag{14}$$

Тогда рассмотрим ту прогрессию представления, которая содержит число $\frac{n}{p_1} = p_1^{a_1 - 1} p_2^{a_2} \dots p_s^{a_s}$. Обозначим шаг этой прогрессии через t. Тогда прогрессия

$$(p_1^{a_1 - 1} p_2^{a_2} \dots p_s^{a_s}, t) \tag{15}$$

будет в ней лежать, поэтому лежит и в множестве $K(n)$. Значит прогрессия (15) не пересекается с прогрессией (n, n). По лемме 1 получаем отсюда, что

$$p_1^{a_1 - 1} p_2^{a_2} \dots p_s^{a_s} \not\equiv n \ (mod \ \text{НОД}(n, t)).$$

Отсюда с неизбежностью следует, что t делится нацело на $p_1^{a_1} = r_n$. Но это противоречит тому, что все элементы представления лежат в множестве $\mathbb{S}(r_n - 1)$. Неравенство (13) доказано. Вместе с неравенством (10) это завершает доказательство теоремы.

■

Список литературы

[1] П. С. Дергач, Э. С. Айрапетов. *О прогрессивном разбиении некоторых подмножеств натурального ряда.* Интеллектуальные системы, 2015. Т.19, вып. 3, М., Сс. 79-86.

[2] П. С. Дергач. *О каноническом регулярном представлении S-тонких языков.* Интеллектуальные системы, 2014. Т.18, вып. 1, М., Сс. 211-242.

[3] П. С. Дергач. *О проблеме вложения допустимых классов.* Интеллектуальные системы, 2015. Т.19, вып. 2, М., Сс. 143-174.

[4] П. С. Дергач. *О двух размерностях спектров тонких языков.* Интеллектуальные системы, 2015. Т.19, вып. 3, М., Сс. 155-174.

[5] П. С. Дергач, Э. С. Айрапетов. *О прогрессивном разбиении последовательности натуральных чисел, имеющей пропуск длины 2.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 67-86.

[6] П. С. Дергач, Е. Д. Данилевская. *О покрытиях и разбиениях натуральных чисел, имеющих два последовательных пропуска длины 1.* Интеллектуальные системы, 2017. Т.21, вып. 1, М., Сс.192-237.

[7] П. С. Дергач. *О структуре вложения прогрессивных множеств сложности два.* Интеллектуальные системы, 2017. Т.21, вып. 2, М., Сс.117-162.

[8] П. С. Дергач, Ж. И. Раджабов. *О длине минимальной алфавитной склейки для класса линейных регулярных языков.* Интеллектуальные системы, 2017. Т.21, вып. 3, М., Сс.120-130.

[9] Д. Е. Александров. *Эффективные методы реализации проверки содержания сетевых пакетов регулярными выражениями.* Интеллектуальные системы, 2014. Т.18, вып. 1, М., Сс. 37-60.

[10] Д. Н. Бабин. *Частотные регулярные языки.* Интеллектуальные системы, 2014. Т.18, вып. 1, М., Сс. 205-210.

[11] Д. Е. Александров. *Об оценках автоматной сложности распознавания классов регулярных языков.* Интеллектуальные системы, 2014. Т.18, вып. 4, М., Сс. 161-190.

[12] В. М. Дементьев. *О звездной высоте регулярного языка и циклической сложности минимального автомата.* Интеллектуальные системы, 2014. Т.18, вып. 4, М., Сс. 215-222.

[13] И. Е. Иванов. *О сохранении периодических последовательностей автоматами с магазинной памятью с однобуквенным магазином.* Интеллектуальные системы, 2015. Т.19, вып. 1, М., Сс. 145-160.

[14] А. А. Петюшко. *О контекстно-свободных биграмных языках.* Интеллектуальные системы, 2015. Т.19, вып. 2, М., Сс. 187-208.

[15] И. Е. Иванов. *Нижняя оценка на максимальную длину периода выходной последовательности автономного автомата с магазинной памятью.* Интеллектуальные системы, 2015. Т.19, вып. 3, М., Сс. 175-194.

[16] В. А. Орлов. *О конечных автоматах с максимальной степенью различимости состояний.* Интеллектуальные системы, 2016. Т.20, вып. 1, М., Сс. 213-222.

[17] П. С. Дергач. *О проблеме проверки однозначности алфавитного декодирования в классе регулярных языков с полиномиальной функцией роста.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 147-202.

[18] А. М. Миронов. *Основные понятия теории вероятностных автоматов.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 283-330.

[19] А. А. Петюшко, Д. Н. Бабин. *Классификация Хомского для матриц биграммных языков.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 331-336.

[20] С. Б. Родин. *О связи линейно реализуемых автоматов и автоматов с максимальной вариативностью относительно кодирования состояний.* Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 337-348.

Сведения об авторах

Дергач Петр Сергеевич
Младший научный сотрудник МГУ имени М. В. Ломоносова
e-mail: dergachpes@mail.ru,
Данилевская Екатерина Дмитриевна
Выпускница факультета ПМиИ филиала МГУ имени М. В. Ломоносова в городе Ташкенте
e-mail: katirina_@mail.ru.

On the progressive representation of periodic sets with restrictions on the beginning and the step

Dergach P.S., Danilevskaya E.D.

In the article the set $K(n) := \mathbb{N} \setminus (n, n)$ is being examined, it's presentation as union of as few arithmetic progressions as possible with constraints to the begining or step is being investigated. In both two cases appropriate accurate estimations have been found.

Key words: arithmetic progression, natural series, minimization problem, types of constraints.