О прогрессивном разбиении некоторых подмножеств натурального ряда

Э. С. Айрапетов, П.С. Дергач

В статье приводится результат о нахождении минимального количества $f(n)$ арифметических прогрессий, необходимых для того, чтобы получить в объединении все натуральные числа, не делящиеся на n. Здесь n - произвольное натуральное число. При этом исследованы два случая. В первом случае прогрессии могут пересекаться, во втором - не могут. В обоих случаях авторам статьи удалось найти точное значение для функции $f(n)$ и привести конструктивное разбиение этого подмножества натурального ряда на $f(n)$ арифметических прогрессий.

Ключевые слова: Натуральный ряд, арифметическая прогрессия, декомпозиция.

Введение

В теории регулярных языков особое место занимает класс регулярных языков с полиномиальной функцией роста. При изучении свойств таких языков, зачастую, необходимо сначала изучить свойства спектров этих языков. Известно, что спектрами полиномиальных языков являются прогрессивные множества и только они. Прогрессивными множествами называем подмножества натурального ряда, образованные объединением конечного количества чисел и арифметических прогрессий. Возникает следующая постановка задачи: для данного прогрессивного множества необходимо найти минимальное количество прогрессий, объединение которых образует это прогрессивное множество. В общем случае задача кажется трудоемкой и пока не решена. Поэтому было решено рассмотреть частный случай этой задачи. В качестве прогрессивного множества мы будем рассматривать множество чисел натурального ряда, которые не делятся на фиксированное число k. При $k = 2^n$ решение задачи приводится в другой статье за авторством П. С. Дергача "О двух размерностях спектров тонких языков", с большой вероятностью публикуемой этим же номером. Использованную там идею удается здесь обобщить. Вычисляется и доказывается общая теоретическая оценка на минимальное количество арифметических прогрессий для рассматриваемых прогрессивных множеств. В дальнейшем планируется получить соответствующий результат и для других классов прогрессивных множеств. Также авторы рекомендуют читателям, которым интересна теория регулярных языков и конечных автоматов, ознакомиться со работами [1-12]. Впрочем, для понимания результатов этой статьи это совсем не обязательно.

Основные определения и результаты

Множество натуральных чисел обозначаем через $\mathbb{N}$. Множество целых неотрицательных чисел обозначаем через $\mathbb{N}_0$. Пусть $a \in \mathbb{N}$, $b \in \mathbb{N}_0$. Тогда *обобщенной арифметической прогрессией с началом a и шагом b* называется множество $\{a + ib \mid i \in \mathbb{N}_0\}$. Для краткости обозначаем эту прогрессию через (a, b). Через $P(k)$ обозначаем множество $\mathbb{N} \setminus (k, k)$. Пусть $k \in \mathbb{N}$. Через $f_1(k)$ обозначаем минимальное количество непересекающихся обобщенных арифметических прогрессий, объединение которых равно $P(k)$. Через $f_2(k)$ обозначаем минимальное количество возможно пересекающихся обобщенных арифметических прогрессий, объединение которых равно $P(k)$.

Теорема 1. *Пусть $k \in \mathbb{N}$ и $k = p_1^{a_1} \cdot p_2^{a_2} \ldots p_{s(k)}^{a_{s(k)}}$ - разложение числа k на простые множители. Тогда*

$$f_1(k) = f_2(k) = a_1(p_1 - 1) + a_2(p_2 - 1) + \ldots + a_{s(k)}(p_{s(k)} - 1).$$

Доказательство вспомогательных утверждений

Лемма 1. Для любых $a, c \in \mathbb{N}^+$ и $b, d \in \mathbb{N}$ верно

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

Доказательство. Пусть $(a \oplus b) \cap (c \oplus d) \neq \emptyset$. Тогда существуют $i, j \in \mathbb{N}^+$ такие, что $a + i \cdot b = c + i \cdot d$. Значит, $a - c = i \cdot (b - d)$. Так как b и d делятся нацело на (b, d), то и $b - d$ делится нацело на (b, d). Поэтому и $a - c$ делится нацело на (b, d), то есть $a \equiv c \ (mod \ (b, d))$.

Пусть теперь $a \equiv c \ (mod \ (b, d))$. Без ограничения общности считаем, что $a \geq c$. Тогда для некоторого $i \in \mathbb{N}^+$ имеем $a = c + i \cdot (b, d)$. Из расширенного алгоритма Евклида получаем существование $j, s \in \mathbb{Z}$, для которых $(b, d) = j \cdot b + s \cdot d$. Значит, $a = c + i \cdot j \cdot b + i \cdot s \cdot d$ и $a - i \cdot j \cdot b = c + i \cdot s \cdot d$. Осталось заметить, что тогда для любого $k \in \mathbb{N}$ верно $a + (k \cdot d - i \cdot j) \cdot b = c + (k \cdot b + i \cdot s) \cdot d$. Очевидно, что для некоторого $k \in \mathbb{N}$ будет выполнено $k \cdot d - i \cdot j, k \cdot b + i \cdot s \in \mathbb{N}^+$. Значит $(a \oplus b) \cap (c \oplus d) \neq \emptyset$.

Таким образом, утверждение леммы 1 доказано.

Доказательство основных утверждений

Теорема 1. *Пусть $k \in \mathbb{N}$ и $k = p_1^{a_1} \cdot p_2^{a_2} \ldots p_{s(k)}^{a_{s(k)}}$ - разложение числа k на простые множители. Тогда*

$$f_1(k) = f_2(k) = a_1(p_1 - 1) + a_2(p_2 - 1) + \ldots + a_{s(k)}(p_{s(k)} - 1).$$

Доказательство. Здесь и далее, без ограничения общности, вместо f_1 и f_2 будем везде писать f. На правильность выкладок это нигде не повлияет. Для произвольного $k \in \mathbb{N}$ через $s(k)$ обозначаем количество различных простых чисел в разложении числа k. Докажем индукцией по $s(k)$, что

$$f_1(k) \leq a_1(p_1 - 1) + a_2(p_2 - 1) + \ldots + a_{s(k)}(p_{s(k)} - 1),$$

$$f_2(k) \leq a_1(p_1 - 1) + a_2(p_2 - 1) + \ldots + a_{s(k)}(p_{s(k)} - 1).$$

База индукции ($s(k) = 1$):
Тогда $k = p_1^{a_1}$. Имеем:

$$P(k) = (1, p_1) \cup (2, p_1) \cup \ldots \cup (p_1 - 1, p_1) \bigcup$$

$$\bigcup (p_1, p_1^2) \cup (2p_1, p_1^2) \cup \ldots \cup (p_1(p_1 - 1), p_1^2) \bigcup$$

$$\ldots$$

$$\bigcup (p_1^{a_1-1}, p_1^{a_1}) \cup (2p_1^{a_1-1}, p_1^{a_1}) \cup \ldots \cup (p_1^{a_1-1}(p_1-1), p_1^{a_1}).$$

Переход индукции $(n \to n+1)$:
Пусть $s(k) = n+1$. Обозначим $p_2^{a_2} \ldots p_{s(k)}^{a_{s(k)}}$ через x. Тогда имеем:

$$P(k) = (1, p_1) \cup (2, p_1) \cup \ldots \cup (p_1 - 1, p_1) \bigcup$$

$$\bigcup (p_1, p_1^2) \cup (2p_1, p_1^2) \cup \ldots \cup (p_1(p_1-1), p_1^2) \bigcup$$

$$\ldots$$

$$\bigcup (p_1^{a_1-1}, p_1^{a_1}) \cup (2p_1^{a_1-1}, p_1^{a_1}) \cup \ldots \cup (p_1^{a_1-1}(p_1-1), p_1^{a_1}) \bigcup$$

$$\bigcup \{i \cdot p_1^{a_1} \mid i \in P(x)\}.$$

Так как $s(x) = n$, то по предположению индукции имеем:

$$f(x) \leq a_2(p_2 - 1) + \ldots + a_{s(k)}(p_{s(k)} - 1).$$

Отсюда немедленно следует, что множество $\{i \cdot p_1^{a_1} \mid i \in P(x)\}$ можно покрыть конечным объединением не более чем $a_2(p_2-1) + \ldots + a_{s(k)}(p_{s(k)} - 1)$ арифметических прогрессий. Окончательно получаем, что

$$f(k) \leq a_1(p_1 - 1) + a_2(p_2 - 1) + \ldots + a_{s(k)}(p_{s(k)} - 1).$$

Переход индукции доказан. Утверждение теоремы в одну сторону доказано.

Докажем утверждение теоремы в другую сторону.

Пусть $s(k) = n$. Для всех $1 \leq i \leq n$ вводим обозначения:

$$I_i = \{x \cdot p_i^l \mid 1 \leq x < p_i, 0 \leq l < a_i\},$$

$$x_i = \frac{k}{p_i^{a_i}}.$$

Рассмотрим множество

$$M = \bigcup_{i=1}^{n} \{r \cdot x_i \mid r \in I_i\}.$$

Пусть $a, b \in M$, $a < b$. Рассмотрим два случая.
Случай 1.
$$a = c \cdot p_i^{l_1} \cdot x_i,\ b = d \cdot p_i^{l_2} \cdot x_i$$
для некоторых
$$1 \leq c, d < p_i,\ 0 \leq l_1 \leq l_2 < a_i,\ 1 \leq i \leq n.$$
Тогда замечаем, что
$$\text{НОД}(b - a, k) =$$
$$= \text{НОД}(d \cdot p_i^{l_2} \cdot x_i - c \cdot p_i^{l_1} \cdot x_i,\ p_i^{a_i} \cdot x_i) =$$
$$= x_i \cdot \text{НОД}(d \cdot p_i^{l_2} - c \cdot p_i^{l_1},\ p_i^{a_i}) = x_i \cdot p_i^{l_1}.$$
Применяя лемму 1, получаем
$$(a, b - a) \cap (k, k) \neq \emptyset \Longleftrightarrow a \equiv k(mod\ x_i \cdot p_i^{l_1}).$$
Но $a - k = c \cdot p_i^{l_1} \cdot x_i - p_i^{a_i} \cdot x_i = x_i \cdot p_i^{l_1} \cdot (c - p_i^{a_i - l_1})$. Таким образом, для любых $a, b \in M$, $a < b$ числа a и b будут в покрытии покрыты разными прогрессиями.
Случай 2.
$$a = c \cdot p_i^{l_1} \cdot x_i,\ b = d \cdot p_j^{l_2} \cdot x_j$$
для некоторых
$$1 \leq c < p_i,\ 0 \leq l_1 < a_i,\ 1 \leq i \leq n,$$
$$1 \leq d < p_j,\ 0 \leq l_2 < a_j,\ 1 \leq j \leq n,$$
$$i \neq j.$$
Тогда замечаем, что
$$\text{НОД}(b - a, k) =$$
$$= \text{НОД}(d \cdot p_j^{l_2} \cdot x_j - c \cdot p_i^{l_1} \cdot x_i,\ p_i^{a_i} \cdot x_i) =$$
$$= \text{НОД}(d \cdot p_j^{l_2} \cdot \frac{k}{p_j^{a_j}} - c \cdot p_i^{l_1} \cdot \frac{k}{p_i^{a_i}},\ k) =$$
$$= \frac{k}{p_i^{a_i} \cdot p_j^{a_j}} \cdot \text{НОД}(d \cdot p_j^{l_2} \cdot p_i^{a_i} - c \cdot p_i^{l_1} \cdot p_j^{a_j},\ p_i^{a_i} \cdot p_j^{a_j}) =$$

$$= \frac{k}{p_i^{a_i} \cdot p_j^{a_j}} \cdot p_i^{l_1} \cdot p_j^{l_2} \cdot \text{НОД}(d \cdot p_i^{a_i - l_1} - c \cdot p_j^{a_j - l_2},\ p_i^{a_i - l_1} \cdot p_j^{a_j - l_2}) =$$

$$= \frac{k}{p_i^{a_i} \cdot p_j^{a_j}} \cdot p_i^{l_1} \cdot p_j^{l_2}.$$

Применяя лемму 1, получаем

$$(a, b-a) \cap (k, k) \neq \emptyset \Longleftrightarrow a \equiv k(mod\ \frac{k}{p_i^{a_i} \cdot p_j^{a_j}} \cdot p_i^{l_1} \cdot p_j^{l_2}).$$

Докажем, что $a-k$ делится нацело на $\frac{k}{p_i^{a_i} \cdot p_j^{a_j}} \cdot p_i^{l_1} \cdot p_j^{l_2}$. В самом деле,

$$\frac{a-k}{\frac{k}{p_i^{a_i} \cdot p_j^{a_j}} \cdot p_i^{l_1} \cdot p_j^{l_2}} =$$

$$= \frac{c \cdot p_i^{l_1} \cdot \frac{k}{p_i^{a_i}} - k}{\frac{k}{p_i^{a_i} \cdot p_j^{a_j}} \cdot p_i^{l_1} \cdot p_j^{l_2}} =$$

$$= c \cdot p_j^{a_j - l_2} - p_i^{a_i - l_1} \cdot p_j^{a_j - l_2}.$$

Объединяя оба случая, получаем, что для любых $a, b \in M,\ a < b$ числа a и b будут в покрытии покрыты разными прогрессиями. Значит,

$$f(k) \geq |M| = \sum_{i=1}^{n} |I_i| = \sum_{i=1}^{n} a_i(p_i - 1).$$

Теорема доказана.

Список литературы

[1] В. Б. Кудрявцев, С. В. Алешин, А. С. Подколзин. *Введение в теорию автоматов*. М.: Наука, 1985.

[2] С. В. Алешин. *Полугруппы и группы автоматов*. Интеллектуальные системы, 2013. Т.17, вып. 1-4, М., Сс. 129-141.

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

[4] И. Е. Иванов. *О некоторых свойствах автоматов с магазинной памятью*. Интеллектуальные системы, 2014. Т.18, вып. 1, М., Сс. 243-252.

[5] А. А. Часовских. *Условия полноты линейно-р-автоматных функций*. Интеллектуальные системы, 2014. Т.18, вып. 3, М., Сс. 203-252.

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

[7] Э. Э. Гасанов. *Прогнозирование периодических сверхсобытий автоматами*. Интеллектуальные системы, 2015. Т.19, вып. 1, М., Сс. 23-34.

[8] 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.

[9] А. А. Летуновский. *Выразимость линейных автоматов относительно расширенной суперпозиции*. Интеллектуальные системы, 2014. Т.19, вып. 1, М., Сс. 161-170.

[10] В. Г. Гербус. *О связи функций автомата и автоматной функции*. Интеллектуальные системы, 2015. Т.19, вып. 2, М., Сс. 109-116.

[11] А. М. Миронов. *Критерий реализуемости функций на строках вероятностными автоматами Мура с числовым выходом*. Интеллектуальные системы, 2014. Т.19, вып. 2, М., Сс. 149-160.

[12] И. Ю. Терехина. *Модель невлияния для квантовых автоматов*. Интеллектуальные системы, 2014. Т.19, вып. 2, М., Сс. 183-190.

About progressive decomposition of some subsets of the natural numbers

E. S. Airapetov, P.S. Dergach

Abstract: The result of finding the minimum number $f(n)$ of arithmetic progressions needed for getting in the union all natural numbers not divided by n is presented in the article. Here n is an arbitrary natural number. There were two cases explored. In the first case the progressions can intersect, in the second case - they cannot. In both cases the authors of the article managed to find the exact value of $f(n)$ function and present the constructive decomposition of this subset of natural series into $f(n)$ arithmetic progressions.

Keywords: natural numbers, arithmetic progression, decomposition.