О прогрессивном разбиении последовательности натуральных чисел, имеющей пропуск длины 2

П. С. Дергач, Э. С. Айрапетов

В статье приводится результат о нахождении минимального количества $f(n)$ арифметических прогрессий, необходимых для того, чтобы получить в объединении все натуральные числа, не сравнимые по модулю n с 0 и -1. Здесь n - произвольное натуральное число. При этом прогрессии могут пересекаться. Приводится точное значение для функции $f(n)$, а также конструктивное разбиение этого подмножества натурального ряда на $f(n)$ арифметических прогрессий.

Ключевые слова: натуральный ряд, арифметическая прогрессия, декомпозиция.

Введение

Прогрессивными множествами называем подмножества натурального ряда, образованные объединением конечного количества чисел и арифметических прогрессий. То есть, это все периодические подмножества натурального ряда, возможно, с предпериодом. Возникает следующая общая постановка задачи: для данного прогрессивного множества необходимо найти минимальное количество прогрессий, объединение которых образует это прогрессивное множество. В курсовой работе [1] была поставлена и успешно решена эта задача для случая, когда прогрессивное множество состоит из всех натуральных чисел, не делящихся на параметр n. То есть, это множество содержит

$n-1$ чисел, один пропуск, $n-1$ чисел, один пропуск и так далее. В дипломной работе было решено обобщить этот результат на случай, когда пропуск имеет длину 2, то есть множество содержит $n-2$ чисел, два пропуска, $n-2$ чисел, два пропуска и так далее. Для этого случая также удалось получить соответствующие оценки. При этом, техника для решения этой задачи осталась прежней: для доказательства верхней оценки используется конструктивное построение, а для доказательства нижней оценки используется метод опорных точек. Однако, наблюдается значительное усложнение описываемой конструкции. С одной стороны, на результат теперь влияет количество простых делителей у n (один он, или их несколько) и наличие среди этих простых делителей числа 2 (или, соответственно, отсутствие этого числа). С другой стороны, конструкция усложняется сама по себе. Это проявляется как в конструктивном построении, так и в описании опорного семейства. Построение опорного семейства носит крайне нетривиальный характер и, вместе с тем, оно все еще сохраняет определенную наглядность. Читатели, интересующиеся теорией формальных языков, также найдут много интересных для себя результатов в работах [2] - [11].

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 $\mathbb{N} \setminus ((k-1, k) \cup (k, k))$. Пусть $k \in \mathbb{N}$. Через $f(k)$ обозначаем минимальное количество обобщенных арифметических прогрессий, объединение которых равно $P(k)$. При этом, прогрессии могут попарно пересекаться.

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

$$f(k) = (2a_1 - 1)(p_1 - 1) - 1.$$

В остальных случаях

$$f(k) = \sum_{i=1}^{s(k)} (2a_i - 1)(p_i - 1).$$

Доказательство вспомогательных утверждений

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

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

Доказательство леммы см. [1]

Доказательство основного утверждения

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

$$f(k) = (2a_1 - 1)(p_1 - 1) - 1.$$

В остальных случаях

$$f(k) = \sum_{i=1}^{s(k)} (2a_i - 1)(p_i - 1).$$

Доказательство.

Часть первая. Доказательство верхних оценок.

Пусть $k \in \mathbb{N}$ и $s(k) = 1$. Докажем, что $f(k) \leqslant (2a_1 - 1)(p_1 - 1) - 1$. Разберем два подслучая. Подслучай первый - k четно, то есть $p_1 = 2$. Тогда

$$P(k) = \{(2^i - 1, 2^{i+1}) \mid 1 \leqslant i \leqslant a_1 - 1\} \cup \{(2^i, 2^{i+1}) \mid 1 \leqslant i \leqslant a_1 - 1\}. \tag{1}$$

Здесь серия

$$\{(2^i - 1, 2^{i+1}) \mid 1 \leqslant i \leqslant a_1 - 1\}$$

накрывает все нечетные числа, дающие по модулю 2^{a_1} остатки, отличные от $2^{a_1} - 1$. В свою очередь, серия

$$\{(2^i, 2^{i+1}) \mid 1 \leq i \leqslant a_1 - 1\}$$

накрывает все четные числа, не делящиеся нацело на 2^{a_1}. В разбиении (1) использовано

$$2(a_1-1)=(2a_1-1)(2-1)-1$$

арифметических прогрессий. Оценка доказана.
Подслучай второй - k нечетно, то есть $p_1>2$. Тогда

$$P(k)=\{(\hat{c_1},p_1)\mid 1\leqslant\hat{c_1}\leqslant p_1-2\}\cup \tag{2.1}$$

$$\cup\{(c_1p_1^i,p_1^{i+1})+c_0\mid 1\leqslant c_1\leqslant p_1-1,\ 1\leqslant i\leqslant a_1-1,\ -1\leqslant c_0\leqslant 0\}. \tag{2.2}$$

Серия (2.1) накрывает все числа, дающие по модулю p_1 остатки, отличные от 0 и p_1-1. Прогрессии в серии $\{c_1p_1,p_1^2\}$ накрывают все числа, делящиеся нацело на p_1, но не делящиеся нацело на p_1^2. Прогрессии в серии $\{c_1p_1^2,p_1^3\}$ накрывают все числа, делящиеся нацело на p_1^2, но не делящиеся нацело на p_1^3. И так далее. В итоге, гиперсерия

$$\{c_1p_1^i,p_1^{i+1}\mid 1\leqslant c_1\leqslant p_1-1,\ 1\leqslant i\leqslant a_1-1\}$$

накрывает все числа, делящиеся нацело на p_1, но не делящиеся нацело на $p_1^{a_1}$. Аналогично, гиперсерия

$$\{c_1p_1^i,p_1^{i+1}-1\mid 1\leqslant c_1\leqslant p_1-1,\ 1\leqslant i\leqslant a_1-1\}$$

накрывает все числа, дающие по модулю p_1 остаток p_1-1, но не дающие по модулю $p_1^{a_1}$ остаток $p_1^{a_1}-1$. Поэтому правая часть равенства (2) накрывает все числа, которые по модулю $p_1^{a_1}$ дают остатки, отличные от 0 или $p_1^{a_1}-1$. Осталось заметить, что количество прогрессий в этом разбиении равно

$$(p_1-2)+2(a_1-1)(p_1-1)=(2a_1-1)(p_1-1)-1.$$

Пусть теперь $s(k)>1$ и $k={p_1}^{a_1}p_2^{a_2}\dots p_{s_k}^{a_{s_k}}$. Докажем, что $f(k)\leqslant\sum\limits_{i=1}^{s(k)}(2a_i-1)(p_i-1)$. Имеем

$$P(k)=\left(\bigcup_{i=1}^{s(k)}\{(\hat{c_i},p_i)\mid 1\leqslant\hat{c_i}\leqslant p_i-2\}\right)\cup \tag{3.1}$$

$$\cup\left(\bigcup_{i=1}^{s(k)}\bigcup_{c_i=1}^{p_i-1}\bigcup_{d_i=1}^{a_i-1}\{(c_ip_1^{a_1}\dots p_{i-1}^{a_{i-1}}p_i^{d_i}p_{i+1}\dots p_{s(k)},p_1^{a_1}\dots p_{i-1}^{a_{i-1}}p_i^{d_i+1}p_{i+1}\dots p_{s(k)})\}\right)\cup \tag{3.2}$$

$$\cup\left(\bigcup_{i=1}^{s(k)}\bigcup_{c_i=1}^{p_i-1}\bigcup_{d_i=1}^{a_i-1}\{(c_ip_1^{a_1}\dots p_{i-1}^{a_{i-1}}p_i^{d_i}p_{i+1}\dots p_{s(k)}-1,p_1^{a_1}\dots p_{i-1}^{a_{i-1}}p_i^{d_i+1}p_{i+1}\dots p_{s(k)})\}\right)\cup \tag{3.3}$$

$$\cup\left(\bigcup_{i=1}^{s(k)-1}\{(x_i,p_ip_{i+1})\mid 1\leqslant x_i\leqslant p_ip_{i+1},\ x_i\equiv 0(mod\ p_i),\ x_i\equiv -1(mod\ p_{i+1})\}\right)\cup \tag{3.4}$$

$$\cup\{(x_{s(k)},p_{s(k)}p_1)\mid 1\leqslant x_{s(k)}\leqslant p_{s(k)}p_1,\ x_{s(k)}\equiv 0(mod\ p_{s(k)}),\ x_{s(k)}\equiv$$
$$\equiv -1(mod\ p_1)\}. \tag{3.5}$$

Серия (3.1) накрывает все числа, дающие по модулям $p_i,\ 2\leqslant i\leqslant s(k)$ остатки, отличные от 0 и p_i-1. Особо нужно оговорить случай, когда $p_1=2$, ведь там один из элементов серии пропадает. Но в этом случае все числа автоматически дают по модулю 2 только остатки 0 и $2-1$. Серия

$$\{(c_1p_1^{d_1}p_2\dots p_{s(k)},c_1p_1^{d_1+1}p_2\dots p_{s(k)})\mid 1\leqslant c_1\leqslant p_1-1,\ 1\leqslant d_1\leqslant$$
$$\leqslant a_1-1\}$$

накрывает все числа, делящиеся нацело на $p_1\dots p_{s(k)}$, но не делящиеся нацело на $p_1^{a_1}p_2\dots p_{s(k)}$. Серия

$$\{(c_2p_1^{a_1}p_2^{d_2}p_3\dots p_{s(k)},p_1^{a_1}p_2^{d_2+1}p_3\dots p_{s(k)})\mid 1\leqslant c_2\leqslant p_2-1,\ 1\leqslant d_2\leqslant$$
$$\leqslant a_2-1\}$$

накрывает все числа, делящиеся нацело на $p_1^{a_1}p_2\dots p_{s(k)}$, но не делящиеся нацело на $p_1^{a_1}p_2^{a_2}p_3\dots p_{s(k)}$. И так далее. Поэтому гиперсерия (3.2) накрывает все числа, делящиеся нацело на $p_1\dots p_{s(k)}$, но не делящиеся нацело на $p_1^{a_1}p_2^{a_2}\dots p_{s(k)}^{a_{s(k)}}$. Аналогично, гиперсерия (3.3) накрывает все числа, дающие по модулю $p_1\dots p_{s(k)}$ остаток $p_1\dots p_{s(k)}-1$, но не дающие по модулю $p_1^{a_1}p_2^{a_2}\dots p_{s(k)}^{a_{s(k)}}$ остаток $p_1^{a_1}p_2^{a_2}\dots p_{s(k)}^{a_{s(k)}}-1$. Покажем, что объединение серий (3.3) и (3.4) накрывает все числа, дающие по модулям $p_i, 1\leqslant i\leqslant s(k)$ остатки 0 или p_i-1, но не дающие одновременно только 0 или только p_i-1. Это верно, так как любое такое число обязательно после (возможно, с циклическим сдвигом от $s(k)$ к 1) какого-то 0 будет иметь иметь ненулевой остаток, то есть остаток $p_i - 1$. Объединяя все полученные наблюдения, заключаем, что равенство (3) действительно выполнено. Осталось заметить что в нем использовано

$$\sum_{i=1}^{s(k)}(p_i-2)+2\sum_{i=1}^{s(k)}(a_i-1)(p_i-1)+(s(k)-1)+1=\sum_{i=1}^{s(k)}(2a_i-1)(p_i-1)$$

арифметических прогрессий. Разбор случаев завершен. Все верхние оценки доказаны.

Часть вторая. Доказательство нижних оценок.

Пусть $k \in \mathbb{N}$ и $s(k) = 1$. Докажем, что $f(k) \geqslant (2a_1 - 1)(p_1 - 1) - 1$. Разберем два подслучая. Подслучай первый - k четно, то есть $k = 2^{a_1}$. Тогда рассмотрим множество

$$A = A_1 \sqcup A_2,\ \text{где}$$

$$A_1 := \{2^i \mid 1 \leqslant i \leqslant a_1 - 1\},\ A_2 := \{2^i - 1 \mid 1 \leqslant i \leqslant a_1 - 1\}.$$

Ясно, что $A \subset P(k)$. Докажем, что любая прогрессия, проходящая через произвольные два элемента x_1, x_2 множества A, выходит за границы множества $P(k)$. Возможны следующие варианты.

1)$x_1, x_2 \in A_1$, то есть $x_1 = 2^{i_1}$, $x_2 = 2^{i_2}$. Без ограничения общности, считаем, что $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, 2^{a_1}) = \text{НОД}(2^{i_2} - 2^{i_1}, 2^{a_1}) = 2^{i_1},$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (2^{a_1}, 2^{a_1}) \neq \emptyset$.

2)$x_1 \in A_1, x_2 \in A_2$, то есть $x_1 = 2^{i_1}$, $x_2 = 2^{i_2} - 1$. Без ограничения общности, считаем, что $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, 2^{a_1}) = \text{НОД}(2^{i_2} - 1 - 2^{i_1}, 2^{a_1}) = 1,$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (2^{a_1}, 2^{a_1}) \neq \emptyset$.

3)$x_1, x_2 \in A_2$, то есть $x_1 = 2^{i_1} - 1$, $x_2 = 2^{i_2} - 1$. Без ограничения общности, считаем, что $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, 2^{a_1}) = \text{НОД}(2^{i_2} - 2^{i_1}, 2^{a_1}) = 2^{i_1},$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (2^{a_1} - 1, 2^{a_1}) \neq \emptyset$.
Все варианты разобраны. Осталось заметить, что количество элементов в множестве A равно

$$2(a_1 - 1) = (2a_1 - 1)(2 - 1) - 1$$

и на каждый такой элемент в разбиении множества $P(k)$ нужна отдельная арифметическая прогрессия.
Подслучай второй - k нечетно, то есть $k = p_1^{a_1}$, $p_1 > 2$. Тогда рассмотрим множество

$$B = \left(\bigsqcup_{i=1}^{a_1-1} B_1^i\right) \sqcup \left(\bigsqcup_{i=1}^{a_1-1} B_2^i\right) \sqcup B_3, \text{ где}$$

$$B_1^i := \{c_1 p_1^i \mid 1 \leqslant c_1 \leqslant p_1 - 1\},$$
$$B_2^i := \{c_1 p_1^i - 1 \mid 1 \leqslant c_1 \leqslant p_1 - 1\},$$
$$B_3 := \{\hat{c_1} \mid 1 \leqslant \hat{c_1} \leqslant p_1 - 2\}.$$

Ясно, что $B \subset P(k)$. Докажем, что любая прогрессия, проходящая через произвольные два элемента x_1, x_2 множества B, выходит за границы множества $P(k)$. С точностью до перестановки местами x_1 и x_2, возможны следующие варианты.

1)$x_1, x_2 \in B_1^i$, то есть $x_1 = i_1 p_1^i$, $1 \leqslant i_1 \leqslant p_1 - 1$, $x_2 = i_2 p_1^i$, $1 \leqslant i_2 \leqslant p_1 - 1$. Без ограничения общности, считаем, что $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1}) = \text{НОД}(i_2 p_1^i - i_1 p_1^i, p_1^{a_1}) =$$

$$= p_1^i \text{НОД}(i_2 - i_1, p_1^{a_1 - i}) = p_1^i,$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1}, p_1^{a_1}) \neq \emptyset$.

2)$x_1, x_2 \in B_2^i$, то есть $x_1 = i_1 p_1^i - 1$, $1 \leqslant i_1 \leqslant p_1 - 1$, $x_2 = i_2 p_1^i - 1$, $1 \leqslant i_2 \leqslant p_1 - 1$. Без ограничения общности, считаем, что $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1}) = \text{НОД}(i_2 p_1^i - i_1 p_1^i, p_1^{a_1}) =$$

$$= p_1^i \text{НОД}(i_2 - i_1, p_1^{a_1 - i}) = p_1^i,$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} - 1, p_1^{a_1}) \neq \emptyset$.

3)$x_1, x_2 \in B_3$, то есть $x_1 = i_1$, $1 \leqslant i_1 \leqslant p_1 - 2$, $x_2 = i_2$, $1 \leqslant i_2 \leqslant p_1 - 2$. Без ограничения общности, считаем, что $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1}) = \text{НОД}(i_2 - i_1, p_1^{a_1}) = 1,$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1}, p_1^{a_1}) \neq \emptyset$.

4)$x_1 \in B_1^i$, $x_2 \in B_1^j$, то есть $x_1 = i_1 p_1^i$, $1 \leqslant i_1 \leqslant p_1 - 1$, $x_2 = i_2 p_1^j$, $1 \leqslant i_2 \leqslant p_1 - 1$. Без ограничения общности, считаем, что $x_1 < x_2$ и $i < j$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1}) = \text{НОД}(i_1 p_1^i - i_2 p_1^j, p_1^{a_1}) =$$

$$= p_1^i \text{НОД}(i_1 - i_2 p_1^{j-i}, p_1^{a_1 - i}) = p_1^i,$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1}, p_1^{a_1}) \neq \emptyset$.

5)$x_1 \in B_2^i$, $x_2 \in B_2^j$, то есть $x_1 = i_1 p_1^i - 1$, $1 \leqslant i_1 \leqslant p_1 - 1$, $x_2 = i_2 p_1^j - 1$, $1 \leqslant i_2 \leqslant p_1 - 1$. Без ограничения общности, считаем, что $x_1 < x_2$ и $i < j$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1}) = \text{НОД}(i_1 p_1^i - i_2 p_1^j, p_1^{a_1}) =$$

$$= p_1^i \text{НОД}(i_1 - i_2 p_1^{j-i}, p_1^{a_1 - i}) = p_1^i,$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} - 1, p_1^{a_1}) \neq \emptyset$.

6)$x_1 \in B_1^i$, $x_2 \in B_2^j$, то есть $x_1 = i_1 p_1^i$, $1 \leqslant i_1 \leqslant p_1 - 1$, $x_2 = i_2 p_1^j - 1$, $1 \leqslant i_2 \leqslant p_1 - 1$. Без ограничения общности, считаем, что $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1}) = \text{НОД}(i_1 p_1^i - (i_2 p_1^j - 1), p_1^{a_1}) = 1,$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1}, p_1^{a_1}) \neq \emptyset$.

7)$x_1 \in B_3$, $x_2 \in B_1^i$, то есть $x_1 = i_1$, $1 \leqslant i_1 \leqslant p_1 - 2$, $x_2 = i_2 p_1^i$, $1 \leqslant i_2 \leqslant p_1 - 1$. Тогда $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1}) = \text{НОД}(i_2 p_1^i - i_1, p_1^{a_1}) = 1,$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1}, p_1^{a_1}) \neq \emptyset$.

8)$x_1 \in B_3$, $x_2 \in B_2^i$, то есть $x_1 = i_1$, $1 \leqslant i_1 \leqslant p_1 - 2$, $x_2 = i_2 p_1^i - 1$, $1 \leqslant i_2 \leqslant p_1 - 1$. Тогда $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1}) = \text{НОД}(i_2 p_1^i - 1 - i_1, p_1^{a_1}) = 1,$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} - 1, p_1^{a_1}) \neq \emptyset$.
Все случаи разобраны. Осталось заметить, что количество элементов в множестве B равно

$$(p_1 - 2) + 2(a_1 - 1)(p_1 - 1) = (2a_1 - 1)(p_1 - 1) - 1$$

и на каждый такой элемент в разбиении множества $P(k)$ нужна отдельная арифметическая прогрессия.

Разберем теперь следующий случай, когда $s(k) > 1$ то есть $k = p_1^{a_1} p_2^{a_2} \ldots p_{s(k)}^{a_{s(k)}}$. Докажем, что $f(k) \geqslant \sum\limits_{i=1}^{s(k)} (2a_i - 1)(p_i - 1)$. Рассмотрим множество

$$C = \left(\bigsqcup_{i=1}^{s(k)} \bigsqcup_{j=1}^{a(i)-1} C_1^{i,j} \right) \sqcup \left(\bigsqcup_{i=1}^{s(k)} \bigsqcup_{j=1}^{a(i)-1} C_2^{i,j} \right) \sqcup \left(\bigsqcup_{i=1}^{s(k)} C_3^{i} \right) \sqcup C_4, \text{ где } (*)$$

$$C_1^{i,j} := \{c_i p_1^{a_1} \ldots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \ldots p_{s(k)}^{a_{s(k)}} \mid 1 \leqslant c_i \leqslant p_i - 1\},$$

$$C_2^{i,j} := \{c_i p_1^{a_1} \ldots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \ldots p_{s(k)}^{a_{s(k)}} - 1 \mid 1 \leqslant c_i \leqslant p_i - 1\},$$

$$C_3^{i} := \bigsqcup_{j=1}^{p_i - 2} \{x_j \mid 1 \leqslant x_j \leqslant p_1^{a_1} \ldots p_{s(k)}^{a_{s(k)}},$$

$$x_j \equiv j (mod\ p_i^{a_i}),\ x_j \equiv 0 (mod\ k/p_i^{a_i})\},$$

$$C_4 := \bigsqcup_{i=1}^{s(k)} \{x_i \mid 1 \leqslant x_i \leqslant p_1^{a_1} \ldots p_{s(k)}^{a_{s(k)}},$$

$$x_i \equiv -1 (mod\ p_i^{a_i}),\ x_i \equiv 0 (mod\ k/p_i^{a_i})\}.$$

Ясно, что $C \subset P(k)$. Ввиду нетривиальности конструкции, сначала необходимо объяснить, почему все множества из $(*)$ попарно непересекаются. Различие элементов внутри одинаковых серий очевидно. Проверим теперь на попарное несовпадение элементы из разных серий. Оказывается, что такие элементы дают разные наборы остатков по модулям $p_1, \ldots, p_k$. В самом деле, у элементов из $C_1^{i,j}$ все эти остатки равны 0; у элементов из $C_2^{i,j}$ эти остатки равны $p_i - 1$; у элементов из C_3^i эти остатки все кроме одного равны 0, а один больше 0 и меньше $p_i - 1$; у элементов из C_4 эти остатки все кроме одного равны 0, а один равен $p_i - 1$. Важно понимать, что здесь мы неявно использовали тот факт, что $s(k) > 1$. Кроме того, если $p_1 = 2$, то нужно сделать оговорку о том, что в этом случае серия C_3^1 вырождается в пустое множество.

Докажем, что любая прогрессия, проходящая через произвольные два элемента x_1, x_2 множества C, выходит за границы множества $P(k)$. С точностью до перестановки местами x_1 и x_2, возможны следующие варианты.

1)$x_1 \in C_1^{i,j}, x_2 \in C_1^{i,j}$, то есть

$$x_1 = i_1 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}},\ 1 \leqslant i_1 \leqslant p_i - 1,\ 1 \leqslant j \leqslant a_i - 1,$$

$$x_2 = i_2 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}},\ 1 \leqslant i_2 \leqslant p_i - 1,\ 1 \leqslant j \leqslant a_i - 1.$$

Без ограничения общности, считаем, что $x_1 < x_2$, то есть $i_1 < i_2$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = \text{НОД}(i_2 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}} -$$

$$- i_1 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \dots$$

$$\dots p_{s(k)}^{a_{s(k)}} \text{НОД}(i_2 - i_1, p_i^{a_i - j}) = p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}},$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

2)$x_1 \in C_1^{i,j_1}, x_2 \in C_1^{i,j_2}$, $j_1 \neq j_2$, то есть

$$x_1 = i_1 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{j_1} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}},\ 1 \leqslant i_1 \leqslant p_i - 1,\ 1 \leqslant j_1 \leqslant a_i - 1,$$

$$x_2 = i_2 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{j_2} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}},\ 1 \leqslant i_2 \leqslant p_i - 1\ 1 \leqslant j_2 \leqslant a_i - 1.$$

Без ограничения общности, считаем, что $x_1 < x_2$ и $j_1 < j_2$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = \text{НОД}(i_2 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{j_1} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}} -$$

$$- i_1 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{j_2} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{j_1} p_{i+1}^{a_{i+1}} \dots$$

$$\dots p_{s(k)}^{a_{s(k)}} \text{НОД}(i_2 - i_1 p_i^{j_2 - j_1}, p_i^{a_i - j_1}) = p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{j_1} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}},$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

3) $x_1 \in C_1^{i_1,j_1}, x_2 \in C_1^{i_2,j_2}$, $i_1 \neq i_2$, то есть

$$x_1 = c_1 p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j_1} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}},\ 1 \leqslant c_1 \leqslant p_{i_1} - 1,\ 1 \leqslant j_1 \leqslant \\ \leqslant a_{i_1} - 1,$$

$$x_2 = c_2 p_1^{a_1} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2}^{j_2} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}},\ 1 \leqslant c_2 \leqslant p_{i_2} - 1\ 1 \leqslant j_2 \leqslant \\ \leqslant a_{i_2} - 1.$$

Без ограничения общности, считаем, что $i_1 < i_2$ и $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = \text{НОД}(c_2 p_1^{a_1} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2}^{j_2} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}} - \\ - c_1 p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j_1} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots \\ \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j_1} p_{i+1}^{a_{i+1}} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2}^{j_2} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}} \cdot \\ \cdot \text{НОД}(c_2 p_{i_1}^{a_{i_1}-j_1} - c_1 p_{i_2}^{a_{i_2}-j_2}, p_{i_1}^{a_{i_1}-j_1} p_{i_2}^{a_{i_2}-j_2}) = \\ = p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j_1} p_{i+1}^{a_{i+1}} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2}^{j_2} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}} \cdot \\ \cdot \text{НОД}(c_2 p_{i_1}^{a_{i_1}-j_1} - c_1 p_{i_2}^{a_{i_2}-j_2}, p_{i_1}^{a_{i_1}-j_1}) = \\ = p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j_1} p_{i+1}^{a_{i+1}} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2}^{j_2} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}},$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

4) $x_1 \in C_2^{i,j}, x_2 \in C_2^{i,j}$, то есть

$$x_1 = i_1 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}} - 1,\ 1 \leqslant i_1 \leqslant p_i - 1,\ 1 \leqslant j \leqslant a_i - 1,$$

$$x_2 = i_2 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}} - 1,\ 1 \leqslant i_2 \leqslant p_i - 1\ 1 \leqslant j \leqslant a_i - 1.$$

Без ограничения общности, считаем, что $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = \text{НОД}(i_2 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}} - \\ - i_1 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \dots \\ \dots p_{s(k)}^{a_{s(k)}} \text{НОД}(i_2 - i_1, p_i^{a_i - j}) = p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^j p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}},$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}} - 1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

5)$x_1 \in C_2^{i,j_1}, x_2 \in C_2^{i,j_2}$, $j_1 \neq j_2$, то есть

$$x_1 = i_1 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{j_1} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}} - 1,\ 1 \leqslant i_1 \leqslant p_i - 1,\ 1 \leqslant j_1 \leqslant a_i - 1,$$

$$x_2 = i_2 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{j_2} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}} - 1,\ 1 \leqslant i_2 \leqslant p_i - 1\ 1 \leqslant j_2 \leqslant a_i - 1.$$

Без ограничения общности, считаем, что $x_1 < x_2$ и $j_1 < j_2$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = \text{НОД}(i_2 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{j_1} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}} -$$

$$- i_1 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{j_2} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{j_1} p_{i+1}^{a_{i+1}} \dots$$

$$\dots p_{s(k)}^{a_{s(k)}} \text{НОД}(i_2 - i_1 p_i^{j_2 - j_1}, p_i^{a_i - j_1}) = p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{j_1} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}},$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}} - 1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

6)$x_1 \in C_2^{i_1,j_1}, x_2 \in C_2^{i_2,j_2}$, $i_1 \neq i_2$, то есть

$$x_1 = c_1 p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j_1} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}} - 1,\ 1 \leqslant c_1 \leqslant p_{i_1} - 1,\ 1 \leqslant j_1 \leqslant$$
$$\leqslant a_{i_1} - 1,$$

$$x_2 = c_2 p_1^{a_1} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2}^{j_2} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}} - 1,\ 1 \leqslant c_2 \leqslant p_{i_2} - 1\ 1 \leqslant j_2 \leqslant$$
$$\leqslant a_{i_2} - 1.$$

Без ограничения общности, считаем, что $i_1 < i_2$ и $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = \text{НОД}(c_2 p_1^{a_1} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2}^{j_2} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}} -$$

$$- c_1 p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j_1} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots$$

$$\dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j_1} p_{i+1}^{a_{i+1}} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2}^{j_2} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}} \cdot$$

$$\cdot \text{НОД}(c_2 p_{i_1}^{a_{i_1} - j_1} - c_1 p_{i_2}^{a_{i_2} - j_2}, p_{i_1}^{a_{i_1} - j_1} p_{i_2}^{a_{i_2} - j_2}) =$$

$$= p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j_1} p_{i+1}^{a_{i+1}} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2}^{j_2} p_{i_2+1}^{a_{i_2+1}} \dots$$

$$\dots p_{s(k)}^{a_{s(k)}} \text{НОД}(c_2 p_{i_1}^{a_{i_1} - j_1} - c_1 p_{i_2}^{a_{i_2} - j_2}, p_{i_1}^{a_{i_1} - j_1}) =$$

$$= p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j_1} p_{i+1}^{a_{i+1}} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2}^{j_2} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}},$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}} - 1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

7)$x_1 \in C_3^i$, $x_2 \in C_3^i$, то есть $1 \leqslant x_1 \leqslant p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}$, $1 \leqslant x_2 \leqslant p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}$ и

$$x_1 \equiv j_1 (mod\ p_i^{a_i}),\ x_1 \equiv 0 (mod\ p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}}),\ 1 \leqslant j_1 \leqslant$$

$$\leqslant p_i - 2,$$

$$x_2 \equiv j_2 (mod\ p_i^{a_i}),\ x_2 \equiv 0 (mod\ p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}}),\ 1 \leqslant j_2 \leq$$

$$\leqslant p_i - 2.$$

Без ограничения общности, считаем, что $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, p_i) = \text{НОД}(j_2 - j_1, p_i) = 1,$$

то

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}}$$

и по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

8)$x_1 \in C_3^{i_1}$, $x_2 \in C_3^{i_2}$, $i_1 \neq i_2$, то есть $1 \leqslant x_1 \leqslant p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}$, $1 \leqslant x_2 \leqslant p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}$ и

$$x_1 \equiv j_1 (mod\, p_{i_1}^{a_{i_1}}),\ x_1 \equiv 0 (mod\, p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}}),\ 1 \leqslant j_1 \leqslant$$

$$\leqslant p_{i_1} - 2,$$

$$x_2 \equiv j_2 (mod\, p_{i_2}^{a_{i_2}}),\ x_2 \equiv 0 (mod\, p_1^{a_1} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}}),\ 1 \leqslant j_2 \leqslant$$

$$\leqslant p_{i_2} - 2.$$

Без ограничения общности, считаем, что $x_1 < x_2$ и $i_1 < i_2$. Так как

$$\text{НОД}(x_2 - x_1, p_{i_1}) = \text{НОД}(-j_1, p_{i_1}) = 1 \text{ и}$$

$$\text{НОД}(x_2 - x_1, p_{i_2}) = \text{НОД}(j_2, p_{i_2}) = 1,$$

то

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1+1}^{a_{i_1+1}} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}}$$

и по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

9)$x_1 \in C_4, x_2 \in C_4$, то есть $1 \leqslant x_1 \leqslant p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}$, $1 \leqslant x_2 \leqslant p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}$ и

$$x_1 \equiv -1 (mod\, p_{i_1}^{a_{i_1}}),\ x_1 \equiv 0 (mod\, p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}}),\ 1 \leqslant j_1 \leqslant$$

$$\leqslant p_{i_1} - 2,$$

$$x_2 \equiv -1 (mod\, p_{i_2}^{a_{i_2}}),\ x_2 \equiv 0 (mod\, p_1^{a_1} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}}),\ 1 \leqslant j_2 \leqslant$$

$$\leqslant p_{i_2} - 2.$$

Без ограничения общности, считаем, что $x_1 < x_2$ и $i_1 < i_2$. Так как

$$\text{НОД}(x_2 - x_1, p_{i_1}) = \text{НОД}(1, p_{i_1}) = 1 \text{ и}$$

$$\text{НОД}(x_2 - x_1, p_{i_2}) = \text{НОД}(-1, p_{i_2}) = 1,$$

то

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1+1}^{a_{i_1+1}} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}}$$

и по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

10)$x_1 \in C_1^{i_1, j_1}, x_2 \in C_2^{i_2, j_2}$, то есть

$$x_1 = c_1 p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j_1} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}},\ 1 \leqslant c_1 \leqslant p_{i_1} - 1,\ 1 \leqslant j_1 \leqslant$$

$$\leqslant a_{i_1} - 1,$$

$$x_2 = c_2 p_1^{a_1} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2}^{j_2} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}} - 1,\ 1 \leqslant c_2 \leqslant p_{i_2} - 1,\ 1 \leqslant j_2 \leqslant$$

$$\leqslant a_{i_2} - 1.$$

Без ограничения общности, считаем, что $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = 1,$$

то по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

11)$x_1 \in C_1^{i,j}, x_2 \in C_3^i$, то есть $1 \leqslant x_2 \leqslant p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}$ и

$$x_1 = c_1 p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_i^{j} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}},\ 1 \leqslant c_1 \leqslant p_i - 1,\ 1 \leqslant j \leqslant a_i - 1,$$

$$x_2 \equiv j_1(mod\ p_i^{a_i}),\ x_2 \equiv 0(mod\ p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}}),\ 1 \leqslant j_1 \leqslant$$
$$\leqslant p_i - 2.$$

Без ограничения общности, считаем, что $x_1 < x_2$. Так как

$$\text{НОД}(x_2 - x_1, p_i) = \text{НОД}(j_1, p_i) = 1,$$

то

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots p_{i-1}^{a_{i-1}} p_{i+1}^{a_{i+1}} \dots p_{s(k)}^{a_{s(k)}}$$

и по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

12)$x_1 \in C_1^{i_1,j}, x_2 \in C_3^{i_2}$, $i_1 \neq i_2$, то есть $1 \leqslant x_2 \leqslant p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}$ и

$$x_1 = c_1 p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}},\ 1 \leqslant c_1 \leqslant p_{i_1} - 1,\ 1 \leqslant j \leqslant$$
$$\leqslant a_{i_1} - 1,$$
$$x_2 \equiv j_1(mod\ p_{i_2}^{a_{i_2}}),\ x_2 \equiv 0(mod\ p_1^{a_1} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}}),\ 1 \leqslant$$
$$\leqslant j_1 \leqslant p_{i_2} - 2.$$

Без ограничения общности, считаем, что $x_1 < x_2$ и $i_1 < i_2$. Так как

$$\text{НОД}(x_2 - x_1, p_{i_1}^{a_{i_1}}) = \text{НОД}(-x_1, p_{i_1}^{a_{i_1}}) = p_{i_1}^{j},$$
$$\text{НОД}(x_2 - x_1, p_{i_2}) = \text{НОД}(j_1, p_{i_2}) = 1,$$

то

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j} p_{i_1+1}^{a_{i_1+1}} \dots$$
$$\dots p_{i_2-1}^{a_{i_2-1}} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}}$$

и по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

13)$x_1 \in C_1^{i_1,j}, x_2 \in C_4$, то есть $1 \leqslant x_2 \leqslant p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}$ и

$$x_1 = c_1 p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}},\ 1 \leqslant c_1 \leqslant p_{i_1} - 1,\ 1 \leqslant$$
$$\leqslant j \leqslant a_{i_1} - 1,$$
$$x_2 \equiv -1(mod\ p_{i_2}^{a_{i_2}}),\ x_2 \equiv 0(mod\ p_1^{a_1} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}}),\ 1 \leqslant$$
$$\leqslant j_1 \leqslant p_{i_2} - 2.$$

Без ограничения общности, считаем, что $x_1 < x_2$. Здесь возможны два варианта. Или $i_1 = i_2$, или $i_1 \neq i_2$. В первом случае

$$\text{НОД}(x_2 - x_1, p_{i_1}) = \text{НОД}(-1, p_{i_1}) = 1 \text{ и}$$

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}}.$$

Во втором случае

$$\text{НОД}(x_2 - x_1, p_{i_1}^{a_{i_1}}) = \text{НОД}(x_1, p_{i_1}^{a_{i_1}}) = p_{i_1}^{j},$$

$$\text{НОД}(x_2 - x_1, p_{i_2}) = \text{НОД}(-1, p_{i_2}) = 1 \text{ и}$$

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j} p_{i_1+1}^{a_{i_1+1}} \dots$$

$$\dots p_{i_2-1}^{a_{i_2-1}} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}}.$$

Так или иначе, по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

14)$x_1 \in C_2^{i_1,j}, x_2 \in C_3^{i_2}$, то есть $1 \leqslant x_2 \leqslant p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}$ и

$$x_1 = c_1 p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}} - 1,\ 1 \leqslant c_1 \leqslant p_{i_1} - 1,\ 1 \leqslant$$

$$\leqslant j \leqslant a_{i_1} - 1,$$

$$x_2 \equiv j_1 (mod\ p_{i_2}^{a_{i_2}}),\ x_2 \equiv 0 (mod\ p_1^{a_1} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}}),\ 1 \leqslant$$

$$\leqslant j_1 \leqslant p_{i_2} - 2.$$

Без ограничения общности, считаем, что $x_1 < x_2$. Тогда

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = 1$$

и по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

15)$x_1 \in C_2^{i_1,j}, x_2 \in C_4$, то есть $1 \leqslant x_2 \leqslant p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}$ и

$$x_1 = c_1 p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}} - 1,\ 1 \leqslant c_1 \leqslant p_{i_1} - 1,\ 1 \leqslant$$

$$\leqslant j \leqslant a_{i_1} - 1,$$

$$x_2 \equiv -1 (mod\ p_{i_2}^{a_{i_2}}),\ x_2 \equiv 0 (mod\ p_1^{a_1} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}}),\ 1 \leqslant$$

$$\leqslant j_1 \leqslant p_{i_2} - 2.$$

Без ограничения общности, считаем, что $x_1 < x_2$. Здесь возможны два варианта. Или $i_1 = i_2$, или $i_1 \neq i_2$. В первом случае

$$\text{НОД}(x_2 - x_1, p_{i_1}^{a_{i_1}}) = \text{НОД}(c_1 p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}}, p_{i_1}^{a_{i_1}}) =$$

$$= p_{i_1}^{j} \text{ и}$$

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = \text{НОД}(x_2 - x_1, p_{i_1}^{a_{i_1}}) = p_{i_1}^{j}.$$

Во втором случае

$$\text{НОД}(x_2 - x_1, p_{i_2}^{a_{i_2}}) = \text{НОД}(c_1 p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1}^{j} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}}, p_{i_2}^{a_{i_2}}) =$$

$$= p_{i_2}^{a_{i_2}} \text{ и}$$

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = \text{НОД}(x_2 - x_1, p_{i_2}^{a_{i_2}}) = p_{i_2}^{a_{i_2}}.$$

Так или иначе, по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}} - 1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

16)$x_1 \in C_3^{i_1}, x_2 \in C_4$, то есть $1 \leqslant x_1 \leqslant p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}$, $1 \leqslant x_2 \leqslant p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}$ и

$$x_1 \equiv j_1 (mod\ p_{i_1}^{a_{i_1}}),\ x_1 \equiv 0 (mod\ p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}}),\ 1 \leqslant$$

$$\leqslant j_1 \leqslant p_{i_1} - 2,$$

$$x_2 \equiv -1 (mod\ p_{i_2}^{a_{i_2}}),\ x_2 \equiv 0 (mod\ p_1^{a_1} \dots p_{i_2-1}^{a_{i_2-1}} p_{i_2+1}^{a_{i_2+1}} \dots p_{s(k)}^{a_{s(k)}}),\ 1 \leqslant$$

$$\leqslant j_1 \leqslant p_{i_2} - 2.$$

Без ограничения общности, считаем, что $x_1 < x_2$. Здесь возможны два варианта. Или $i_1 = i_2$, или $i_1 \neq i_2$. В первом случае

$$\text{НОД}(x_2 - x_1, p_{i_1}) = \text{НОД}(-1 - j_1, p_{i_1}) = 1 \text{ и}$$

$$\text{НОД}(x_2 - x_1, p_1^{a_1} \dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1} \dots p_{i_1-1}^{a_{i_1-1}} p_{i_1+1}^{a_{i_1+1}} \dots p_{s(k)}^{a_{s(k)}}.$$

Во втором случае, без ограничения общности, считаем, что $i_1 < i_2$. Тогда

$$\text{НОД}(x_2 - x_1, p_{i_1}) = \text{НОД}(x_1, p_{i_1}) = 1,$$

$$\text{НОД}(x_2 - x_1, p_{i_2}) = \text{НОД}(-1, p_{i_2}) = 1 \text{ и}$$

НОД$(x_2-x_1, p_1^{a_1}\dots p_{s(k)}^{a_{s(k)}}) = p_1^{a_1}\dots p_{i_1-1}^{a_{i_1-1}} p_{i_1+1}^{a_{i_1+1}}\dots p_{i_2-1}^{a_{i_2-1}} p_{i_2+1}^{a_{i_2+1}}\dots p_{s(k)}^{a_{s(k)}}$.

Так или иначе, по лемме 1 имеем $(x_1, x_2 - x_1) \cap (p_1^{a_1}\dots p_{s(k)}^{a_{s(k)}}, p_1^{a_1}\dots p_{s(k)}^{a_{s(k)}}) \neq \emptyset$.

Все случаи разобраны. Осталось заметить, что количество элементов в множестве C равно

$$2\sum_{i=1}^{s(k)}(a_i-1)(p_i-1) + \sum_{i=1}^{s(k)}(p_i-2) + s(k) = \sum_{i=1}^{s(k)}(2a_i-1)(p_i-1)$$

и на каждый такой элемент в разбиении множества $P(k)$ нужна отдельная арифметическая прогрессия. Разбор случаев завершен. Все нижние оценки доказаны.

Список литературы

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

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

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

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

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

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

[7] 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.

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

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

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

[11] 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.