

О покрытиях и разбиениях натуральных чисел, имеющих два последовательных пропуска длины 1

П. С. Дергач, Е. Д. Данилевская

В статье приводится результат о нахождении минимального количества $L(n)$ арифметических прогрессий, необходимых для того, чтобы получить в объединении все натуральные числа, не сравнимые по модулю n с 0 и -2 . Здесь n — произвольное натуральное число. При этом прогрессии могут пересекаться. Приводится точное значение для функции $L(n)$, а также конструктивное разбиение этого подмножества натурального ряда на $L(n)$ арифметических прогрессий.

Ключевые слова: натуральный ряд, арифметическая прогрессия, декомпозиция.

Введение

В рамках данной курсовой работы продолжаются исследования задачи о разбиении прогрессивных множеств на минимальное количество арифметических прогрессий. Прогрессивными множествами называем подмножества натурального ряда, образованные объединением конечного количества арифметических прогрессий. В курсовой работе задача решается в предположении, что прогрессивное множество состоит из всех таких натуральных чисел, которые по некоторому фиксированному натуральному числу n не дают остатки 0 и $n - 2$. То есть, это множество содержит $n - 2$ последовательных натуральных чисел, один пропуск, число, один пропуск и дальше опять $n - 2$ чисел, пропуск, число, пропуск и так далее. О решении похожих задач можно прочитать в статьях [1-5]. О других интересных аспектах исследований авторов и других ученых в смежных областях к тематике данной работы можно прочитать в [6-16].

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 *арифметической прогрессией с началом a и шагом b* называется множество

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

Через $T(n)$ обозначаем множество

$$T(n) := \mathbb{N} \setminus ((n-2, n) \cup (n, n)).$$

Пусть $n \in \mathbb{N}$. Через $L(n)$ обозначаем минимальное количество арифметических прогрессий, на которые можно разбить множество $T(n)$.

Множество $X \subseteq \mathbb{N}$ называем *опорным семейством для множества $Y \subseteq \mathbb{N}$* , если для любых $x_1, x_2 \in X$, $x_1 < x_2$ выполнено

$$(x_1, x_2 - x_1) \cap Y \neq \emptyset.$$

Теорема 1. Пусть $n \in \mathbb{N}$ и $n = p_1^{a_1} \cdot p_2^{a_2} \dots p_t^{a_t}$ — разложение числа n на простые множители и $p_1 < p_2 < \dots < p_t$. Тогда в зависимости от случаев

$$L(n) = 2a_1 - 3, \quad p_1 = 2, t = 1;$$

$$L(n) = (2a_2 - 1)(p_2 - 1) + (2a_1 - 2), \quad p_1 = 2, t = 2;$$

$$L(n) = (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + 1, \quad p_1 = 2, t > 2, a_1 = 1;$$

$$L(n) = (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + (2a_1 - 2), \quad p_1 = 2, t > 2, a_1 > 1;$$

$$L(n) = (2a_1 - 1)(p_1 - 1) - 1, \quad p_1 > 2, t = 1;$$

$$L(n) = (2a_1 - 1)(p_1 - 1) + \dots + (2a_t - 1)(p_t - 1), \quad p_1 > 2, t > 1.$$

Доказательство вспомогательных утверждений

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

$$(a, b) \cap (c, d) \neq \emptyset \iff a \equiv c \pmod{\text{НОД}(b, d)}.$$

Доказательство леммы см. в [1].

Лемма 2. Пусть $n \in \mathbb{N}$, $X \subseteq T(n)$, $Y = (n-2, n) \cup (n, n)$ и X - опорное семейство для Y . Тогда

$$L(n) \geq |X|.$$

Доказательство.

В любом разбиении множества $T(n)$ на арифметические прогрессии ни в какой из прогрессий не будет одновременно два числа из опорного семейства. В самом деле, если бы это было не так, то тогда для некоторых чисел $x_1, x_2 \in X$ прогрессия $(x_1, x_2 - x_1)$ лежала бы целиком в какой-то прогрессии разбиения и при этом пересекалась бы с множеством Y . Но ни одна из прогрессий разбиения с Y пересекаться не будет, так как

$$T(n) = \mathbb{N} \setminus ((n-2, n) \cup (n, n)).$$

Лемма доказана.

Доказательство основного утверждения

Теорема 1. Пусть $n \in \mathbb{N}$ и $n = p_1^{a_1} \cdot p_2^{a_2} \dots p_t^{a_t}$ — разложение числа n на простые множители и $p_1 < p_2 < \dots < p_t$. Тогда в зависимости от случаев

$$L(n) = 2a_1 - 3, \quad p_1 = 2, t = 1;$$

$$L(n) = (2a_2 - 1)(p_2 - 1) + (2a_1 - 2), \quad p_1 = 2, t = 2;$$

$$L(n) = (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + 1, \quad p_1 = 2, t > 2, a_1 = 1;$$

$$L(n) = (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + (2a_1 - 2), \quad p_1 = 2, t > 2, a_1 > 1;$$

$$L(n) = (2a_1 - 1)(p_1 - 1) - 1, \quad p_1 > 2, t = 1;$$

$$L(n) = (2a_1 - 1)(p_1 - 1) + \dots + (2a_t - 1)(p_t - 1), \quad p_1 > 2, t > 1.$$

Доказательство.

Пусть $p_1 = 2, t = 1$. Докажем тогда, что

$$L(n) = L(2^{a_1}) = 2a_1 - 3.$$

Сначала представим $T(n)$ в виде объединения $2a_1 - 3$ арифметических прогрессий. Это можно сделать следующим образом:

$$\begin{aligned} T(n) &= (1, 2) \cup (2, 8) \cup (4, 8) \cup \dots \cup (2^{a_1-1} - 2, 2^{a_1}) \cup (2^{a_1-1}, 2^{a_1}) = \\ &= (1, 2) \cup ((2, 8) \cup \dots \cup (2^{a_1-1} - 2, 2^{a_1})) \cup ((4, 8) \cup \dots \cup (2^{a_1-1}, 2^{a_1})). \end{aligned}$$

Видно, что здесь $1 + (a_1 - 2) + (a_1 - 2) = 2a_1 - 3$ прогрессий. И множество

$$(4, 8) \cup \dots \cup (2^{a_1-1}, 2^{a_1})$$

покрывает все четные числа, делящиеся на 4, но не дающие остатка 0 по модулю 2^{a_1} . А множество

$$(2, 8) \cup \dots \cup (2^{a_1-1} - 2, 2^{a_1})$$

покрывает все четные числа, не делящиеся на 4 и не дающие остатка $2^{a_1} - 2$ по модулю 2^{a_1} . Поэтому

$$L(2^{a_1}) \leq 2a_1 - 3.$$

Покажем, что

$$L(2^{a_1}) \geq 2a_1 - 3.$$

Рассмотрим множества

$$\begin{aligned} X_1 &:= \{1\}, \\ X_2 &:= \{2, 6, 14, \dots, 2^{a_1-1} - 2\}, \\ X_3 &:= \{4, 8, 16, \dots, 2^{a_1-1}\}, \\ Y &:= (2^{a_1} - 2, 2^{a_1}) \cup (2^{a_1}, 2^{a_1}). \end{aligned}$$

Покажем, что множество

$$X := X_1 \cup X_2 \cup X_3$$

будет опорным семейством для множества Y . Пусть $x_1, x_2 \in X$, $x_1 < x_2$. Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1, x_2 - x_1) \cap (2^{a_1} - 2, 2^{a_1}) \neq \emptyset, \quad (1)$$

$$(x_1, x_2 - x_1) \cap (2^{a_1}, 2^{a_1}) \neq \emptyset. \quad (2)$$

Возможны случаи:

Случай 1.

$x_1 \in X_1, x_2 \in X_2$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1}) = 1$ и по лемме 1 верно (1).

Случай 2.

$x_1 \in X_1, x_2 \in X_3$. Случай аналогичен предыдущему.

Случай 3.

$x_1 \in X_2, x_2 \in X_2$. Пусть

$$x_1 = 2^{d_1} - 2, \quad x_2 = 2^{d_2} - 2.$$

Тогда $\text{НОД}(x_2 - x_1, 2^{a_1}) = 2^{d_1}$ и по лемме 1 верно (1).

Случай 4.

$x_1 \in X_2, x_2 \in X_3$. Пусть

$$x_1 = 2^{d_1} - 2, \quad x_2 = 2^{d_2}.$$

Тогда $\text{НОД}(x_2 - x_1, 2^{a_1}) = 2$ и по лемме 1 верно (1).

Случай 5.

$x_1 \in X_3, x_2 \in X_2$. Случай аналогичен предыдущему.

Случай 6.

$x_1 \in X_3, x_2 \in X_3$. Пусть

$$x_1 = 2^{d_1}, \quad x_2 = 2^{d_2}.$$

Тогда $\text{НОД}(x_2 - x_1, 2^{a_1}) = 2^{d_1}$ и по лемме 1 верно (2).

Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y . Но в множестве X всего

$$|X_1| + |X_2| + |X_3| = 1 + (a_1 - 2) + (a_1 - 2)$$

элементов. Поэтому по лемме 2 получаем $L(2^{a_1}) \geq 2a_1 - 3$. В случае, когда $p_1 = 2, t = 1$, утверждение теоремы доказано.

Пусть $p_1 = 2, t = 2$. Докажем тогда, что

$$L(n) = L(2^{a_1} p_2^{a_2}) = (2a_2 - 1)(p_2 - 1) + (2a_1 - 2).$$

Здесь возможны два варианта:

$$1) a_1 = 1; \quad 2) a_1 > 1.$$

В первом варианте для доказательства верхней оценки нужно представить $T(n)$ в виде объединения $(2a_2 - 1)(p_2 - 1)$ арифметических прогрессий. Это можно сделать следующим образом:

$$T(n) = (1, 2) \cup ((2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \dots \cup (2p_2 - 4, 2p_2)) \cup$$

$$\begin{aligned}
& \cup((2p_2 - 2, 2p_2^2) \cup (4p_2 - 2, 2p_2^2) \cup (6p_2 - 2, 2p_2^2) \cup \dots \cup ((2p_2 - 2)p_2 - 2, 2p_2^2)) \cup \\
& \cup((2p_2^2 - 2, 2p_2^3) \cup (4p_2^2 - 2, 2p_2^3) \cup (6p_2^2 - 2, 2p_2^3) \cup \dots \cup ((2p_2 - 2)p_2^2 - 2, 2p_2^3)) \cup \\
& \quad \cup \dots \cup ((2p_2^{a_2-1} - 2, 2p_2^{a_2}) \cup (4p_2^{a_2-1} - 2, 2p_2^{a_2}) \cup (6p_2^{a_2-1} - 2, 2p_2^{a_2}) \cup \\
& \quad \cup \dots \cup ((2p_2 - 2)p_2^{a_2-1} - 2, 2p_2^{a_2})) \cup \\
& \quad \cup((2p_2, 2p_2^2) \cup (4p_2, 2p_2^2) \cup (6p_2, 2p_2^2) \cup \dots \cup ((2p_2 - 2)p_2, 2p_2^2)) \cup \\
& \quad \cup((2p_2^2, 2p_2^3) \cup (4p_2^2, 2p_2^3) \cup (6p_2^2, 2p_2^3) \cup \dots \cup ((2p_2 - 2)p_2^2, 2p_2^3)) \cup \dots \cup \\
& \quad \cup((2p_2^{a_2-1}, 2p_2^{a_2}) \cup (4p_2^{a_2-1}, 2p_2^{a_2}) \cup (6p_2^{a_2-1}, 2p_2^{a_2}) \cup \dots \cup ((2p_2 - 2)p_2^{a_2-1}, 2p_2^{a_2})).
\end{aligned}$$

Видно, что здесь $1 + (p_2 - 2) + 2(a_2 - 1)(p_2 - 1) = (2a_2 - 1)(p_2 - 1)$ прогрессий. Множество

$$(2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \dots \cup (2p_2 - 4, 2p_2)$$

покрывает все четные числа, не дающие остатков 0 и $p_2 - 2$ по модулю p_2 . Множество

$$\begin{aligned}
& ((2p_2 - 2, 2p_2^2) \cup (4p_2 - 2, 2p_2^2) \cup (6p_2 - 2, 2p_2^2) \cup \dots \cup ((2p_2 - 2)p_2 - 2, 2p_2^2)) \cup \\
& \cup((2p_2^2 - 2, 2p_2^3) \cup (4p_2^2 - 2, 2p_2^3) \cup (6p_2^2 - 2, 2p_2^3) \cup \dots \cup ((2p_2 - 2)p_2^2 - 2, 2p_2^3)) \cup \\
& \quad \cup \dots \cup ((2p_2^{a_2-1} - 2, 2p_2^{a_2}) \cup (4p_2^{a_2-1} - 2, 2p_2^{a_2}) \cup \\
& \quad \cup (6p_2^{a_2-1} - 2, 2p_2^{a_2}) \cup \dots \cup ((2p_2 - 2)p_2^{a_2-1} - 2, 2p_2^{a_2}))
\end{aligned}$$

покрывает все четные числа, дающие остаток $p_2 - 2$ по модулю p_2 и не дающие остатка $p_2^{a_2} - 2$ по модулю $p_2^{a_2}$. И множество

$$\begin{aligned}
& ((2p_2, 2p_2^2) \cup (4p_2, 2p_2^2) \cup (6p_2, 2p_2^2) \cup \dots \cup ((2p_2 - 2)p_2, 2p_2^2)) \cup \\
& \cup((2p_2^2, 2p_2^3) \cup (4p_2^2, 2p_2^3) \cup (6p_2^2, 2p_2^3) \cup \dots \cup ((2p_2 - 2)p_2^2, 2p_2^3)) \cup \dots \cup \\
& \cup((2p_2^{a_2-1}, 2p_2^{a_2}) \cup (4p_2^{a_2-1}, 2p_2^{a_2}) \cup (6p_2^{a_2-1}, 2p_2^{a_2}) \cup \dots \cup ((2p_2 - 2)p_2^{a_2-1}, 2p_2^{a_2}))
\end{aligned}$$

покрывает все четные числа, дающие остаток 0 по модулю p_2 и не дающие остатка 0 по модулю $p_2^{a_2}$. Поэтому

$$L(2p_2^{a_2}) \leq (2a_2 - 1)(p_2 - 1).$$

Для доказательства нижней оценки введем обозначения

$$X_1 := \{p_2^{a_2}\},$$

$$\begin{aligned}
X_2 &:= \{2, 4, 6, \dots, 2(p_2 - 2)\}, \\
X_3^1 &:= \{2p_2 - 2, 4p_2 - 2, 6p_2 - 2, \dots, 2(p_2 - 1)p_2 - 2\}, \\
X_3^2 &:= \{2p_2^2 - 2, 4p_2^2 - 2, 6p_2^2 - 2, \dots, 2(p_2 - 1)p_2^2 - 2\}, \\
&\dots\dots\dots \\
X_3^{a_2-1} &:= \{2p_2^{a_2-1} - 2, 4p_2^{a_2-1} - 2, 6p_2^{a_2-1} - 2, \dots, 2(p_2 - 1)p_2^{a_2-1} - 2\}, \\
X_4^1 &:= \{2p_2, 4p_2, 6p_2, \dots, 2(p_2 - 1)p_2\}, \\
X_4^2 &:= \{2p_2^2, 4p_2^2, 6p_2^2, \dots, 2(p_2 - 1)p_2^2\}, \\
&\dots\dots\dots \\
X_4^{a_2-1} &:= \{2p_2^{a_2-1}, 4p_2^{a_2-1}, 6p_2^{a_2-1}, \dots, 2(p_2 - 1)p_2^{a_2-1}\}, \\
Y &:= (2p_2^{a_2} - 2, 2p_2^{a_2}) \cup (2p_2^{a_2}, 2p_2^{a_2})
\end{aligned}$$

и покажем, что множество

$$X := X_1 \cup X_2 \cup X_3^1 \cup \dots \cup X_3^{a_2-1} \cup X_4^1 \cup \dots \cup X_4^{a_2-1}$$

будет опорным семейством для множества Y . Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1, x_2 - x_1) \cap (2p_2^{a_2} - 2, 2p_2^{a_2}) \neq \emptyset, \quad (3)$$

$$(x_1, x_2 - x_1) \cap (2p_2^{a_2}, 2p_2^{a_2}) \neq \emptyset. \quad (4)$$

Пусть $x_1, x_2 \in X$, $x_1 < x_2$. Возможны случаи:

Случай 1.

$x_1 \in X_1, x_2 \in X_2$ или $x_2 \in X_1, x_1 \in X_2$. Тогда $\text{НОД}(x_2 - x_1, 2p_2^{a_2}) = 1$ и по лемме 1 верно (3).

Случай 2.

$x_1 \in X_1, x_2 \in X_3^i$ или $x_2 \in X_1, x_1 \in X_3^i$. Случай аналогичен предыдущему.

Случай 3.

$x_1 \in X_1, x_2 \in X_4^i$ или $x_2 \in X_1, x_1 \in X_4^i$. Тогда $\text{НОД}(x_2 - x_1, 2p_2^{a_2}) = p_2^i$ и по лемме 1 верно (4).

Случай 4.

$x_1 \in X_2, x_2 \in X_2$. Тогда $\text{НОД}(x_2 - x_1, 2p_2^{a_2}) = 2$ и по лемме 1 верно (3).

Случай 5.

$x_1 \in X_2, x_2 \in X_3^i$ или $x_2 \in X_2, x_1 \in X_3^i$. Случай аналогичен предыдущему.

Случай 6.

$x_1 \in X_2, x_2 \in X_4^i$ или $x_2 \in X_2, x_1 \in X_4^i$. Случай аналогичен предыдущему.

Случай 7.

$x_1 \in X_3^i, x_2 \in X_3^i$. Тогда $\text{НОД}(x_2 - x_1, 2p_2^{a_2}) = 2p_2^i$ и по лемме 1 верно (3).

Случай 8.

$x_1 \in X_3^i, x_2 \in X_3^j, i < j$. Случай аналогичен предыдущему.

Случай 9.

$x_1 \in X_3^i, x_2 \in X_3^j, i > j$. Тогда $\text{НОД}(x_2 - x_1, 2p_2^{a_2}) = 2p_2^j$ и по лемме 1 верно (3).

Случай 10.

$x_1 \in X_3^i, x_2 \in X_4^j$. Тогда $\text{НОД}(x_2 - x_1, 2p_2^{a_2}) = 2$ и по лемме 1 верно (3).

Случай 11.

$x_1 \in X_4^i, x_2 \in X_4^i$. Тогда $\text{НОД}(x_2 - x_1, 2p_2^{a_2}) = 2p_2^i$ и по лемме 1 верно (4).

Случай 12.

$x_1 \in X_4^i, x_2 \in X_4^j, i < j$. Случай аналогичен предыдущему.

Случай 13.

$x_1 \in X_4^i, x_2 \in X_4^j, i > j$. Тогда $\text{НОД}(x_2 - x_1, 2p_2^{a_2}) = 2p_2^j$ и по лемме 1 верно (4).

Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y . Но в множестве X всего

$$\begin{aligned} & |X_1| + |X_2| + |X_3^1| + \dots + |X_3^{a_2-1}| + |X_4^1| + \dots + |X_4^{a_2-1}| = \\ & = 1 + (p_2 - 2) + 2(a_2 - 1)(p_2 - 1) = (2a_2 - 1)(p_2 - 1) \end{aligned}$$

элементов. Поэтому по лемме 2 получаем $L(2p_2^{a_2}) \geq (2a_2 - 1)(p_2 - 1)$.

Во втором варианте для доказательства верхней оценки нужно представить $T(n)$ в виде объединения $(2a_2 - 1)(p_2 - 1) + (2a_1 - 2)$ арифметических прогрессий. Это можно сделать следующим образом:

$$\begin{aligned} T(n) = & (1, 2) \cup ((2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \dots \cup (2p_2 - 4, 2p_2)) \cup \\ & \cup((4p_2 - 2, 8p_2) \cup (8p_2 - 2, 16p_2) \cup \dots \cup ((2^{a_1-1}p_2 - 2, 2^{a_1}p_2)) \cup \\ & \cup((2^{a_1}p_2 - 2, 2^{a_1}p_2^2) \cup (2^{a_1}p_2^2 - 2, 2^{a_1}p_2^3) \cup \dots \cup (2^{a_1}p_2^{a_2-1} - 2, 2^{a_1}p_2^{a_2})) \cup \\ & \cup((2 \cdot 2^{a_1}p_2 - 2, 2^{a_1}p_2^2) \cup (2 \cdot 2^{a_1}p_2^2 - 2, 2^{a_1}p_2^3) \cup \dots \cup \\ & \cup(2 \cdot 2^{a_1}p_2^{a_2-1} - 2, 2^{a_1}p_2^{a_2})) \cup \dots \cup (((p_2 - 1)2^{a_1}p_2 - 2, 2^{a_1}p_2^2) \cup \\ & \cup((p_2 - 1)2^{a_1}p_2^2 - 2, 2^{a_1}p_2^3) \cup \dots \cup ((p_2 - 1)2^{a_1}p_2^{a_2-1} - 2, 2^{a_1}p_2^{a_2})) \cup \\ & \cup((4p_2, 8p_2) \cup (8p_2, 16p_2) \cup \dots \cup ((2^{a_1-1}p_2, 2^{a_1}p_2)) \cup \end{aligned}$$

$$\begin{aligned}
& \cup ((2^{a_1} p_2, 2^{a_1} p_2^2) \cup (2^{a_1} p_2^2, 2^{a_1} p_2^3) \cup \dots \cup (2^{a_1} p_2^{a_2-1}, 2^{a_1} p_2^{a_2})) \cup \\
& \cup ((2 \cdot 2^{a_1} p_2, 2^{a_1} p_2^2) \cup (2 \cdot 2^{a_1} p_2^2, 2^{a_1} p_2^3) \cup \dots \cup (2 \cdot 2^{a_1} p_2^{a_2-1}, 2^{a_1} p_2^{a_2})) \cup \\
& \cup \dots \cup ((p_2 - 1) 2^{a_1} p_2, 2^{a_1} p_2^2) \cup ((p_2 - 1) 2^{a_1} p_2^2, 2^{a_1} p_2^3) \cup \\
& \cup \dots \cup ((p_2 - 1) 2^{a_1} p_2^{a_2-1}, 2^{a_1} p_2^{a_2})) \cup ((2p_2 - 2, 4p_2) \cup (2p_2, 4p_2)).
\end{aligned}$$

Видно, что здесь

$$\begin{aligned}
& 1 + (p_2 - 2) + 2(a_1 - 2) + 2(a_1 - 1)(p_2 - 1) + 2 = \\
& = (2a_2 - 1)(p_2 - 1) + (2a_1 - 2)
\end{aligned}$$

прогрессий. Множество

$$(2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \dots \cup (2p_2 - 4, 2p_2)$$

покрывает все четные числа, не дающие остатков 0 и $p_2 - 2$ по модулю p_2 . Множество

$$\begin{aligned}
& ((4p_2 - 2, 8p_2) \cup (8p_2 - 2, 16p_2) \cup \dots \cup ((2^{a_1-1} p_2 - 2, 2^{a_1} p_2)) \cup \\
& \cup ((2^{a_1} p_2 - 2, 2^{a_1} p_2^2) \cup (2^{a_1} p_2^2 - 2, 2^{a_1} p_2^3) \cup \dots \cup (2^{a_1} p_2^{a_2-1} - 2, 2^{a_1} p_2^{a_2})) \cup \\
& \cup ((2 \cdot 2^{a_1} p_2 - 2, 2^{a_1} p_2^2) \cup (2 \cdot 2^{a_1} p_2^2 - 2, 2^{a_1} p_2^3) \cup \dots \cup (2 \cdot 2^{a_1} p_2^{a_2-1} - 2, 2^{a_1} p_2^{a_2})) \cup \\
& \cup \dots \cup (((p_2 - 1) 2^{a_1} p_2 - 2, 2^{a_1} p_2^2) \cup ((p_2 - 1) 2^{a_1} p_2^2 - 2, 2^{a_1} p_2^3) \cup \\
& \cup \dots \cup ((p_2 - 1) 2^{a_1} p_2^{a_2-1} - 2, 2^{a_1} p_2^{a_2}))
\end{aligned}$$

покрывает все числа, дающие остаток 2 по модулю 4, дающие остаток $p_2 - 2$ по модулю p_2 и не дающие остатка $2^{a_1} p_2^{a_2} - 2$ по модулю $2^{a_1} p_2^{a_2}$. И множество

$$\begin{aligned}
& ((4p_2, 8p_2) \cup (8p_2, 16p_2) \cup \dots \cup ((2^{a_1-1} p_2, 2^{a_1} p_2)) \cup \\
& \cup ((2^{a_1} p_2, 2^{a_1} p_2^2) \cup (2^{a_1} p_2^2, 2^{a_1} p_2^3) \cup \dots \cup (2^{a_1} p_2^{a_2-1}, 2^{a_1} p_2^{a_2})) \cup \\
& \cup ((2 \cdot 2^{a_1} p_2, 2^{a_1} p_2^2) \cup (2 \cdot 2^{a_1} p_2^2, 2^{a_1} p_2^3) \cup \dots \cup (2 \cdot 2^{a_1} p_2^{a_2-1}, 2^{a_1} p_2^{a_2})) \cup \\
& \cup \dots \cup (((p_2 - 1) 2^{a_1} p_2, 2^{a_1} p_2^2) \cup ((p_2 - 1) 2^{a_1} p_2^2, 2^{a_1} p_2^3) \cup \\
& \cup \dots \cup ((p_2 - 1) 2^{a_1} p_2^{a_2-1}, 2^{a_1} p_2^{a_2}))
\end{aligned}$$

покрывает все числа, дающие остаток 0 по модулю 4, дающие остаток 0 по модулю p_2 и не дающие остатка 0 по модулю $2^{a_1} p_2^{a_2}$. Множество

$$(2p_2 - 2, 4p_2)$$

покрывает все числа, дающие остаток 0 по модулю 4 и дающие остаток $p_2 - 2$ по модулю p_2 . Наконец, множество

$$(2p_2, 4p_2)$$

покрывает все числа, дающие остаток 2 по модулю 4 и дающие остаток 0 по модулю p_2 . Поэтому

$$L(2p_2^{a_2}) \leq (2a_2 - 1)(p_2 - 1) + (2a_1 - 2).$$

Для доказательства нижней оценки введем обозначения

$$\begin{aligned} X_1 &:= \{p_2^{a_2}\}, \\ X_2 &:= \{4p_2^{a_2} - 2, 8p_2^{a_2} - 2, \dots, 2^{a_1-1}p_2^{a_2} - 2\}, \\ X_3 &:= \{4p_2^{a_2}, 8p_2^{a_2}, \dots, 2^{a_1-1}p_2^{a_2}\}, \\ X_4^1 &:= \{2^{a_1}p_2 - 2, 2 \cdot 2^{a_1}p_2 - 2, \dots, (a_2 - 1)2^{a_1}p_2 - 2\}, \\ X_4^2 &:= \{2^{a_1}p_2^2 - 2, 2 \cdot 2^{a_1}p_2^2 - 2, \dots, (a_2 - 1)2^{a_1}p_2^2 - 2\}, \\ &\dots\dots\dots \\ X_4^{a_2-1} &:= \{2^{a_1}p_2^{a_2-1} - 2, 2 \cdot 2^{a_1}p_2^{a_2-1} - 2, \dots, (a_2 - 1)2^{a_1}p_2^{a_2-1} - 2\}, \\ X_5^1 &:= \{2^{a_1}p_2, 2 \cdot 2^{a_1}p_2, \dots, (a_2 - 1)2^{a_1}p_2\}, \\ X_5^2 &:= \{2^{a_1}p_2^2, 2 \cdot 2^{a_1}p_2^2, \dots, (a_2 - 1)2^{a_1}p_2^2\}, \\ &\dots\dots\dots \\ X_5^{a_2-1} &:= \{2^{a_1}p_2^{a_2-1}, 2 \cdot 2^{a_1}p_2^{a_2-1}, \dots, (a_2 - 1)2^{a_1}p_2^{a_2-1}\}, \\ X_6 &:= \{a, b, c_1, \dots, c_{p_2-3}, c_{p_2-1}\}, \\ Y &:= (2^{a_2}p_2^{a_2} - 2, 2^{a_2}p_2^{a_2}) \cup (2^{a_2}p_2^{a_2}, 2^{a_2}p_2^{a_2}), \end{aligned}$$

где $a \equiv 0 \pmod{2^{a_1}}$, $a \equiv -2 \pmod{p_2^{a_2}}$, $b \equiv -2 \pmod{2^{a_1}}$, $b \equiv 0 \pmod{p_2^{a_2}}$, $c_i \equiv 0 \pmod{2^{a_1}}$, $c_i \equiv i \pmod{p_2^{a_2}}$. Покажем, что множество

$$X := X_1 \cup X_2 \cup X_3 \cup X_4^1 \cup \dots \cup X_4^{a_2-1} \cup X_5^1 \cup \dots \cup X_5^{a_2-1} \cup X_6$$

будет опорным семейством для множества Y . Пусть $x_1, x_2 \in X$, $x_1 < x_2$. Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1, x_2 - x_1) \cap (2^{a_1}p_2^{a_2} - 2, 2^{a_1}p_2^{a_2}) \neq \emptyset, \quad (5)$$

$$(x_1, x_2 - x_1) \cap (2^{a_1} p_2^{a_2}, 2^{a_1} p_2^{a_2}) \neq \emptyset. \quad (6)$$

Возможны случаи:

Случай 1.

$x_1 \in X_1, x_2 \in X_2$ или $x_2 \in X_1, x_1 \in X_2$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 1$ и по лемме 1 верно (5).

Случай 2.

$x_1 \in X_1, x_2 \in X_3$ или $x_2 \in X_1, x_1 \in X_3$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = p_2^{a_2}$ и по лемме 1 верно (6).

Случай 3.

$x_1 \in X_1, x_2 \in X_4^i$ или $x_2 \in X_1, x_1 \in X_4^i$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 1$ и по лемме 1 верно (5).

Случай 4.

$x_1 \in X_1, x_2 \in X_5^i$ или $x_2 \in X_1, x_1 \in X_5^i$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = p_2^i$ и по лемме 1 верно (6).

Случай 5.

$x_1 \in X_1, x_2 = a$ или $x_2 \in X_1, x_1 = a$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 1$ и по лемме 1 верно (5).

Случай 6.

$x_1 \in X_1, x_2 = b$ или $x_2 \in X_1, x_1 = b$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = p_2^{a_2}$ и по лемме 1 верно (6).

Случай 7.

$x_1 \in X_1, x_2 = c_i$ или $x_2 \in X_1, x_1 = c_i$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 1$ и по лемме 1 верно (5).

Случай 8.

$x_1 \in X_2, x_2 \in X_2$, то есть $x_1 = 2^{i_1} p_2^{a_2} - 2, x_2 = 2^{i_2} p_2^{a_2} - 2$. Тогда верно $\text{НОД}(x_2 - x_1, 2 p_2^{a_2}) = 2^{i_1} p_2^{a_2}$ и по лемме 1 получаем (5).

Случай 9.

$x_1 \in X_2, x_2 \in X_3$ или $x_2 \in X_2, x_1 \in X_3$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 10.

$x_1 \in X_2, x_2 \in X_4^i$ или $x_2 \in X_2, x_1 \in X_4^i$. Пусть элемент из X_2 равен $2^j p_2^{a_2} - 2$. Тогда имеет место $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^j p_2^i$ и по лемме 1 верно (5).

Случай 11.

$x_1 \in X_2, x_2 \in X_5^i$ или $x_2 \in X_2, x_1 \in X_5^i$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 12.

$x_1 \in X_2, x_2 = a$ или $x_2 \in X_2, x_1 = a$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2 p_2^{a_2}$ и

по лемме 1 верно (5).

Случай 13.

$x_1 \in X_2, x_2 = b$ или $x_2 \in X_2, x_1 = b$. Пусть элемент из X_2 равен $2^j p_2^{a_2} - 2$. Тогда имеет место $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^j$ и по лемме 1 верно (5).

Случай 14.

$x_1 \in X_2, x_2 = c_i$ или $x_2 \in X_2, x_1 = c_i$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 15.

$x_1 \in X_3, x_2 \in X_3$, то есть $x_1 = 2^{i_1} p_2^{a_2}$, $x_2 = 2^{i_2} p_2^{a_2}$. Тогда верно, что $\text{НОД}(x_2 - x_1, 2 p_2^{a_2}) = 2^{i_1} p_2^{a_2}$ и по лемме 1 получаем (6).

Случай 16.

$x_1 \in X_3, x_2 \in X_4^i$ или $x_2 \in X_3, x_1 \in X_4^i$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 17.

$x_1 \in X_3, x_2 \in X_5^i$ или $x_2 \in X_3, x_1 \in X_5^i$. Пусть элемент из X_3 равен $2^j p_2^{a_2}$. Тогда имеет место $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^j p_2^i$ и по лемме 1 верно (6).

Случай 18.

$x_1 \in X_3, x_2 = a$ или $x_2 \in X_3, x_1 = a$. Пусть элемент из X_3 равен $2^j p_2^{a_2}$. Тогда имеет место равенство $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^j$ и по лемме 1 верно (6).

Случай 19.

$x_1 \in X_3, x_2 = b$ или $x_2 \in X_3, x_1 = b$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2 p_2^{a_2}$ и по лемме 1 верно (6).

Случай 20.

$x_1 \in X_3, x_2 = c_i$ или $x_2 \in X_3, x_1 = c_i$. Пусть элемент из X_3 равен $2^j p_2^{a_2}$. Тогда имеет место равенство $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^j$ и по лемме 1 верно (6).

Случай 21.

$x_1 \in X_4^i, x_2 \in X_4^i$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1} p_2^i$ и по лемме 1 верно (5).

Случай 22.

$x_1 \in X_4^i, x_2 \in X_4^j, i < j$. Случай аналогичен предыдущему.

Случай 23.

$x_1 \in X_4^i, x_2 \in X_4^j, i > j$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1} p_2^j$ и по лемме 1 верно (5).

Случай 24.

$x_1 \in X_4^i, x_2 \in X_5^j$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 25.

$x_1 \in X_4^i, x_2 = a$ или $x_2 \in X_4^i, x_1 = a$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2p_2^i$ и по лемме 1 верно (5).

Случай 26.

$x_1 \in X_4^i, x_2 = b$ или $x_2 \in X_4^i, x_1 = b$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1}$ и по лемме 1 верно (5).

Случай 27.

$x_1 \in X_4^i, x_2 = c_i$ или $x_2 \in X_4^i, x_1 = c_i$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 28.

$x_1 \in X_5^i, x_2 \in X_5^i$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1} p_2^i$ и по лемме 1 верно (6).

Случай 29.

$x_1 \in X_5^i, x_2 \in X_5^j, i < j$. Случай аналогичен предыдущему.

Случай 30. $x_1 \in X_5^i, x_2 \in X_5^j, i > j$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1} p_2^j$ и по лемме 1 верно (6).

Случай 31.

$x_1 \in X_5^i, x_2 = a$ или $x_2 \in X_5^i, x_1 = a$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1}$ и по лемме 1 верно (6).

Случай 32.

$x_1 \in X_5^i, x_2 = b$ или $x_2 \in X_5^i, x_1 = b$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2p_2^i$ и по лемме 1 верно (6).

Случай 33.

$x_1 \in X_5^i, x_2 = c_i$ или $x_2 \in X_5^i, x_1 = c_i$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1}$ и по лемме 1 верно (6).

Случай 34.

$x_1 = a, x_2 = b$ или $x_2 = a, x_1 = b$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Случай 35.

$x_1 = a, x_2 = c$ или $x_2 = a, x_1 = c$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2^{a_1}$ и по лемме 1 верно (6).

Случай 36.

$x_1 = b, x_2 = c$ или $x_2 = b, x_1 = c$. Тогда $\text{НОД}(x_2 - x_1, 2^{a_1} p_2^{a_2}) = 2$ и по лемме 1 верно (5).

Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y . Но в множестве X всего

$$\begin{aligned} & |X_1| + |X_2| + |X_3| + |X_4^1| + \dots + |X_4^{a_2-1}| + |X_5^1| + \dots + |X_5^{a_2-1}| + |X_6| = \\ & = 1 + 2(a_1 - 2) + 2(a_2 - 1)(p_2 - 1) + 2 + (p_2 - 2) = \end{aligned}$$

$$= (2a_2 - 1)(p_2 - 1) + 2(a_1 - 1)$$

элементов. Поэтому по лемме 2 получаем

$$L(2p_2^{a_2}) \geq (2a_2 - 1)(p_2 - 1) + 2(a_1 - 1).$$

В случае, когда $p_1 = 2, t = 2$, утверждение теоремы доказано.

Пусть $p_1 = 2, t > 2, a_1 = 1$. Докажем тогда, что

$$L(n) = L(2p_2^{a_2} \dots p_t^{a_t}) = (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + 1.$$

для доказательства верхней оценки нужно представить $T(n)$ в виде объединения

$$(2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + 1$$

арифметических прогрессий. Это можно сделать следующим образом:

$$\begin{aligned} T(n) = & (1, 2) \cup ((2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \dots \cup (2p_2 - 4, 2p_2)) \cup \\ & \cup ((2, 2p_3) \cup (4, 2p_3) \cup (6, 2p_3) \cup \dots \cup (2p_3 - 4, 2p_3)) \cup \dots \cup \\ & \cup ((2, 2p_t) \cup (4, 2p_t) \cup (6, 2p_t) \cup \dots \cup (2p_t - 4, 2p_t)) \cup \\ & \cup ((1 \cdot 2p_2p_3 \dots p_t - 2, 2p_2^2p_3 \dots p_t) \cup (2 \cdot 2p_2p_3 \dots p_t - 2, 2p_2^2p_3 \dots p_t) \cup \\ & \cup \dots \cup ((p_2 - 1) \cdot 2p_2p_3 \dots p_t - 2, 2p_2^2p_3 \dots p_t)) \cup \\ & \cup ((1 \cdot 2p_2^2p_3 \dots p_t - 2, 2p_2^3p_3 \dots p_t) \cup (2 \cdot 2p_2^2p_3 \dots p_t - 2, 2p_2^3p_3 \dots p_t) \cup \\ & \cup \dots \cup ((p_2 - 1) \cdot 2p_2^2p_3 \dots p_t - 2, 2p_2^3p_3 \dots p_t)) \cup \\ & \dots \dots \dots \cup ((1 \cdot 2p_2^{a_2-1}p_3 \dots p_t - 2, 2p_2^{a_2}p_3 \dots p_t) \cup \\ & \cup (2 \cdot 2p_2^{a_2-1}p_3 \dots p_t - 2, 2p_2^{a_2}p_3 \dots p_t) \cup \dots \cup \\ & \cup ((p_2 - 1) \cdot 2p_2^{a_2-1}p_3 \dots p_t - 2, 2p_2^{a_2}p_3 \dots p_t)) \cup \\ & \cup ((1 \cdot 2p_2^{a_2}p_3 \dots p_t - 2, 2p_2^{a_2}p_3^2p_4 \dots p_t) \cup \\ & \cup (2 \cdot 2p_2^{a_2}p_3 \dots p_t - 2, 2p_2^{a_2}p_3^2p_4 \dots p_t) \cup \\ & \cup \dots \cup ((p_3 - 1) \cdot 2p_2^{a_2}p_3 \dots p_t - 2, 2p_2^{a_2}p_3^2p_4 \dots p_t)) \cup \\ & \cup ((1 \cdot 2p_2^{a_2}p_3^2p_4 \dots p_t - 2, 2p_2^{a_2}p_3^3p_4 \dots p_t) \cup \\ & \cup (2 \cdot 2p_2^{a_2}p_3^2p_4 \dots p_t - 2, 2p_2^{a_2}p_3^3p_4 \dots p_t) \cup \end{aligned}$$

$$\begin{aligned}
& \cup \dots \cup ((p_3 - 1) \cdot 2p_2^{a_2} p_3^2 p_4 \dots p_t - 2, 2p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t - 2, 2p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \cup (2 \cdot 2p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t - 2, 2p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t - 2, 2p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup (2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup ((1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup (2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup (2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \dots \cup \\
& \cup ((p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup ((1 \cdot 2p_2 p_3 \dots p_t, 2p_2^2 p_3 \dots p_t) \cup (2 \cdot 2p_2 p_3 \dots p_t, 2p_2^2 p_3 \dots p_t) \cup \dots \cup \\
& \cup ((p_2 - 1) \cdot 2p_2 p_3 \dots p_t, 2p_2^2 p_3 \dots p_t) \cup \\
& \cup ((1 \cdot 2p_2^2 p_3 \dots p_t, 2p_2^3 p_3 \dots p_t) \cup (2 \cdot 2p_2^2 p_3 \dots p_t, 2p_2^3 p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot 2p_2^2 p_3 \dots p_t, 2p_2^3 p_3 \dots p_t) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2p_2^{a_2-1} p_3 \dots p_t, 2p_2^{a_2} p_3 \dots p_t) \cup \\
& \cup (2 \cdot 2p_2^{a_2-1} p_3 \dots p_t, 2p_2^{a_2} p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot 2p_2^{a_2-1} p_3 \dots p_t, 2p_2^{a_2} p_3 \dots p_t) \cup \\
& \cup ((1 \cdot 2p_2^{a_2} p_3 \dots p_t, 2p_2^{a_2} p_3^2 p_4 \dots p_t) \cup \\
& \cup (2 \cdot 2p_2^{a_2} p_3 \dots p_t, 2p_2^{a_2} p_3^2 p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2p_2^{a_2} p_3 \dots p_t, 2p_2^{a_2} p_3^2 p_4 \dots p_t) \cup
\end{aligned}$$

$$\begin{aligned}
& \cup((1 \cdot 2p_2^{a_2} p_3^2 p_4 \dots p_t, 2p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \cup(2 \cdot 2p_2^{a_2} p_3^2 p_4 \dots p_t, 2p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2p_2^{a_2} p_3^2 p_4 \dots p_t, 2p_2^{a_2} p_3^3 p_4 \dots p_t)) \cup \\
& \dots \dots \dots \\
& \cup((1 \cdot 2p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t, 2p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \cup(2 \cdot 2p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t, 2p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t, 2p_2^{a_2} p_3^{a_3} p_4 \dots p_t)) \cup \\
& \dots \dots \dots \\
& \cup((1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup(2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2)) \cup \\
& \cup((1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup(2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3)) \cup \\
& \dots \dots \dots \\
& \cup((1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup(2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t})) \cup \\
& \cup(2a_1, 2p_2 p_t) \cup (2a_2, 2p_2 p_3) \cup \dots \cup (2a_{t-1}, 2p_{t-1} p_t),
\end{aligned}$$

где при $i = 1$ имеем $1 \leq a_1 \leq p_2 p_t$, $a_1 \equiv 0 \pmod{p_t}$, $a_1 \equiv -1 \pmod{p_2}$ и при $2 \leq i \leq t-1$ имеем $1 \leq a_i \leq p_i p_{i+1}$, $a_i \equiv 0 \pmod{p_i}$, $a_i \equiv -1 \pmod{p_{i+1}}$.
Здесь серия

$$\begin{aligned} & ((2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \dots \cup (2p_2 - 4, 2p_2)) \cup \\ & \cup ((2, 2p_3) \cup (4, 2p_3) \cup (6, 2p_3) \cup \dots \cup (2p_3 - 4, 2p_3)) \cup \dots \cup \\ & \cup ((2, 2p_t) \cup (4, 2p_t) \cup (6, 2p_t) \cup \dots \cup (2p_t - 4, 2p_t)) \end{aligned}$$

накрывает все четные числа, не сравнимые с 0 и -2 по модулям $p_2, \dots, p_t$.
Серия

$$\begin{aligned}
& ((1 \cdot 2p_2p_3 \dots p_t - 2, 2p_2^2p_3 \dots p_t) \cup (2 \cdot 2p_2p_3 \dots p_t - 2, 2p_2^2p_3 \dots p_t) \cup \\
& \quad \cup \dots \cup ((p_2 - 1) \cdot 2p_2p_3 \dots p_t - 2, 2p_2^2p_3 \dots p_t)) \cup \\
& \cup ((1 \cdot 2p_2^2p_3 \dots p_t - 2, 2p_2^3p_3 \dots p_t) \cup (2 \cdot 2p_2^2p_3 \dots p_t - 2, 2p_2^3p_3 \dots p_t) \cup \\
& \quad \cup \dots \cup ((p_2 - 1) \cdot 2p_2^2p_3 \dots p_t - 2, 2p_2^3p_3 \dots p_t)) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2p_2^{a_2-1}p_3 \dots p_t - 2, 2p_2^{a_2}p_3 \dots p_t) \cup \\
& \quad \cup (2 \cdot 2p_2^{a_2-1}p_3 \dots p_t - 2, 2p_2^{a_2}p_3 \dots p_t) \cup \\
& \quad \cup \dots \cup ((p_2 - 1) \cdot 2p_2^{a_2-1}p_3 \dots p_t - 2, 2p_2^{a_2}p_3 \dots p_t)) \cup \\
& \quad \cup ((1 \cdot 2p_2^{a_2}p_3 \dots p_t - 2, 2p_2^{a_2}p_3^2p_4 \dots p_t) \cup \\
& \quad \cup (2 \cdot 2p_2^{a_2}p_3 \dots p_t - 2, 2p_2^{a_2}p_3^2p_4 \dots p_t) \cup \\
& \quad \cup \dots \cup ((p_3 - 1) \cdot 2p_2^{a_2}p_3 \dots p_t - 2, 2p_2^{a_2}p_3^2p_4 \dots p_t)) \cup \\
& \quad \cup ((1 \cdot 2p_2^{a_2}p_3^2p_4 \dots p_t - 2, 2p_2^{a_2}p_3^3p_4 \dots p_t) \cup \\
& \quad \cup (2 \cdot 2p_2^{a_2}p_3^2p_4 \dots p_t - 2, 2p_2^{a_2}p_3^3p_4 \dots p_t) \cup \\
& \quad \cup \dots \cup ((p_3 - 1) \cdot 2p_2^{a_2}p_3^2p_4 \dots p_t - 2, 2p_2^{a_2}p_3^3p_4 \dots p_t)) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2p_2^{a_2}p_3^{a_3-1}p_4 \dots p_t - 2, 2p_2^{a_2}p_3^{a_3}p_4 \dots p_t) \cup \\
& \quad \cup (2 \cdot 2p_2^{a_2}p_3^{a_3-1}p_4 \dots p_t - 2, 2p_2^{a_2}p_3^{a_3}p_4 \dots p_t) \cup \\
& \quad \cup \dots \cup ((p_3 - 1) \cdot 2p_2^{a_2}p_3^{a_3-1}p_4 \dots p_t - 2, 2p_2^{a_2}p_3^{a_3}p_4 \dots p_t)) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}}p_t - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}}p_t^2) \cup \\
& \quad \cup (2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}}p_t - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}}p_t^2) \cup \\
& \quad \cup \dots \cup ((p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}}p_t - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}}p_t^2)) \cup \\
& \quad \cup ((1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}}p_t^2 - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}}p_t^3) \cup \\
& \quad \cup (2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}}p_t^2 - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}}p_t^3) \cup \dots \cup \\
& \quad \cup ((p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}}p_t^2 - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}}p_t^3)) \cup
\end{aligned}$$

$$\begin{aligned}
& \cup((1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup(2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}))
\end{aligned}$$

накрывает все четные числа, сравнимые с -2 по модулям $p_2, \dots, p_t$, но не сравнимые с -2 по модулю $2p_2^{a_2} \dots p_t^{a_t}$. Серия

$$\begin{aligned}
& ((1 \cdot 2p_2 p_3 \dots p_t, 2p_2^2 p_3 \dots p_t) \cup (2 \cdot 2p_2 p_3 \dots p_t, 2p_2^2 p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot 2p_2 p_3 \dots p_t, 2p_2^2 p_3 \dots p_t)) \cup \\
& \cup((1 \cdot 2p_2^2 p_3 \dots p_t, 2p_2^3 p_3 \dots p_t) \cup (2 \cdot 2p_2^2 p_3 \dots p_t, 2p_2^3 p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot 2p_2^2 p_3 \dots p_t, 2p_2^3 p_3 \dots p_t)) \cup
\end{aligned}$$

$$\begin{aligned}
& \cup((1 \cdot 2p_2^{a_2-1} p_3 \dots p_t, 2p_2^{a_2} p_3 \dots p_t) \cup \\
& \cup(2 \cdot 2p_2^{a_2-1} p_3 \dots p_t, 2p_2^{a_2} p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot 2p_2^{a_2-1} p_3 \dots p_t, 2p_2^{a_2} p_3 \dots p_t)) \cup \\
& \cup((1 \cdot 2p_2^{a_2} p_3 \dots p_t, 2p_2^{a_2} p_3^2 p_4 \dots p_t) \cup \\
& \cup(2 \cdot 2p_2^{a_2} p_3 \dots p_t, 2p_2^{a_2} p_3^2 p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2p_2^{a_2} p_3 \dots p_t, 2p_2^{a_2} p_3^2 p_4 \dots p_t)) \cup \\
& \cup((1 \cdot 2p_2^{a_2} p_3^2 p_4 \dots p_t, 2p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \cup(2 \cdot 2p_2^{a_2} p_3^2 p_4 \dots p_t, 2p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2p_2^{a_2} p_3^2 p_4 \dots p_t, 2p_2^{a_2} p_3^3 p_4 \dots p_t)) \cup
\end{aligned}$$

$$\begin{aligned}
& \cup((1 \cdot 2p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t, 2p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \cup(2 \cdot 2p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t, 2p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t, 2p_2^{a_2} p_3^{a_3} p_4 \dots p_t)) \cup
\end{aligned}$$

$$\begin{aligned}
& \cup((1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup(2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup
\end{aligned}$$

$$\begin{aligned}
& \cup \dots \cup ((p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \quad \cup ((1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \quad \cup (2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \quad \cup (2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t})
\end{aligned}$$

накрывает все четные числа, сравнимые с 0 по модулям $2p_2, \dots, 2p_t$, но не сравнимые с 0 по модулю $2p_2^{a_2} \dots p_t^{a_t}$. Наконец, серия

$$(2a_1, 2p_2 p_t) \cup (2a_2, 2p_2 p_3) \cup \dots \cup (2a_{t-1}, 2p_{t-1} p_t)$$

накрывает все четные числа, сравнимые с 0 или -2 по модулям $p_2, \dots, p_t$, но не сравнимые с 0 или -2 по модулю $2p_2 \dots p_t$. Поэтому

$$\begin{aligned}
L(n) & \leq 1 + \sum_{i=2}^t (p_i - 2) + 2 \sum_{i=2}^t (a_i - 1)(p_i - 1) + (t - 1) = \\
& = (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + 1.
\end{aligned}$$

Для доказательства нижней оценки введем обозначения

$$\begin{aligned}
X_1 & := \{p_2^{a_2} \dots p_t^{a_t}\}, \\
X_2^{2,1} & := \{1 \cdot 2p_2 p_3^{a_3} \dots p_t^{a_t} - 2, 2 \cdot 2p_2 p_3^{a_3} \dots p_t^{a_t} - 2, \dots, (p_2 - 1) \cdot 2p_2 p_3^{a_3} \dots p_t^{a_t} - 2\}, \\
X_2^{2,2} & := \{1 \cdot 2p_2^2 p_3^{a_3} \dots p_t^{a_t} - 2, 2 \cdot 2p_2^2 p_3^{a_3} \dots p_t^{a_t} - 2, \dots, (p_2 - 1) \cdot 2p_2^2 p_3^{a_3} \dots p_t^{a_t} - 2\}, \\
& \dots \dots \dots \\
X_2^{2,a_2-1} & := \{1 \cdot 2p_2^{a_2-1} p_3^{a_3} \dots p_t^{a_t} - 2, \dots, (p_2 - 1) \cdot 2p_2^{a_2-1} p_3^{a_3} \dots p_t^{a_t} - 2\}, \\
& \dots \dots \dots \\
X_2^{t,1} & := \{1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t - 2, \dots, (p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t - 2\}, \\
X_2^{t,2} & := \{1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, \dots, (p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2\}, \\
& \dots \dots \dots
\end{aligned}$$

$$\begin{aligned}
X_2^{t,a_t-1} &:= \{1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_{t-1}-1} - 2, \dots, (p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_{t-1}-1} - 2\}, \\
X_3^{2,1} &:= \{1 \cdot 2p_2 p_3^{a_3} \dots p_t^{a_t}, 2 \cdot 2p_2 p_3^{a_3} \dots p_t^{a_t}, \dots, (p_2 - 1) \cdot 2p_2 p_3^{a_3} \dots p_t^{a_t}\}, \\
X_3^{2,2} &:= \{1 \cdot 2p_2^2 p_3^{a_3} \dots p_t^{a_t}, 2 \cdot 2p_2^2 p_3^{a_3} \dots p_t^{a_t}, \dots, (p_2 - 1) \cdot 2p_2^2 p_3^{a_3} \dots p_t^{a_t}\}, \\
&\dots\dots\dots \\
X_3^{2,a_2-1} &:= \{1 \cdot 2p_2^{a_2-1} p_3^{a_3} \dots p_t^{a_t}, \dots, (p_2 - 1) \cdot 2p_2^{a_2-1} p_3^{a_3} \dots p_t^{a_t}\}, \\
&\dots\dots\dots \\
X_3^{t,1} &:= \{1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, \dots, (p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t\}, \\
X_3^{t,2} &:= \{1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, \dots, (p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2\}, \\
&\dots\dots\dots \\
X_3^{t,a_t-1} &:= \{1 \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, \dots, (p_t - 1) \cdot 2p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}\}, \\
X_4^2 &:= \{2b_{2,1}, \dots, 2b_{2,p_2-2}\}, \\
&\dots\dots\dots \\
X_4^t &:= \{2b_{t,1}, \dots, 2b_{t,p_t-2}\}, \\
X_5 &:= \{2c_2, \dots, 2c_{t-1}, 2c_t\}, \\
Y &:= (2p_2^{a_2} \dots p_t^{a_t} - 2, 2p_2^{a_2} \dots p_t^{a_t}) \cup (2p_2^{a_2} \dots p_t^{a_t}, 2p_2^{a_2} \dots p_t^{a_t}),
\end{aligned}$$

где

$$\begin{aligned}
b_{i,j} &\equiv j \pmod{p_i^{a_i}}, \quad b_{i,j} \equiv 0 \pmod{\frac{n}{2p_i^{a_i}}}, \\
c_i &\equiv -1 \pmod{p_i^{a_i}}, \quad c_i \equiv 0 \pmod{\frac{n}{2p_i^{a_i}}}.
\end{aligned}$$

Покажем, что множество

$$\begin{aligned}
X &:= X_1 \cup X_2^{2,1} \cup \dots \cup X_2^{t,a_t-1} \cup \\
&\cup X_3^{2,1} \cup \dots \cup X_3^{t,a_t-1} \cup X_4^2 \cup \dots \cup X_4^t \cup X_5
\end{aligned}$$

будет опорным семейством для множества Y . Пусть $x_1, x_2 \in X$, $x_1 < x_2$. Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1, x_2 - x_1) \cap (n - 2, n) \neq \emptyset, \quad (7)$$

$$(x_1, x_2 - x_1) \cap (n, n) \neq \emptyset. \quad (8)$$

Возможны случаи:

Случай 1.

$x_1 \in X_1, x_2 \in X_2^{i,j}$ или $x_2 \in X_1, x_1 \in X_2^{i,j}$. Тогда $\text{НОД}(x_2 - x_1, n) = 1$ и значит по лемме 1 верно (7).

Случай 2.

$x_1 \in X_1, x_2 \in X_3^{i,j}$ или $x_2 \in X_1, x_1 \in X_3^{i,j}$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{2p_i^{a_i}} p_i^j$ и по лемме 1 верно (8).

Случай 3.

$x_1 \in X_1, x_2 \in X_4^i$ или $x_2 \in X_1, x_1 \in X_4^i$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{2p_i^{a_i}}$ и по лемме 1 верно (8).

Случай 4.

$x_1 \in X_1, x_2 = c_i$ или $x_2 \in X_1, x_1 = c_i$. Случай аналогичен предыдущему.

Случай 5.

$x_1 \in X_2^{i,j_1}, x_2 \in X_2^{i,j_2}, j_1 \leq j_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_1}$ и по лемме 1 верно (7).

Случай 6.

$x_1 \in X_2^{i,j_1}, x_2 \in X_2^{i,j_2}, j_1 > j_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_2}$ и по лемме 1 верно (7).

Случай 7.

$x_1 \in X_2^{i_1,j_1}, x_2 \in X_2^{i_2,j_2}, i_1 \neq i_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_{i_1}^{a_{i_1}} p_{i_2}^{a_{i_2}}} p_{i_1}^{j_1} p_{i_2}^{j_2}$ и по лемме 1 верно (7).

Случай 8.

$x_1 \in X_2^{i_1,j_1}, x_2 \in X_3^{i_2,j_2}$ или $x_2 \in X_2^{i_1,j_1}, x_1 \in X_3^{i_2,j_2}$. Тогда верно, что $\text{НОД}(x_2 - x_1, n) = 2$ и значит по лемме 1 получаем (7).

Случай 9.

$x_1 \in X_2^{i,j}, x_2 \in X_4^k$ или $x_2 \in X_2^{i,j}, x_1 \in X_4^k$. Случай аналогичен предыдущему.

Случай 10.

$x_1 \in X_2^{i,j}, x_2 = c_i$ или $x_2 \in X_2^{i,j}, x_1 = c_i$. Тогда $\text{НОД}(x_2 - x_1, n) = 2p_i^j$ и по лемме 1 верно (7).

Случай 11.

$x_1 \in X_2^{i_1,j}, x_2 = c_{i_2}, i_1 \neq i_2$ или $x_2 \in X_2^{i_1,j}, x_1 = c_{i_2}, i_1 \neq i_2$. Тогда $\text{НОД}(x_2 - x_1, n) = 2p_{i_2}^{a_{i_2}}$ и по лемме 1 верно (7).

Случай 12.

$x_1 \in X_3^{i,j_1}, x_2 \in X_3^{i,j_2}, j_1 \leq j_2$. Случай аналогичен случаю 5.

Случай 13.

$x_1 \in X_3^{i,j_1}, x_2 \in X_3^{i,j_2}, j_1 > j_2$. Случай аналогичен случаю 6.

Случай 14.

$x_1 \in X_3^{i_1, j_1}, x_2 \in X_3^{i_2, j_2}, i_1 \neq i_2$. Случай аналогичен случаю 7.

Случай 15.

$x_1 \in X_3^{i, j}, x_2 \in X_4^i$ или $x_2 \in X_3^{i, j}, x_1 \in X_4^i$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i}}$ и по лемме 1 верно (8).

Случай 16.

$x_1 \in X_3^{i, j}, x_2 \in X_4^k, i \neq k$ или $x_2 \in X_3^{i, j}, x_1 \in X_4^i, i \neq k$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i} p_k^{a_k}} p_i^j$ и по лемме 1 верно (8).

Случай 17.

$x_1 \in X_3^{i, j}, x_2 = c_i$ или $x_2 \in X_2^{i, j}, x_1 = c_i$. Случай аналогичен случаю 15.

Случай 18.

$x_1 \in X_3^{i, j}, x_2 = c_k, i \neq k$ или $x_2 \in X_3^{i, j}, x_1 = c_k, i \neq k$. Случай аналогичен случаю 16.

Случай 19.

$x_1 \in X_4^i, x_2 \in X_4^i$. Случай аналогичен случаю 15.

Случай 20.

$x_1 \in X_4^i, x_2 \in X_4^j, i \neq j$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i} p_j^{a_j}}$ и по лемме 1 верно (8).

Случай 21.

$x_1 \in X_4^i, x_2 = c_i$ или $x_1 \in X_4^i, x_2 = c_i$. Случай аналогичен случаю 15.

Случай 22.

$x_1 \in X_4^i, x_2 = c_j, i \neq j$ или $x_2 \in X_4^i, x_1 = c_j, i \neq j$. Случай аналогичен случаю 20.

Случай 23.

$x_1 = c_i, x_2 = c_j$. Случай аналогичен случаю 20.

Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y . Но в множестве X всего

$$\begin{aligned} & |X_1| + |X_2^{2,1}| + \dots + |X_2^{t, a_t-1}| + |X_3^{2,1}| + \dots + |X_3^{t, a_t-1}| + |X_4^2| + \dots + |X_4^t| + |X_5| = \\ & = 1 + 2(p_2 - 1)(a_2 - 1) + \dots + 2(p_t - 1)(a_t - 1) + (p_2 - 2) + \dots + (p_t - 2) + (t - 1) = \\ & = (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + 1. \end{aligned}$$

элементов. Поэтому по лемме 2 получаем

$$L(2p_2^{a_2} \dots p_t^{a_t}) \geq (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + 1.$$

В случае, когда $p_1 = 2, t > 2, a_1 = 1$, утверждение теоремы доказано.

Пусть $p_1 = 2, t > 2, a_1 > 1$. Докажем тогда, что

$$L(n) = L(2^{a_1} p_2^{a_2} \dots p_t^{a_t}) = (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + (2a_1 - 2).$$

Для доказательства верхней оценки нужно представить $T(n)$ в виде объединения

$$(2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + (2a_1 - 2)$$

арифметических прогрессий. Это можно сделать следующим образом:

$$\begin{aligned} T(n) = & (1, 2) \cup ((2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \dots \cup (2p_2 - 4, 2p_2)) \cup \\ & \cup ((2, 2p_3) \cup (4, 2p_3) \cup (6, 2p_3) \cup \dots \cup (2p_3 - 4, 2p_3)) \cup \dots \cup \\ & \cup ((2, 2p_t) \cup (4, 2p_t) \cup (6, 2p_t) \cup \dots \cup (2p_t - 4, 2p_t)) \cup \\ & \cup ((4p_2 \dots p_t - 2, 8p_2 \dots p_t) \cup (8p_2 \dots p_t - 2, 16p_2 \dots p_t) \cup \\ & \quad \cup \dots \cup (2^{a_1-1} p_2 \dots p_t - 2, 2^{a_1} p_2 \dots p_t)) \cup \\ & \quad \cup ((1 \cdot 2^{a_1} p_2 p_3 \dots p_t - 2, 2^{a_1} p_2^2 p_3 \dots p_t) \cup \\ & \quad \cup (2 \cdot 2^{a_1} p_2 p_3 \dots p_t - 2, 2^{a_1} p_2^2 p_3 \dots p_t) \cup \\ & \quad \cup \dots \cup ((p_2 - 1) \cdot 2^{a_1} p_2 p_3 \dots p_t - 2, 2^{a_1} p_2^2 p_3 \dots p_t)) \cup \\ & \quad \cup ((1 \cdot 2^{a_1} p_2^2 p_3 \dots p_t - 2, 2^{a_1} p_2^3 p_3 \dots p_t) \cup \\ & \quad \cup (2 \cdot 2^{a_1} p_2^2 p_3 \dots p_t - 2, 2^{a_1} p_2^3 p_3 \dots p_t) \cup \\ & \quad \cup \dots \cup ((p_2 - 1) \cdot 2^{a_1} p_2^2 p_3 \dots p_t - 2, 2^{a_1} p_2^3 p_3 \dots p_t)) \cup \\ & \quad \dots \dots \dots \cup ((1 \cdot 2^{a_1} p_2^{a_2-1} p_3 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3 \dots p_t) \cup \\ & \quad \cup (2 \cdot 2^{a_1} p_2^{a_2-1} p_3 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3 \dots p_t) \cup \\ & \quad \cup \dots \cup ((p_2 - 1) \cdot 2^{a_1} p_2^{a_2-1} p_3 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3 \dots p_t)) \cup \\ & \quad \cup ((1 \cdot 2^{a_1} p_2^{a_2} p_3 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t) \cup \\ & \quad \cup (2 \cdot 2^{a_1} p_2^{a_2} p_3 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t) \cup \\ & \quad \cup \dots \cup ((p_3 - 1) \cdot 2^{a_1} p_2^{a_2} p_3 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t)) \cup \\ & \quad \cup ((1 \cdot 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\ & \quad \cup (2 \cdot 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \end{aligned}$$

$$\begin{aligned}
& \cup \dots \cup ((p_3 - 1) \cdot 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2^{a_1} p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \cup (2 \cdot 2^{a_1} p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2^{a_1} p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup (2 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup ((1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup (2 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup (2 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \dots \cup \\
& \cup ((p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup ((4p_2 \dots p_t, 8p_2 \dots p_t) \cup (8p_2 \dots p_t, 16p_2 \dots p_t) \cup \dots \cup \\
& \cup (2^{a_1-1} p_2 \dots p_t, 2^{a_1} p_2 \dots p_t) \cup \\
& \cup ((1 \cdot 2^{a_1} p_2 p_3 \dots p_t, 2^{a_1} p_2^2 p_3 \dots p_t) \cup \\
& \cup (2 \cdot 2^{a_1} p_2 p_3 \dots p_t, 2^{a_1} p_2^2 p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot 2^{a_1} p_2 p_3 \dots p_t, 2^{a_1} p_2^2 p_3 \dots p_t) \cup \\
& \cup ((1 \cdot 2^{a_1} p_2^2 p_3 \dots p_t, 2p_2^3 p_3 \dots p_t) \cup \\
& \cup (2 \cdot 2^{a_1} p_2^2 p_3 \dots p_t, 2^{a_1} p_2^3 p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot 2^{a_1} p_2^2 p_3 \dots p_t, 2^{a_1} p_2^3 p_3 \dots p_t) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2^{a_1} p_2^{a_2-1} p_3 \dots p_t, 2^{a_1} p_2^{a_2} p_3 \dots p_t) \cup \\
& \cup (2 \cdot 2^{a_1} p_2^{a_2-1} p_3 \dots p_t, 2^{a_1} p_2^{a_2} p_3 \dots p_t) \cup
\end{aligned}$$

$$\begin{aligned}
& \cup \dots \cup ((p_2 - 1) \cdot 2^{a_1} p_2^{a_2-1} p_3 \dots p_t, 2^{a_1} p_2^{a_2} p_3 \dots p_t) \cup \\
& \quad \cup ((1 \cdot 2^{a_1} p_2^{a_2} p_3 \dots p_t, 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t) \cup \\
& \quad \cup (2 \cdot 2^{a_1} p_2^{a_2} p_3 \dots p_t, 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2^{a_1} p_2^{a_2} p_3 \dots p_t, 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t) \cup \\
& \quad \cup ((1 \cdot 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t, 2^{a_1} p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \quad \cup (2 \cdot 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t, 2^{a_1} p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t, 2^{a_1} p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2^{a_1} p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t, 2^{a_1} p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \quad \cup (2 \cdot 2^{a_1} p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t, 2^{a_1} p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2^{a_1} p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t, 2^{a_1} p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \quad \cup (2 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \quad \cup ((1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \quad \cup (2 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \quad \cup (2 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup ((2a_1, 4p_2) \cup (2a_2, 2p_2 p_3) \dots \cup (2a_{t-1}, 2p_{t-1} p_t) \cup (2a_t, 4p_t)),
\end{aligned}$$

где при $1 \leq i \leq t-1$ имеем

$$1 \leq a_i \leq p_i p_{i+1}, \quad a_i \equiv 0 \pmod{p_i}, \quad a_i \equiv -1 \pmod{p_{i+1}}$$

и при $i = t$ имеем

$$1 \leq a_t \leq 2p_t, \quad a_t \equiv 0 \pmod{p_t}, \quad a_t \equiv -1 \pmod{2}.$$

Здесь серия

$$\begin{aligned} & ((2, 2p_2) \cup (4, 2p_2) \cup (6, 2p_2) \cup \dots \cup (2p_2 - 4, 2p_2)) \cup \\ & \cup ((2, 2p_3) \cup (4, 2p_3) \cup (6, 2p_3) \cup \dots \cup \\ & \cup (2p_3 - 4, 2p_3)) \cup \dots \cup ((2, 2p_t) \cup (4, 2p_t) \cup (6, 2p_t) \cup \dots \cup (2p_t - 4, 2p_t)) \end{aligned}$$

накрывает все четные числа, не сравнимые с 0 и -2 по модулям $p_2, \dots, p_t$.

Серия

$$\begin{aligned} & ((4p_2 \dots p_t - 2, 8p_2 \dots p_t) \cup (8p_2 \dots p_t - 2, 16p_2 \dots p_t) \cup \\ & \cup \dots \cup (2^{a_1-1}p_2 \dots p_t - 2, 2^{a_1}p_2 \dots p_t)) \cup \\ & \cup ((1 \cdot 2^{a_1}p_2p_3 \dots p_t - 2, 2^{a_1}p_2^2p_3 \dots p_t) \cup \\ & \cup (2 \cdot 2^{a_1}p_2p_3 \dots p_t - 2, 2^{a_1}p_2^2p_3 \dots p_t) \cup \\ & \cup \dots \cup ((p_2 - 1) \cdot 2^{a_1}p_2p_3 \dots p_t - 2, 2^{a_1}p_2^2p_3 \dots p_t)) \cup \\ & \cup ((1 \cdot 2^{a_1}p_2^2p_3 \dots p_t - 2, 2^{a_1}p_2^3p_3 \dots p_t) \cup \\ & \cup (2 \cdot 2^{a_1}p_2^2p_3 \dots p_t - 2, 2^{a_1}p_2^3p_3 \dots p_t) \cup \\ & \cup \dots \cup ((p_2 - 1) \cdot 2^{a_1}p_2^2p_3 \dots p_t - 2, 2^{a_1}p_2^3p_3 \dots p_t)) \cup \\ & \dots \dots \dots \cup ((1 \cdot 2^{a_1}p_2^{a_2-1}p_3 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3 \dots p_t) \cup \\ & \cup (2 \cdot 2^{a_1}p_2^{a_2-1}p_3 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3 \dots p_t) \cup \\ & \cup \dots \cup ((p_2 - 1) \cdot 2^{a_1}p_2^{a_2-1}p_3 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3 \dots p_t)) \cup \\ & \cup ((1 \cdot 2^{a_1}p_2^{a_2}p_3 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3^2p_4 \dots p_t) \cup \\ & \cup (2 \cdot 2^{a_1}p_2^{a_2}p_3 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3^2p_4 \dots p_t) \cup \\ & \cup \dots \cup ((p_3 - 1) \cdot 2^{a_1}p_2^{a_2}p_3 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3^2p_4 \dots p_t)) \cup \\ & \cup ((1 \cdot 2^{a_1}p_2^{a_2}p_3^2p_4 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3^3p_4 \dots p_t) \cup \\ & \cup (2 \cdot 2^{a_1}p_2^{a_2}p_3^2p_4 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3^3p_4 \dots p_t) \cup \\ & \cup \dots \cup ((p_3 - 1) \cdot 2^{a_1}p_2^{a_2}p_3^2p_4 \dots p_t - 2, 2^{a_1}p_2^{a_2}p_3^3p_4 \dots p_t)) \cup \end{aligned}$$

$$\begin{aligned}
& \dots\dots\dots \\
& \cup((1 \cdot 2^{a_1} p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \cup(2 \cdot 2^{a_1} p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2^{a_1} p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t - 2, 2^{a_1} p_2^{a_2} p_3^{a_3} p_4 \dots p_t)) \cup \\
& \dots\dots\dots \\
& \cup((1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup(2 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2)) \cup \\
& \cup((1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup(2 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \dots \cup \\
& \cup((p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3)) \cup \\
& \dots\dots\dots \\
& \cup((1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup(2 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}))
\end{aligned}$$

накрывает все четные числа, сравнимые с -2 по модулям $4, p_2, \dots, p_t$, но не сравнимые с -2 по модулю $2^{a_1} p_2^{a_2} \dots p_t^{a_t}$. Серия

$$\begin{aligned}
& ((4p_2 \dots p_t, 8p_2 \dots p_t) \cup (8p_2 \dots p_t, 16p_2 \dots p_t) \cup \\
& \cup \dots \cup (2^{a_1-1} p_2 \dots p_t, 2^{a_1} p_2 \dots p_t)) \cup \\
& \cup((1 \cdot 2^{a_1} p_2 p_3 \dots p_t, 2^{a_1} p_2^2 p_3 \dots p_t) \cup (2 \cdot 2^{a_1} p_2 p_3 \dots p_t, 2^{a_1} p_2^2 p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot 2^{a_1} p_2 p_3 \dots p_t, 2^{a_1} p_2^2 p_3 \dots p_t)) \cup \\
& \cup((1 \cdot 2^{a_1} p_2^2 p_3 \dots p_t, 2^{a_1} p_2^3 p_3 \dots p_t) \cup (2 \cdot 2^{a_1} p_2^2 p_3 \dots p_t, 2^{a_1} p_2^3 p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot 2^{a_1} p_2^2 p_3 \dots p_t, 2^{a_1} p_2^3 p_3 \dots p_t)) \cup \\
& \dots\dots\dots \\
& \cup((1 \cdot 2^{a_1} p_2^{a_2-1} p_3 \dots p_t, 2^{a_1} p_2^{a_2} p_3 \dots p_t) \cup \\
& \cup(2 \cdot 2^{a_1} p_2^{a_2-1} p_3 \dots p_t, 2^{a_1} p_2^{a_2} p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot 2^{a_1} p_2^{a_2-1} p_3 \dots p_t, 2^{a_1} p_2^{a_2} p_3 \dots p_t)) \cup
\end{aligned}$$

$$\begin{aligned}
& \cup ((1 \cdot 2^{a_1} p_2^{a_2} p_3 \dots p_t, 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t) \cup \\
& \cup (2 \cdot 2^{a_1} p_2^{a_2} p_3 \dots p_t, 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2^{a_1} p_2^{a_2} p_3 \dots p_t, 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t)) \cup \\
& \cup ((1 \cdot 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t, 2^{a_1} p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \cup (2 \cdot 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t, 2^{a_1} p_2^{a_2} p_3^3 p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2^{a_1} p_2^{a_2} p_3^2 p_4 \dots p_t, 2^{a_1} p_2^{a_2} p_3^3 p_4 \dots p_t)) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2^{a_1} p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t, 2^{a_1} p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \cup (2 \cdot 2^{a_1} p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t, 2^{a_1} p_2^{a_2} p_3^{a_3} p_4 \dots p_t) \cup \\
& \cup \dots \cup ((p_3 - 1) \cdot 2^{a_1} p_2^{a_2} p_3^{a_3-1} p_4 \dots p_t, 2^{a_1} p_2^{a_2} p_3^{a_3} p_4 \dots p_t)) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup (2 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2)) \cup \\
& \cup ((1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup (2 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^3)) \cup \\
& \dots \dots \dots \cup ((1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup (2 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}))
\end{aligned}$$

накрывает все четные числа, сравнимые с 0 по модулям $4, p_2, \dots, p_t$, но не сравнимые с 0 по модулю $2^{a_1} p_2^{a_2} \dots p_t^{a_t}$. Наконец, серия

$$(2a_1, 4p_2) \cup (2a_2, 2p_2p_3) \dots \cup (2a_{t-1}, 2p_{t-1}p_t) \cup (2a_t, 4p_t)$$

накрывает все четные числа, сравнимые с 0 или -2 по модулям $4, p_2, \dots, p_t$, но не сравнимые с 0 или -2 по модулю $4p_2 \dots p_t$. Поэтому

$$L(n) \leq 1 + \sum_{i=2}^t (p_i - 2) + 2(a_1 - 2) + 2 \sum_{i=2}^t (a_i - 1)(p_i - 1) + t =$$

$$= (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + (2a_1 - 2).$$

Для доказательства нижней оценки введем обозначения

$$\begin{aligned} X_1 &:= \{p_2^{a_2} \dots p_t^{a_t}\}, \\ X_2^2 &:= \{2^2 p_2^{a_2} \dots p_t^{a_t} - 2\}, \dots, X_2^{a_1-1} := \{2^{a_1-1} p_2^{a_2} \dots p_t^{a_t} - 2\}, \\ X_3^2 &:= \{2^2 p_2^{a_2} \dots p_t^{a_t}\}, \dots, X_3^{a_1-1} := \{2^{a_1-1} p_2^{a_2} \dots p_t^{a_t}\}, \\ X_4^{2,1} &:= \{1 \cdot 2^{a_1} p_2 p_3^{a_3} \dots p_t^{a_t} - 2, \dots, (p_2 - 1) \cdot 2^{a_1} p_2 p_3^{a_3} \dots p_t^{a_t} - 2\}, \\ X_4^{2,2} &:= \{1 \cdot 2^{a_1} p_2^2 p_3^{a_3} \dots p_t^{a_t} - 2, \dots, (p_2 - 1) \cdot 2^{a_1} p_2^2 p_3^{a_3} \dots p_t^{a_t} - 2\}, \\ &\dots\dots\dots \\ X_4^{2,a_2-1} &:= \{1 \cdot 2^{a_1} p_2^{a_2-1} p_3^{a_3} \dots p_t^{a_t} - 2, \dots, (p_2 - 1) \cdot 2^{a_1} p_2^{a_2-1} p_3^{a_3} \dots p_t^{a_t} - 2\}, \\ &\dots\dots\dots \\ X_3^{t,1} &:= \{1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t - 2, \dots, (p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t - 2\}, \\ X_4^{t,2} &:= \{1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, \dots, (p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2\}, \\ &\dots\dots\dots \\ X_4^{t,a_t-1} &:= \{1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, \dots, (p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2\}, \\ X_5^{2,1} &:= \{1 \cdot 2^{a_1} p_2 p_3^{a_3} \dots p_t^{a_t}, \dots, (p_2 - 1) \cdot 2^{a_1} p_2 p_3^{a_3} \dots p_t^{a_t}\}, \\ X_5^{2,2} &:= \{1 \cdot 2^{a_1} p_2^2 p_3^{a_3} \dots p_t^{a_t}, \dots, (p_2 - 1) \cdot 2^{a_1} p_2^2 p_3^{a_3} \dots p_t^{a_t}\}, \\ &\dots\dots\dots \\ X_5^{2,a_2-1} &:= \{1 \cdot 2^{a_1} p_2^{a_2-1} p_3^{a_3} \dots p_t^{a_t}, \dots, (p_2 - 1) \cdot 2^{a_1} p_2^{a_2-1} p_3^{a_3} \dots p_t^{a_t}\}, \\ &\dots\dots\dots \\ X_5^{t,1} &:= \{1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t, \dots, (p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t\}, \\ X_5^{t,2} &:= \{1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2, \dots, (p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2\}, \\ &\dots\dots\dots \\ X_5^{t,a_t-1} &:= \{1 \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, \dots, (p_t - 1) \cdot 2^{a_1} p_2^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}\}, \\ X_6^2 &:= \{2b_{2,1}, \dots, 2b_{2,p_2-2}\}, \\ &\dots\dots\dots \\ X_6^t &:= \{2b_{t,1}, \dots, 2b_{t,p_t-2}\}, \end{aligned}$$

$$X_7 := \{2c_1, \dots, 2c_{t-1}, 2c_t\},$$

$$Y := (2p_2^{a_2} \dots p_t^{a_t} - 2, 2p_2^{a_2} \dots p_t^{a_t}) \cup (2p_2^{a_2} \dots p_t^{a_t}, 2p_2^{a_2} \dots p_t^{a_t}),$$

где

$$b_{i,j} \equiv j \pmod{p_i^{a_i}}, \quad b_{i,j} \equiv 0 \pmod{\frac{n}{2p_i^{a_i}}},$$

$$c_1 \equiv -1 \pmod{2^{a_1-1}}, \quad c_1 \equiv 0 \pmod{\frac{n}{2^{a_1}}}$$

и при $2 \leq i \leq t$ верно

$$c_i \equiv -1 \pmod{p_i^{a_i}}, \quad c_i \equiv 0 \pmod{\frac{n}{2p_i^{a_i}}}.$$

Покажем, что множество

$$X := X_1 \cup X_2^2 \cup \dots \cup X_2^{a_1-1} \cup X_3^2 \cup \dots \cup X_3^{a_1-1} \cup X_4^{2,1} \cup$$

$$\cup \dots \cup X_4^{t,a_t-1} \cup X_5^{2,1} \cup \dots \cup X_5^{t,a_t-1} \cup X_6^2 \cup \dots \cup X_6^t \cup X_7$$

будет опорным семейством для множества Y . Пусть $x_1, x_2 \in X$, $x_1 < x_2$. Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1, x_2 - x_1) \cap (n - 2, n) \neq \emptyset, \quad (9)$$

$$(x_1, x_2 - x_1) \cap (n, n) \neq \emptyset. \quad (10)$$

Возможны случаи:

Случай 1.

$x_1 \in X_1, x_2 \in X_2^i$ или $x_2 \in X_1, x_1 \in X_2^i$. Тогда $\text{НОД}(x_2 - x_1, n) = 2$ и значит по лемме 1 верно (9).

Случай 2.

$x_1 \in X_1, x_2 \in X_3^i$ или $x_2 \in X_1, x_1 \in X_3^i$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{2^{a_1}}$ и по лемме 1 верно (10).

Случай 3.

$x_1 \in X_1, x_2 \in X_4^{i,j}$ или $x_2 \in X_1, x_1 \in X_4^{i,j}$. Тогда $\text{НОД}(x_2 - x_1, n) = 1$ и по лемме 1 верно (9).

Случай 4.

$x_1 \in X_1, x_2 \in X_5^{i,j}$ или $x_2 \in X_1, x_1 \in X_5^{i,j}$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{2^{a_1} p_i^{a_i} p_i^j}$ и по лемме 1 верно (10).

Случай 5.

$x_1 \in X_1, x_2 \in X_6^i$ или $x_2 \in X_1, x_1 \in X_6^i$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i}}$ и по

лемме 1 верно (10).

Случай 6.

$x_1 \in X_1, x_2 = c_1$ или $x_2 \in X_1, x_1 = c_1$. Случай аналогичен случаю 2.

Случай 7.

$x_1 \in X_1, x_2 = c_i, i > 1$ или $x_2 \in X_1, x_1 = c_i, i > 1$. Тогда верно, что $\text{НОД}(x_2 - x_1, n) = \frac{n}{2^{a_1} p_i^{a_i}}$ и значит по лемме 1 получаем (10).

Случай 8.

$x_1 \in X_2^i, x_2 \in X_2^j, i < j$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{2^{a_1}} 2^i$ и по лемме 1 верно (9).

Случай 9.

$x_1 \in X_2^i, x_2 \in X_2^j, i > j$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{2^{a_1}} 2^j$ и по лемме 1 верно (9).

Случай 10.

$x_1 \in X_2^i, x_2 \in X_3^j$. Случай аналогичен случаю 1.

Случай 11.

$x_1 \in X_2^i, x_2 \in X_4^{j,k}$ или $x_2 \in X_2^i, x_1 \in X_4^{j,k}$. Тогда в этом случае верно, что $\text{НОД}(x_2 - x_1, n) = \frac{n}{2^{a_1} p_j^{a_j}} 2^i p_j^k$ и значит по лемме 1 получаем (9).

Случай 12.

$x_1 \in X_2^i, x_2 \in X_5^{j,k}$ или $x_2 \in X_2^i, x_1 \in X_5^{j,k}$. Случай аналогичен случаю 1.

Случай 13.

$x_1 \in X_2^i, x_2 \in X_6^j$ или $x_2 \in X_2^i, x_1 \in X_6^j$. Случай аналогичен случаю 1.

Случай 14.

$x_1 \in X_2^i, x_2 = c_1$ или $x_2 \in X_2^i, x_1 = c_1$. Тогда $\text{НОД}(x_2 - x_1, n) = 2^i$ и по лемме 1 верно (9).

Случай 15.

$x_1 \in X_2^i, x_2 = c_j, j > 1$ или $x_2 \in X_2^i, x_1 = c_j, j > 1$. Тогда верно, что $\text{НОД}(x_2 - x_1, n) = p_j^{a_j}$ и значит по лемме 1 получаем (9).

Случай 16.

$x_1 \in X_3^i, x_2 \in X_4^{j,k}$ или $x_2 \in X_3^i, x_1 \in X_4^{j,k}$. Случай аналогичен случаю 1.

Случай 17.

$x_1 \in X_3^i, x_2 \in X_5^{j,k}$ или $x_2 \in X_3^i, x_1 \in X_5^{j,k}$. Тогда в этом случае верно, что $\text{НОД}(x_2 - x_1, n) = \frac{n}{2^{a_1} p_j^{a_j}} 2^i p_j^k$ и значит по лемме 1 получаем (10).

Случай 18.

$x_1 \in X_3^i, x_2 \in X_6^j$ или $x_3 \in X_2^i, x_1 \in X_6^j$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{2^{a_1} p_j^{a_j}} 2^i$

и по лемме 1 верно (10).

Случай 19.

$x_1 \in X_3^i, x_2 = c_1$ или $x_2 \in X_3^i, x_1 = c_1$. Тогда $\text{НОД}(x_2 - x_1, n) = 2^{\frac{n}{2^{a_1}}}$ и по

лемме 1 верно (10).

Случай 20.

$x_1 \in X_3^i, x_2 = c_j, j > 1$ или $x_2 \in X_3^i, x_1 = c_j, j > 1$. Случай аналогичен случаю 18.

Случай 21.

$x_1 \in X_4^{i,j_1}, x_2 \in X_4^{i,j_2}, j_1 \leq j_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_1}$ и по лемме 1 верно (9).

Случай 22.

$x_1 \in X_4^{i,j_1}, x_2 \in X_4^{i,j_2}, j_1 > j_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_2}$ и по лемме 1 верно (9).

Случай 23.

$x_1 \in X_4^{i_1,j_1}, x_2 \in X_4^{i_2,j_2}, i_1 \neq i_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_{i_1}^{a_{i_1}} p_{i_2}^{a_{i_2}}} p_{i_1}^{j_1} p_{i_2}^{j_2}$ и по лемме 1 верно (9).

Случай 24.

$x_1 \in X_4^{i_1,j_1}, x_2 \in X_5^{i_2,j_2}$. Случай аналогичен случаю 1.

Случай 25.

$x_1 \in X_4^{i,j}, x_2 \in X_6^k$ или $x_2 \in X_4^{i,j}, x_1 \in X_6^k$. Случай аналогичен случаю 1.

Случай 26.

$x_1 \in X_4^{i,j}, x_2 = c_1$ или $x_2 \in X_4^{i,j}, x_1 = c_1$. Тогда $\text{НОД}(x_2 - x_1, n) = 2^{a_1}$ и по лемме 1 верно (9).

Случай 27.

$x_1 \in X_4^{i,j}, x_2 = c_k, k > 1$ или $x_2 \in X_4^{i,j}, x_1 = c_k, k > 1$. Тогда верно, что $\text{НОД}(x_2 - x_1, n) = 2p_i^j$ и по лемме 1 получаем (9).

Случай 28.

$x_1 \in X_5^{i,j_1}, x_2 \in X_5^{i,j_2}, j_1 \leq j_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_1}$ и по лемме 1 верно (10).

Случай 29.

$x_1 \in X_5^{i,j_1}, x_2 \in X_5^{i,j_2}, j_1 > j_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_2}$ и по лемме 1 верно (10).

Случай 30.

$x_1 \in X_5^{i_1,j_1}, x_2 \in X_5^{i_2,j_2}, i_1 \neq i_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_{i_1}^{a_{i_1}} p_{i_2}^{a_{i_2}}} p_{i_1}^{j_1} p_{i_2}^{j_2}$ и по лемме 1 верно (10).

Случай 31.

$x_1 \in X_5^{i,j}, x_2 \in X_6^i$ или $x_2 \in X_5^{i,j}, x_1 \in X_6^i$. Случай аналогичен случаю 5.

Случай 32.

$x_1 \in X_5^{i,j}, x_2 \in X_6^k, i \neq k$ или $x_2 \in X_5^{i,j}, x_1 \in X_6^k, i \neq k$. Тогда верно, что

$\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i} p_k^{a_k}} p_i^j$ и по лемме 1 получаем (10).

Случай 33.

$x_1 \in X_5^{i,j}, x_2 = c_1$ или $x_2 \in X_5^{i,j}, x_1 = c_1$. Тогда $\text{НОД}(x_2 - x_1, n) = 2 \frac{n}{2^{a_1} p_i^{a_i}} p_i^j$ и по лемме 1 верно (10).

Случай 34.

$x_1 \in X_5^{i,j}, x_2 = c_i$, или $x_2 \in X_5^{i,j}, x_1 = c_i$. Случай аналогичен случаю 5.

Случай 35.

$x_1 \in X_5^{i,j}, x_2 = c_k, k \neq i$ или $x_2 \in X_5^{i,j}, x_1 = c_k, k \neq i$. Тогда верно, что $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_k^{a_k} p_i^{a_i}} p_i^j$ и по лемме 1 получаем (10).

Случай 36.

$x_1 \in X_6^i, x_2 \in X_6^i$. Случай аналогичен случаю 5.

Случай 37.

$x_1 \in X_6^i, x_2 \in X_6^j, i \neq j$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i} p_j^{a_j}}$ и по лемме 1 верно (10).

Случай 38.

$x_1 \in X_6^i, x_2 = c_i$ или $x_1 \in X_6^i, x_2 = c_i$. Случай аналогичен случаю 5.

Случай 39.

$x_1 \in X_6^i, x_2 = c_1$ или $x_2 \in X_6^i, x_1 = c_1$. Тогда $\text{НОД}(x_2 - x_1, n) = 2 \frac{n}{2^{a_1} p_i^{a_i}}$ и по лемме 1 верно (10).

Случай 40.

$x_1 \in X_6^i, x_2 = c_j, i \neq j \neq 1$ или $x_2 \in X_6^i, x_1 = c_j, i \neq j \neq 1$. Случай аналогичен случаю 37.

Случай 41.

$x_1 = c_1, x_2 = c_i, i > 1$ или $x_2 = c_1, x_1 = c_i, i > 1$. Случай аналогичен случаю 39.

Случай 42.

$x_1 = c_i, x_2 = c_j, i, j \neq 1$. Случай аналогичен случаю 37.

Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y . Но в множестве X всего

$$\begin{aligned}
& |X_1| + |X_2^2| + \dots + |X_2^{a_1-1}| + |X_3^2| + \dots + |X_3^{a_1-1}| + \\
& + |X_4^{2,1}| + \dots + |X_4^{t, a_t-1}| + |X_5^{2,1}| + \\
& + \dots + |X_5^{t, a_t-1}| + |X_6^2| + \dots + |X_6^t| + |X_7| = \\
& = 1 + 2(a_1 - 2) + 2(p_2 - 1)(a_2 - 1) + \\
& + \dots + 2(p_t - 1)(a_t - 1) + (p_2 - 2) + \dots + (p_t - 2) + t =
\end{aligned}$$

$$= (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + (2a_1 - 2)$$

элементов. Поэтому по лемме 2 получаем

$$L(2^{a_1} p_2^{a_2} \dots p_t^{a_t}) \geq (2a_2 - 1)(p_2 - 1) + \dots + (2a_t - 1)(p_t - 1) + (2a_1 - 2).$$

В случае, когда $p_1 = 2, t > 2, a_1 > 1$, утверждение теоремы доказано.

Пусть $p_1 > 2, t = 1$. Докажем тогда, что

$$L(n) = L(p_1^{a_1}) = (2a_1 - 1)(p_1 - 1) - 1.$$

Сначала представим $T(n)$ в виде объединения $(2a_1 - 1)(p_1 - 1) - 1$ арифметических прогрессий. Это можно сделать следующим образом:

$$\begin{aligned} T(n) = & ((1, p_1) \cup (2, p_1) \cup \dots \cup (p_1 - 3, p_1) \cup (p_1 - 1, p_1)) \cup \\ & \cup((p_1 - 2, p_1^2) \cup (2p_1 - 2, p_1^2) \cup \dots \cup ((p_1 - 1)p_1 - 2, p_1^2)) \cup \\ & \cup((p_1^2 - 2, p_1^3) \cup (2p_1^2 - 2, p_1^3) \cup \dots \cup ((p_1 - 1)p_1^2 - 2, p_1^3)) \cup \\ & \dots \dots \dots \cup((p_1^{a_1-1} - 2, p_1^{a_1}) \cup (2p_1^{a_1-1} - 2, p_1^{a_1}) \cup \dots \cup ((p_1 - 1)p_1^{a_1-1} - 2, p_1^{a_1})) \cup \\ & \cup((p_1, p_1^2) \cup (2p_1, p_1^2) \cup \dots \cup ((p_1 - 1)p_1, p_1^2)) \cup \\ & \cup((p_1^2, p_1^3) \cup (2p_1^2, p_1^3) \cup \dots \cup ((p_1 - 1)p_1^2, p_1^3)) \cup \\ & \dots \dots \dots \cup((p_1^{a_1-1}, p_1^{a_1}) \cup (2p_1^{a_1-1}, p_1^{a_1}) \cup \dots \cup ((p_1 - 1)p_1^{a_1-1}, p_1^{a_1})). \end{aligned}$$

Видно, что здесь $(p_1 - 2) + 2(a_1 - 1)(p_1 - 1) = (2a_1 - 1)(p_1 - 1) - 1$ прогрессий. Множество

$$(1, p_1) \cup (2, p_1) \cup \dots \cup (p_1 - 3, p_1) \cup (p_1 - 1, p_1)$$

покрывает все числа, не сравнимые с 0 или -2 по модулю p_1 . Множество

$$\begin{aligned} & ((p_1 - 2, p_1^2) \cup (2p_1 - 2, p_1^2) \cup \dots \cup ((p_1 - 1)p_1 - 2, p_1^2)) \cup \\ & \cup((p_1^2 - 2, p_1^3) \cup (2p_1^2 - 2, p_1^3) \cup \dots \cup ((p_1 - 1)p_1^2 - 2, p_1^3)) \cup \\ & \dots \dots \dots \cup((p_1^{a_1-1} - 2, p_1^{a_1}) \cup (2p_1^{a_1-1} - 2, p_1^{a_1}) \cup \dots \cup ((p_1 - 1)p_1^{a_1-1} - 2, p_1^{a_1})) \end{aligned}$$

покрывает все числа, сравнимые с -2 по модулю p_1 , но не сравнимые с -2 по модулю $p_1^{a_1}$. Наконец, множество

$$\begin{aligned} & \cup((p_1, p_1^2) \cup (2p_1, p_1^2) \cup \dots \cup ((p_1 - 1)p_1, p_1^2)) \cup \\ & \cup((p_1^2, p_1^3) \cup (2p_1^2, p_1^3) \cup \dots \cup ((p_1 - 1)p_1^2, p_1^3)) \cup \\ & \dots \dots \dots \cup((p_1^{a_1-1}, p_1^{a_1}) \cup (2p_1^{a_1-1}, p_1^{a_1}) \cup \dots \cup ((p_1 - 1)p_1^{a_1-1}, p_1^{a_1})) \end{aligned}$$

покрывает все числа, сравнимые с 0 по модулю p_1 , но не сравнимые с 0 по модулю $p_1^{a_1}$. Поэтому

$$L(p_1^{a_1}) \leq (2a_1 - 1)(p_1 - 1) - 1.$$

Покажем, что

$$L(p_1^{a_1}) \geq (2a_1 - 1)(p_1 - 1) - 1.$$

Рассмотрим множества

$$\begin{aligned} X_1 &:= \{1, 2, \dots, p_1 - 3, p_1 - 1\}, \\ X_2^1 &:= \{p_1 - 2, 2p_1 - 2, \dots, (p_1 - 1)p_1 - 2\}, \\ X_2^2 &:= \{p_1^2 - 2, 2p_1^2 - 2, \dots, (p_1 - 1)p_1^2 - 2\}, \\ &\dots \dots \dots X_2^{a_1-1} := \{p_1^{a_1-1} - 2, 2p_1^{a_1-1} - 2, \dots, (p_1 - 1)p_1^{a_1-1} - 2\}, \\ X_3^1 &:= \{p_1, 2p_1, \dots, (p_1 - 1)p_1\}, \\ X_3^2 &:= \{p_1^2, 2p_1^2, \dots, (p_1 - 1)p_1^2\}, \\ &\dots \dots \dots X_3^{a_1-1} := \{p_1^{a_1-1}, 2p_1^{a_1-1}, \dots, (p_1 - 1)p_1^{a_1-1}\}, \\ Y &:= (2^{a_1} - 2, 2^{a_1}) \cup (2^{a_1}, 2^{a_1}). \end{aligned}$$

Покажем, что множество

$$X := X_1 \cup X_2^1 \cup \dots \cup X_2^{a_1-1} \cup X_3^1 \cup \dots \cup X_3^{a_1-1}$$

будет опорным семейством для множества Y . Пусть $x_1, x_2 \in X$, $x_1 < x_2$. Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1, x_2 - x_1) \cap (n - 2, n) \neq \emptyset, \quad (11)$$

$$(x_1, x_2 - x_1) \cap (n, n) \neq \emptyset. \quad (12)$$

Возможны случаи:

Случай 1.

$x_1 \in X_1, x_2 \in X_1$. Тогда $\text{НОД}(x_2 - x_1, n) = 1$ и по лемме 1 верно (11).

Случай 2.

$x_1 \in X_1, x_2 \in X_2^i$ или $x_2 \in X_1, x_1 \in X_2^i$. Случай аналогичен случаю 1.

Случай 3.

$x_1 \in X_1, x_2 \in X_3^i$ или $x_2 \in X_1, x_1 \in X_3^i$. Случай аналогичен случаю 1.

Случай 4.

$x_1 \in X_2^i, x_2 \in X_2^i$. Тогда $\text{НОД}(x_2 - x_1, n) = p_1^i$ и по лемме 1 верно (11).

Случай 5.

$x_1 \in X_2^i, x_2 \in X_2^j, i < j$. Тогда $\text{НОД}(x_2 - x_1, n) = p_1^i$ и поэтому по лемме 1 получаем (11).

Случай 6.

$x_1 \in X_2^i, x_2 \in X_2^j, i > j$. Тогда $\text{НОД}(x_2 - x_1, n) = p_1^j$ и поэтому по лемме 1 получаем (11).

Случай 7.

$x_1 \in X_2^i, x_2 \in X_3^j$. Случай аналогичен случаю 1.

Случай 8.

$x_1 \in X_3^i, x_2 \in X_3^i$. Тогда $\text{НОД}(x_2 - x_1, n) = p_1^i$ и по лемме 1 верно (12).

Случай 9.

$x_1 \in X_3^i, x_2 \in X_3^j, i < j$. Тогда $\text{НОД}(x_2 - x_1, n) = p_1^i$ и поэтому по лемме 1 верно (12).

Случай 10.

$x_1 \in X_3^i, x_2 \in X_3^j, i > j$. Тогда $\text{НОД}(x_2 - x_1, n) = p_1^j$ и поэтому по лемме 1 верно (12).

Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y . Но в множестве X всего

$$\begin{aligned} & |X_1| + |X_2^1| + |X_2^2| + \dots + |X_2^{a_1-1}| + |X_3^1| + |X_3^2| + \dots + |X_3^{a_1-1}| = \\ & = (p_1 - 2) + 2(a_1 - 1)(p_1 - 1) = (2a_1 - 1)(p_1 - 1) - 1 \end{aligned}$$

элементов. Поэтому по лемме 2 получаем

$$L(p_1^{a_1}) \geq (2a_1 - 1)(p_1 - 1) - 1.$$

В случае, когда $p_1 > 2, t = 1$, утверждение теоремы доказано.

Пусть $p_1 > 2, t > 1$. Докажем тогда, что

$$L(n) = L(p_1^{a_1} \dots p_t^{a_t}) = (2a_1 - 1)(p_1 - 1) + \dots + (2a_t - 1)(p_t - 1).$$

Для доказательства верхней оценки нужно представить $T(n)$ в виде объединения

$$(2a_1 - 1)(p_1 - 1) + \dots + (2a_t - 1)(p_t - 1)$$

арифметических прогрессий. Это можно сделать следующим образом:

$$\begin{aligned}
 T(n) = & ((1, p_1) \cup (2, p_1) \cup \dots \cup (p_1 - 3, p_1) \cup (p_1 - 1, p_1)) \cup \\
 & ((1, p_2) \cup (2, p_2) \cup \dots \cup (p_2 - 3, p_2) \cup (p_2 - 1, p_2)) \cup \\
 & \cup \dots \cup ((1, p_t) \cup (2, p_t) \cup \dots \cup (p_t - 3, p_t) \cup (p_t - 1, p_t)) \cup \\
 & \cup ((1 \cdot p_1 p_2 \dots p_t - 2, p_1^2 p_2 \dots p_t) \cup (2 \cdot p_1 p_2 \dots p_t - 2, p_1^2 p_2 \dots p_t) \cup \\
 & \cup \dots \cup ((p_1 - 1) \cdot p_1 p_2 \dots p_t - 2, p_1^2 p_2 \dots p_t)) \cup \\
 & \cup ((1 \cdot p_1^2 p_2 \dots p_t - 2, p_1^3 p_2 \dots p_t) \cup (2 \cdot p_1^2 p_2 \dots p_t - 2, p_1^3 p_2 \dots p_t) \cup \\
 & \cup \dots \cup ((p_2 - 1) \cdot p_1^2 p_2 \dots p_t - 2, p_1^3 p_2 \dots p_t)) \cup \\
 & \dots \dots \dots \cup ((1 \cdot p_1^{a_1-1} p_2 \dots p_t - 2, p_1^{a_1} p_2 \dots p_t) \cup \\
 & \cup (2 \cdot p_1^{a_1-1} p_2 \dots p_t - 2, p_1^{a_1} p_2 \dots p_t) \cup \\
 & \cup \dots \cup ((p_1 - 1) \cdot p_1^{a_1-1} p_2 \dots p_t - 2, p_1^{a_1} p_2 \dots p_t)) \cup \\
 & \cup ((1 \cdot p_1^{a_1} p_2 \dots p_t - 2, p_1^{a_1} p_2^2 p_3 \dots p_t) \cup \\
 & \cup (2 \cdot p_1^{a_1} p_2 \dots p_t - 2, p_1^{a_1} p_2^2 p_3 \dots p_t) \cup \\
 & \cup \dots \cup ((p_2 - 1) \cdot p_1^{a_1} p_2 \dots p_t - 2, p_1^{a_1} p_2^2 p_3 \dots p_t)) \cup \\
 & \cup ((1 \cdot p_1^{a_1} p_2^2 p_3 \dots p_t - 2, p_1^{a_1} p_2^3 p_3 \dots p_t) \cup \\
 & \cup (2 \cdot p_1^{a_1} p_2^2 p_3 \dots p_t - 2, p_1^{a_1} p_2^3 p_3 \dots p_t) \cup \\
 & \cup \dots \cup ((p_2 - 1) \cdot p_1^{a_1} p_2^2 p_3 \dots p_t - 2, p_1^{a_1} p_2^3 p_3 \dots p_t)) \cup \\
 & \dots \dots \dots \cup ((1 \cdot p_1^{a_1} p_2^{a_2-1} p_3 \dots p_t - 2, p_1^{a_1} p_2^{a_2} p_3 \dots p_t) \cup \\
 & \cup (2 \cdot p_1^{a_1} p_2^{a_2-1} p_3 \dots p_t - 2, p_1^{a_1} p_2^{a_2} p_3 \dots p_t) \cup \\
 & \cup \dots \cup ((p_2 - 1) \cdot p_1^{a_1} p_2^{a_2-1} p_3 \dots p_t - 2, p_1^{a_1} p_2^{a_2} p_3 \dots p_t)) \cup \\
 & \dots \dots \dots \cup ((1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}-1} p_t - 2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup
 \end{aligned}$$

$$\begin{aligned}
& \cup (2 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t - 2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t - 2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup ((1 \cdot p_1^{a_2} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup (2 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \dots \dots \dots \cup ((1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup (2 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup ((1 \cdot p_1 p_2 \dots p_t, p_1^2 p_2 \dots p_t) \cup (2 \cdot p_1 p_2 \dots p_t, p_1^2 p_2 \dots p_t) \cup \\
& \cup \dots \cup ((p_1 - 1) \cdot p_1 p_2 \dots p_t, p_1^2 p_2 \dots p_t)) \cup \\
& \cup ((1 \cdot p_1^2 p_2 \dots p_t, p_1^3 p_2 \dots p_t) \cup (2 \cdot p_1^2 p_2 \dots p_t, p_1^3 p_2 \dots p_t) \cup \\
& \cup \dots \cup ((p_1 - 1) \cdot p_1^2 p_2 \dots p_t, p_1^3 p_2 \dots p_t)) \cup \\
& \dots \dots \dots \cup ((1 \cdot p_1^{a_1-1} p_2 \dots p_t, p_1^{a_1} p_2 \dots p_t) \cup (2 \cdot p_1^{a_1-1} p_2 \dots p_t, p_1^{a_1} p_2 \dots p_t) \cup \\
& \cup \dots \cup ((p_1 - 1) \cdot p_1^{a_1-1} p_2 \dots p_t, p_1^{a_1} p_2 \dots p_t)) \cup \\
& \cup ((1 \cdot p_1^{a_1} p_2 \dots p_t, p_1^{a_1} p_2^2 p_3 \dots p_t) \cup \\
& \cup (2 \cdot p_1^{a_1} p_2 \dots p_t, p_1^{a_1} p_2^2 p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot p_1^{a_1} p_2 \dots p_t, p_1^{a_1} p_2^2 p_3 \dots p_t)) \cup \\
& \cup ((1 \cdot p_1^{a_1} p_2^2 p_3 \dots p_t, p_1^{a_1} p_2^3 p_3 \dots p_t) \cup \\
& \cup (2 \cdot p_1^{a_1} p_2^2 p_3 \dots p_t, p_1^{a_1} p_2^3 p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot p_1^{a_1} p_2^2 p_3 \dots p_t, p_1^{a_1} p_2^3 p_3 \dots p_t)) \cup \\
& \dots \dots \dots \cup ((1 \cdot p_1^{a_1} p_2^{a_2-1} p_3 \dots p_t, p_1^{a_1} p_2^{a_2} p_3 \dots p_t) \cup \\
& \cup (2 \cdot p_1^{a_1} p_2^{a_2-1} p_3 \dots p_t, p_1^{a_1} p_2^{a_2} p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot p_1^{a_1} p_2^{a_2-1} p_3 \dots p_t, p_1^{a_1} p_2^{a_2} p_3 \dots p_t)) \cup \\
& \dots \dots \dots
\end{aligned}$$

$$\begin{aligned}
& \cup((1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup(2 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup((1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup(2 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \dots \dots \dots \cup((1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup(2 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup((2a_1, 2p_1p_2) \cup (2a_2, 2p_2p_3) \dots \cup (2a_{t-1}, 2p_{t-1}p_t) \cup (2a_t, 2p_tp_1)),
\end{aligned}$$

где при $1 \leq i \leq t-1$ имеем

$$1 \leq a_i \leq p_i p_{i+1}, \quad a_i \equiv 0 \pmod{p_i}, \quad a_i \equiv -1 \pmod{p_{i+1}}$$

и при $i = t$ имеем

$$1 \leq a_t \leq p_1 p_t, \quad a_t \equiv 0 \pmod{p_t}, \quad a_t \equiv -1 \pmod{p_1}.$$

Здесь серия

$$\begin{aligned}
& ((1, p_1) \cup (2, p_1) \cup \dots \cup (p_1 - 3, p_1) \cup (p_1 - 1, p_1)) \cup \\
& ((1, p_2) \cup (2, p_2) \cup \dots \cup (p_2 - 3, p_2) \cup (p_2 - 1, p_2)) \cup \\
& \cup \dots \cup ((1, p_t) \cup (2, p_t) \cup \dots \cup (p_t - 3, p_t) \cup (p_t - 1, p_t))
\end{aligned}$$

накрывает все числа, не сравнимые с 0 и -2 по модулям $p_1, \dots, p_t$. Серия

$$\begin{aligned}
& ((1 \cdot p_1 p_2 \dots p_t - 2, p_1^2 p_2 \dots p_t) \cup (2 \cdot p_1 p_2 \dots p_t - 2, p_1^2 p_2 \dots p_t) \cup \\
& \cup \dots \cup ((p_1 - 1) \cdot p_1 p_2 \dots p_t - 2, p_1^2 p_2 \dots p_t)) \cup \\
& \cup((1 \cdot p_1^2 p_2 \dots p_t - 2, p_1^3 p_2 \dots p_t) \cup (2 \cdot p_1^2 p_2 \dots p_t - 2, p_1^3 p_2 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot p_1^2 p_2 \dots p_t - 2, p_1^3 p_2 \dots p_t)) \cup \\
& \dots \dots \dots
\end{aligned}$$

накрывает все числа, сравнимые с -2 по модулям $p_1, \dots, p_t$, но не сравнимые с -2 по модулю $p_1^{a_1} \dots p_t^{a_t}$. Серия

$$((1 \cdot p_1 p_2 \dots p_t, p_1^2 p_2 \dots p_t) \cup (2 \cdot p_1 p_2 \dots p_t, p_1^2 p_2 \dots p_t) \cup$$

$$\begin{aligned}
& \cup \dots \cup ((p_1 - 1) \cdot p_1 p_2 \dots p_t, p_1^2 p_2 \dots p_t)) \cup \\
& \cup ((1 \cdot p_1^2 p_2 \dots p_t, p_1^3 p_2 \dots p_t) \cup (2 \cdot p_1^2 p_2 \dots p_t, p_1^3 p_2 \dots p_t) \cup \\
& \cup \dots \cup ((p_1 - 1) \cdot p_1^2 p_2 \dots p_t, p_1^3 p_2 \dots p_t)) \cup \\
& \dots \dots \dots \\
& \cup ((1 \cdot p_1^{a_1-1} p_2 \dots p_t, p_1^{a_1} p_2 \dots p_t) \cup \\
& \cup (2 \cdot p_1^{a_2-1} p_2 \dots p_t, p_1^{a_1} p_2 \dots p_t) \cup \\
& \cup \dots \cup ((p_1 - 1) \cdot p_1^{a_1-1} p_2 \dots p_t, p_1^{a_1} p_2 \dots p_t)) \cup \\
& \cup ((1 \cdot p_1^{a_1} p_2 \dots p_t, p_1^{a_1} p_2^2 p_3 \dots p_t) \cup \\
& \cup (2 \cdot p_1^{a_1} p_2 \dots p_t, p_1^{a_1} p_2^2 p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot p_1^{a_1} p_2 \dots p_t, p_1^{a_1} p_2^2 p_3 \dots p_t)) \cup \\
& \cup ((1 \cdot p_1^{a_1} p_2^2 p_3 \dots p_t, p_1^{a_1} p_2^3 p_3 \dots p_t) \cup \\
& \cup (2 \cdot p_1^{a_1} p_2^2 p_3 \dots p_t, p_1^{a_1} p_2^3 p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot p_1^{a_1} p_2^2 p_3 \dots p_t, p_1^{a_1} p_2^3 p_3 \dots p_t)) \cup \\
& \dots \dots \dots \\
& \cup ((1 \cdot p_1^{a_1} p_2^{a_2-1} p_3 \dots p_t, p_1^{a_1} p_2^{a_2} p_3 \dots p_t) \cup \\
& \cup (2 \cdot p_1^{a_1} p_2^{a_2-1} p_3 \dots p_t, p_1^{a_1} p_2^{a_2} p_3 \dots p_t) \cup \\
& \cup \dots \cup ((p_2 - 1) \cdot p_1^{a_1} p_2^{a_2-1} p_3 \dots p_t, p_1^{a_1} p_2^{a_2} p_3 \dots p_t)) \cup \\
& \dots \dots \dots \\
& \cup ((1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}-1} p_t, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup (2 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}-1} p_t, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}-1} p_t, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2)) \cup \\
& \cup ((1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}-1} p_t^2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup (2 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}-1} p_t^2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^3) \cup \\
& \cup \dots \cup ((p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}-1} p_t^2, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^3)) \cup \\
& \dots \dots \dots \\
& \cup ((1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}-1} p_t^{a_t-1}, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup \\
& \cup (2 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}-1} p_t^{a_t-1}, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}) \cup
\end{aligned}$$

$$\cup \dots \cup ((p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t}))$$

накрывает все числа, сравнимые с 0 по модулям $p_1, \dots, p_t$, но не сравнимые с 0 по модулю $p_1^{a_1} \dots p_t^{a_t}$. Наконец, серия

$$(2a_1, 2p_1p_2) \cup (2a_2, 2p_2p_3) \dots \cup (2a_{t-1}, 2p_{t-1}p_t) \cup (2a_t, 2p_tp_1)$$

накрывает все числа, сравнимые с 0 или -2 по модулям $p_1, \dots, p_t$, но не сравнимые с 0 или -2 по модулю $p_1 \dots p_t$. Поэтому

$$\begin{aligned} L(n) &\leq \sum_{i=1}^t (p_i - 2) + 2 \sum_{i=1}^t (a_i - 1)(p_i - 1) + t = \\ &= (2a_1 - 1)(p_1 - 1) + \dots + (2a_t - 1)(p_t - 1). \end{aligned}$$

Для доказательства нижней оценки введем обозначения

$$\begin{aligned} X_1^{1,1} &:= \{1 \cdot p_1 p_2^{a_2} \dots p_t^{a_t} - 2, \dots, (p_1 - 1) \cdot p_1 p_2^{a_2} \dots p_t^{a_t} - 2\}, \\ X_1^{1,2} &:= \{1 \cdot p_1^2 p_2^{a_2} \dots p_t^{a_t} - 2, \dots, (p_1 - 1) \cdot p_1^2 p_2^{a_2} \dots p_t^{a_t} - 2\}, \\ &\dots \dots \dots \\ X_1^{1,a_1-1} &:= \{1 \cdot p_1^{a_1-1} p_2^{a_2} \dots p_t^{a_t} - 2, \dots, (p_1 - 1) \cdot p_1^{a_1-1} p_2^{a_2} \dots p_t^{a_t} - 2\}, \\ &\dots \dots \dots \\ X_1^{t,1} &:= \{1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t - 2, \dots, (p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t - 2\}, \\ X_1^{t,2} &:= \{1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2, \dots, (p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2 - 2\}, \\ &\dots \dots \dots \\ X_1^{t,a_t-1} &:= \{1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2, \dots, (p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1} - 2\}, \\ X_2^{1,1} &:= \{1 \cdot p_1 p_2^{a_2} \dots p_t^{a_t}, \dots, (p_1 - 1) \cdot p_1 p_2^{a_2} \dots p_t^{a_t}\}, \\ X_2^{1,2} &:= \{1 \cdot p_1^2 p_2^{a_2} \dots p_t^{a_t}, \dots, (p_1 - 1) \cdot p_1^2 p_2^{a_2} \dots p_t^{a_t}\}, \\ &\dots \dots \dots \\ X_2^{1,a_1-1} &:= \{1 \cdot p_1^{a_1-1} p_2^{a_2} \dots p_t^{a_t}, \dots, (p_1 - 1) \cdot p_1^{a_1-1} p_2^{a_2} \dots p_t^{a_t}\}, \\ &\dots \dots \dots \\ X_2^{t,1} &:= \{1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t, \dots, (p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t\}, \\ X_2^{t,2} &:= \{1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2, \dots, (p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^2\}, \end{aligned}$$

$$\begin{aligned}
& \dots\dots\dots \\
X_2^{t,a_t-1} &:= \{1 \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}, \dots, (p_t - 1) \cdot p_1^{a_1} \dots p_{t-1}^{a_{t-1}} p_t^{a_t-1}\}, \\
X_3^1 &:= \{b_{1,1}, \dots, b_{1,p_1-2}\}, \\
& \dots\dots\dots \\
X_3^t &:= \{b_{t,1}, \dots, b_{t,p_t-2}\}, \\
X_4 &:= \{c_1, \dots, c_t\}, \\
Y &:= (p_1^{a_1} \dots p_t^{a_t} - 2, p_1^{a_1} \dots p_t^{a_t}) \cup (p_1^{a_1} \dots p_t^{a_t}, p_1^{a_1} \dots p_t^{a_t}),
\end{aligned}$$

где

$$\begin{aligned}
b_{i,j} &\equiv j \pmod{p_i^{a_i}}, \quad b_{i,j} \equiv 0 \pmod{\frac{n}{p_i^{a_i}}}, \\
c_i &\equiv -1 \pmod{p_i^{a_i}}, \quad c_i \equiv 0 \pmod{\frac{n}{p_i^{a_i}}}.
\end{aligned}$$

Покажем, что множество

$$X := X_1^{1,1} \cup \dots \cup X_1^{t,a_t-1} \cup X_2^{1,1} \cup \dots \cup X_2^{t,a_t-1} \cup X_3^1 \cup \dots \cup X_3^t \cup X_4$$

будет опорным семейством для множества Y . Пусть $x_1, x_2 \in X$, $x_1 < x_2$. Нужно доказать, что выполнено хотя бы одно из двух условий:

$$(x_1, x_2 - x_1) \cap (n - 2, n) \neq \emptyset, \quad (13)$$

$$(x_1, x_2 - x_1) \cap (n, n) \neq \emptyset. \quad (14)$$

Возможны случаи:

Случай 1.

$x_1 \in X_1^{i,j_1}, x_2 \in X_1^{i,j_2}, j_1 \leq j_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_1}$ и по лемме 1 верно (13).

Случай 2.

$x_1 \in X_1^{i,j_1}, x_2 \in X_1^{i,j_2}, j_1 > j_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_2}$ и по лемме 1 верно (13).

Случай 3.

$x_1 \in X_1^{i_1,j_1}, x_2 \in X_1^{i_2,j_2}, i_1 \neq i_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_{i_1}^{a_{i_1}} p_{i_2}^{a_{i_2}}} p_{i_1}^{j_1} p_{i_2}^{j_2}$ и

по лемме 1 верно (13).

Случай 4.

$x_1 \in X_1^{i_1,j_1}, x_2 \in X_2^{i_2,j_2}$. Тогда $\text{НОД}(x_2 - x_1, n) = 1$ и по лемме 1 получаем, что верно (13).

Случай 5.

$x_1 \in X_1^{i,j}, x_2 \in X_3^k$ или $x_2 \in X_1^{i,j}, x_1 \in X_3^k$. Случай аналогичен случаю 4.

Случай 6.

$x_1 \in X_1^{i,j}, x_2 = c_i$ или $x_2 \in X_1^{i,j}, x_1 = c_i$. Тогда $\text{НОД}(x_2 - x_1, n) = p_i^j$ и по лемме 1 верно (13).

Случай 7.

$x_1 \in X_1^{i,j}, x_2 = c_k, k \neq i$ или $x_2 \in X_1^{i,j}, x_1 = c_k, k \neq i$. Тогда верно, что $\text{НОД}(x_2 - x_1, n) = p_i^{a_i}$ и по лемме 1 получаем (13).

Случай 8.

$x_1 \in X_2^{i,j_1}, x_2 \in X_2^{i,j_2}, j_1 \leq j_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_1}$ и по лемме 1 верно (14).

Случай 9.

$x_1 \in X_2^{i,j_1}, x_2 \in X_2^{i,j_2}, j_1 > j_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i}} p_i^{j_2}$ и по лемме 1 верно (14).

Случай 10.

$x_1 \in X_2^{i_1,j_1}, x_2 \in X_2^{i_2,j_2}, i_1 \neq i_2$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_{i_1}^{a_{i_1}} p_{i_2}^{a_{i_2}}} p_{i_1}^{j_1} p_{i_2}^{j_2}$ и по лемме 1 верно (14).

Случай 11.

$x_1 \in X_2^{i,j}, x_2 \in X_3^i$ или $x_2 \in X_1^{i,j}, x_1 \in X_3^i$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i}}$ и по лемме 1 верно (14).

Случай 12.

$x_1 \in X_2^{i,j}, x_2 \in X_3^k, i \neq k$ или $x_2 \in X_2^{i,j}, x_1 \in X_3^k, i \neq k$. Тогда верно, что $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i} p_k^{a_k}} p_i^j$ и по лемме 1 получаем (14).

Случай 13.

$x_1 \in X_2^{i,j}, x_2 = c_i$ или $x_2 \in X_2^{i,j}, x_1 = c_i$. Случай аналогичен случаю 11.

Случай 14.

$x_1 \in X_2^{i,j}, x_2 = c_k, k \neq i$ или $x_2 \in X_2^{i,j}, x_1 = c_k, k \neq i$. Случай аналогичен случаю 12.

Случай 15.

$x_1 \in X_3^i, x_2 \in X_3^i$. Случай аналогичен случаю 11.

Случай 16.

$x_1 \in X_3^i, x_2 \in X_3^j, i \neq j$. Тогда $\text{НОД}(x_2 - x_1, n) = \frac{n}{p_i^{a_i} p_j^{a_j}}$ и по лемме 1 верно (14).

Случай 17.

$x_1 \in X_3^i, x_2 = c_i$ или $x_1 \in X_3^i, x_2 = c_i$. Случай аналогичен случаю 11.

Случай 18.

$x_1 \in X_3^i, x_2 = c_j, i \neq j$ или $x_2 \in X_3^i, x_1 = c_j, i \neq j$. Случай аналогичен случаю 16.

Случай 19.

$x_1 = c_i, x_2 = c_j$. Случай аналогичен случаю 16.

Разбор случаев завершен. Мы показали, что множество X будет опорным семейством для Y . Но в множестве X всего

$$\begin{aligned} & |X_1^{1,1}| + \dots + |X_1^{t,a_t-1}| + |X_2^{1,1}| + \dots + |X_2^{t,a_t-1}| + |X_3^1| + \dots + |X_3^t| + |X_4| = \\ & = 2(p_1 - 1)(a_1 - 1) + \dots + 2(p_t - 1)(a_t - 1) + (p_1 - 2) + \dots + (p_t - 2) + t = \\ & = (2a_1 - 1)(p_1 - 1) + \dots + (2a_t - 1)(p_t - 1) \end{aligned}$$

элементов. Поэтому по лемме 2 получаем

$$L(p_1^{a_1} \dots p_t^{a_t}) \geq (2a_1 - 1)(p_1 - 1) + \dots + (2a_t - 1)(p_t - 1).$$

В случае, когда $p_1 > 2, t > 1$, утверждение теоремы доказано. ■

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

- [6] Д. Н. Бабин. *Частотные регулярные языки*. Интеллектуальные системы, 2014. Т.18, вып. 1, М., Сс. 205-210.
- [7] Д. Е. Александров. *Об оценках автоматной сложности распознавания классов регулярных языков*. Интеллектуальные системы, 2014. Т.18, вып. 4, М., Сс. 161-190.
- [8] В. М. Дементьев. *О звездной высоте регулярного языка и циклической сложности минимального автомата*. Интеллектуальные системы, 2014. Т.18, вып. 4, М., Сс. 215-222.
- [9] 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.
- [10] А. А. Петюшко. *О контекстно-свободных биграмных языках*. Интеллектуальные системы, 2015. Т.19, вып. 2, М., Сс. 187-208.
- [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.
- [12] В. А. Орлов. *О конечных автоматах с максимальной степенью различимости состояний*. Интеллектуальные системы, 2016. Т.20, вып. 1, М., Сс. 213-222.
- [13] 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.
- [14] А. М. Миронов. *Основные понятия теории вероятностных автоматов*. Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 283-330.
- [15] А. А. Петюшко, Д. Н. Бабин. *Классификация Хомского для матриц биграммных языков*. Интеллектуальные системы, 2016. Т.20, вып. 2, М., Сс. 331-336.
- [16] 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.