DOI: 10.24888/2500-1957-2020-4-94-110

УДК 511.1

# ПОДХОД К ПОИСКУ ПРОСТЫХ ЧИСЕЛ СРЕДИ ЧЛЕНОВ ПОСЛЕДОВАТЕЛЬНОСТИ НАТУРАЛЬНОГО РЯДА СПЕЦИАЛЬНОГО ВИДА

**Дмитрий Вадимович Поляков**
к.т.н.
dimadress@mail.ru
г. Тамбов
**Андрей Иванович Попов**
к.п.н., доцент
olimp_popov@mail.ru
г. Тамбов
**Анастасия Николаевна Толмачева**
a.tolma4yova@yandex.ru
г. Тамбов

Тамбовский государственный технический университет

**Аннотация.** В статье рассматривается проблема поиска простых чисел из заданного диапазона и факторизации больших чисел. Актуальность исследования обусловлена распространением ассиметричных криптографических алгоритмов в качестве методов обеспечения безопасного сеанса в глобальной сети, что обуславливает потребность дополнительных исследований, уточняющих свойства ряда простых чисел. Механизмы поиска простых чисел востребованы криптологией как для повышения безопасности работы глобальной сети, так и для разработки новых методов атак на ассиметричные криптографические системы шифрования. В работе рассматривается последовательность чисел, для которой ряд простых чисел является подпоследовательностью. Для построения этой последовательности предлагается разбить ряд натуральных чисел на полуинтервалы, границами которых являются произведения некоторого количества первых простых чисел. Показано, что на каждом таком полуинтервале имеет место множество специального вида, которому, в том числе, принадлежат простые числа, попадающие в соответствующий полуинтервал. Это множеств представляет интерес, так как его плотность ниже плотности натурального ряда. Это означает потенциальную возможность построения данного множества алгоритмом с относительно низкой асимптотической сложностью. В работе приводится и доказывается ряд утверждений и следствий из них, проливающих свет на свойства последовательности, полученной из объединения множеств специального вида. Показано на языке теории множеств возможного итеративного построения исследуемой последовательности, а также то, что для неё ряд простых чисел является подпоследовательностью. Полученные теоретические результаты позволяют спроектировать алгоритм поиска простых чисел в заданном диапазоне, а также создают задел на построение быстрых алгоритмов факторизации больших чисел.

**Ключевые слова:** простые числа, арифметика, поиск простых чисел, построение ряда простых чисел.

## Теоретический анализ проблемы

В настоящее время, простые числа и закон их распределения вызывают все больший интерес. С одной стороны, несмотря на то что, исследования ряда простых чисел берут своё начало в античности, сегодня всё ещё существует несколько неразрешённых проблем, таких как, например, проблема Гольдбаха [11], гипотеза Лежандра [7], вторая и четвёртая проблемы Ландау [3]. Кроме того, развитие математики, а именно исследование алгебраических групп привело к появлению понятия «простого элемента» [5] в коммутативных полугруппах и «простого идеала» [5] в коммутативных кольцах. Оба эти понятия являются обобщением простого числа, и исследование их свойств осложняется тем, что даже при рассмотрении простых чисел в арифметике остаются не до конца исследованные вопросы.

С другой стороны, исследование ряда простых чисел стало приобретать все большее практическое значение. Данные числа легли в основу криптографических механизмов защиты информации, таких, например, как асимметричный алгоритм шифрования *RSA* [6]. Безопасность информации, защищённой такими криптографическими алгоритмами, основывается на сложности факторизации больших целых чисел. С этой проблемой связаны две задачи: поиск всех простых чисел в интервале от 2 до $n$, где $n$ – некоторое заданное число и проверка является ли данное число простым. Для ответа на последний вопрос часто используются тесты на простоту. Эти алгоритмы позволяют детерминировано или с некоторой вероятностью определить является ли то или иное число простым. Примером таких тестов могут послужить тесты Миллера [10], Штрассена [12], Люка [2], *BPSW* [8], *ECPP* [9], *AKS* [1].

Задача факторизации простых чисел, получила множество подходов к решению: это и классическое решето Эратосфена, и методы Полларда, Бента, Монте-Карло, Ферма [2] и другие.

Вместе с тем вопрос построения ряда простых чисел остаётся открытым и исследования в этой области продолжаются. А с распространением ассиметричных криптографических алгоритмов, как методов обеспечения безопасного сеанса в глобальной сети, любые результаты исследований, уточняющие свойства ряда простых чисел, могут быть особенно важны. Заметим, что исследования простых чисел востребованы криптологией как для повышения безопасности работы глобальной сети, так и для разработки новых методов атак на ассиметричные криптографические системы шифрования.

## Методы и организация исследования

При создании данной работы были использованы математические аппараты теории чисел и теории множеств, а также теория алгоритмизации.

В данной работе предлагается последовательность чисел, для которой ряд простых чисел является подпоследовательностью. Для построения данной последовательности введём в рассмотрение подмножества простых чисел специального вида. Пусть $P_k$ – множество $k$ первых простых чисел: $P_k = \{p_1, p_2, \dots, p_k\}$. Будем считать для определенности и без ограничения общности, что $p_i < p_j$ для $\forall i < j | i, j = \overline{1,k}$. То есть $p_i$–$i$-ое простое число, $\forall i = \overline{1,k}$. Обозначим $P_\infty$ – множество всех простых чисел. Тогда верно, что $P_\infty = \lim\limits_{k\to\infty} P_k$, а также $P_k \subset P_{k+1} = P_k \cup \{p_k\}$ и $P_k \subset P_\infty, \forall k \in N$.

Для разрешения проблемы поиска простых чисел из заданного диапазона приводится и доказывается ряд утверждений, позволяющих построить и проанализировать последовательность, которая содержит в себе множество простых чисел. Авторами исследованы свойства построенной последовательности.

## Результаты и их обсуждение

Возьмём и зафиксируем произвольное число $k \in N$. Произведение $k$ первых простых чисел будем обозначать $M_k$, то есть $M_k = \prod_{p\in P_k} p$. Отметим также, что из обозначения и

определения $P_k$, следует, что $M_{k+1} = M_k p_{k+1}, \forall k \in N$. В таблице 1 представлены примеры $M_k$ для нескольких значений $k$.

*Таблица 1.*
*Соответствие между k и $M_k$.*

| $\boldsymbol{k}$ | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|
| $\boldsymbol{M_k}$ | 2 | 6 | 30 | 210 | 2310 | 30030 |

Рассмотрим отображение $n: N \to N$, такое, что $(\forall k \in N)((\forall p^* \in P_{n(k)})(p^* < M_k) \wedge (\forall \hat{p} \in P_\infty \backslash P_{n(k)})(\hat{p} > M_k))$. Другими словами, $P_{n(k)}$ – множество простых чисел, меньших $M_k$. Заметим, что определение корректно, хотя в нем не учитывается случай, когда некоторое простое число равно $M_k$, так как для $k > 1$ это невозможно в силу способа задания $M_k$, как произведения $k$ первых простых чисел.

Отметим, что, по сути, $n(k)$ представляет собой номер максимального простого числа меньшего $M_k$, то есть $p_{n(k)} < M_k < p_{n(k)+1}$, или $n(k)$ можно определить как число простых чисел меньших $M_k$. Это также означает, что $n(k) = \left|P_{n(k)}\right|$, где $|\ |$ – мощность множества.

Отдельно следует сказать о случае, когда $k = 1$, при таком $k$ удобно считать $M_1 = 2$, то есть первому простому числу. Тогда очевидно, что согласно определению рассматриваемого отображения $n(1) = 0$, так как простые числа меньше 2 – отсутствуют.

И хотя для $n$ аналитическое выражение неизвестно, легко ограничить значение $n(k)$ сверху. Действительно, если разбить $P_{n(k)}$ на два множества: $P_k = \{p_1, p_2, \dots, p_k\}$ и $P_{n(k)} \backslash P_k = \{p_{k+1}, p_{k+2}, \dots, p_{n(k)}\}$, томожно заметить, что все элементы $P_{n(k)} \backslash P_k$ взаимно просты с $M_k$, а элементы $P_k$, напротив, являются делителями $M_k$. Тогда, обозначив $\Xi_k$ – множество чисел взаимно простых с $M_k$, с одной стороны получим, что $P_{n(k)} \backslash P_k \subset \Xi_k$ и значит $\left|P_{n(k)} \backslash P_k\right| \leq |\Xi_k| = \phi(M_k)$, где $\phi(\cdot)$ – функция Эйлера [4], а с другой, так как $P_k \subset P_{n(k)}$, то$\left|P_{n(k)} \backslash P_k\right| = \left|P_{n(k)}\right| - |P_k| = n(k) - k$. Таким образом, имеем неравенство:

$$n(k) - k \leq \phi(M_k)$$

или

$$n(k) \leq \phi(M_k) + k$$

или, согласно аналитическому виду функции Эйлера [12] и виду $M_k$:

$$n(k) \leq \prod_{i=1}^{k} (p_i - 1) + k \qquad (1)$$

То, что (1) выполняется для рассмотренных выше примеров продемонстрировано в Таблице 2.

Из таблицы 2 видно, что, по крайней мере, на начальном этапе $n(k)$ несильно отличается от $\phi(M_k) + k$. Это означает, что в множестве взаимно простых с $M_k$ и не превосходящих его чисел, хотя бы при малых $k$ велика доля элементов множества $P_{n(k)} \backslash P_k$.

Введём в рассмотрение два семейства множества. Множества первого семейства$(U_k)$ построим для каждого натурального числа$k$ как $U_k = \left\{p_{k+1}^{a_1} \cdot p_{k+2}^{a_2} \cdot \ldots \cdot p_{n(k)}^{a_{n(k)-k}} | a_i \in N \cup \{0\}, \forall i = \overline{1, n(k) - k}\right\}$. Второе семейство множеств определим через первое: $G_k = \{g \in U_k |\ \ g < M_k\}, \forall k \in N$.

Стоит провести одно немаловажное наблюдение, а именно, что для $\forall k \in N \backslash \{1\}$ минимальный элемент $G_k$ – единица. Действительно, при $a_i = 0, \forall i = \overline{1, n(k) - k}$ произведение $p_{k+1}^{a_1} \cdot p_{k+2}^{a_2} \cdot \ldots \cdot p_{n(k)}^{a_{n(k)-k}} = p_{k+1}^0 \cdot p_{k+2}^0 \cdot \ldots \cdot p_{n(k)}^0 = 1$, кроме того $1 < M_k, \forall k \geq 1$, а, следовательно, $1 \in G_k$.

*Таблица 2.*
*Соответствие между* $k$, $M_k$, $n(k)$ *и* $\phi(M_k)+k$.

| $k$ | $M_k$ | $n(k)$ | $\phi(M_k)+k$ | $P_k$ |
|---|---|---|---|---|
| 1 | 2 | 0 | 2 | {2} |
| 2 | 6 | 3 | 4 | {2, 3} |
| 3 | 30 | 10 | 11 | {2, 3, 5} |
| 4 | 210 | 46 | 52 | {2, 3, 5, 7} |
| 5 | 2310 | 343 | 485 | {2, 3, 5, 7, 11} |
| 6 | 30030 | 3248 | 5766 | {2, 3, 5, 7, 11, 13} |

**Теорема.** $(\forall \boldsymbol{k} \in \boldsymbol{N}\backslash\{\boldsymbol{1}\})(\forall \boldsymbol{p} \in \boldsymbol{P_\infty}, \boldsymbol{p} > \boldsymbol{M_k})(\exists \boldsymbol{l} \in \boldsymbol{N}, \boldsymbol{r} \in \boldsymbol{G_k} | \boldsymbol{p} = \boldsymbol{l} \cdot \boldsymbol{M_k} + \boldsymbol{r})$

*Доказательство*. Возьмем и зафиксируем некоторое $k \in N\backslash\{1\}$. Рассмотрим произвольное число $p \in P_\infty, p > M_k$. Известно [4], что $\exists l \in N, r \in N \cup \{0\}, 0 \le r \le M_k$, такие что $p = l \cdot M_k + r$. Осталось показать, что $r \in G_k$.

Во-первых, покажем, что $r \neq 0$. Действительно, если предложить, что $r = 0$, то это будет означать, что$p$ кратно $M_k$, а так как $M_k$, при выбранном $k$, число составное по определению, то данное предположение вступает в противоречие с простотой $p$.

Во-вторых, заметим, что если $\hat{p}$ – некоторое простое число и $r$ кратно $\hat{p}$, то $\hat{p} \in P_{n(k)}$. Действительно, с одной стороны, $r < M_k$ по построению, а с другой из кратности остатка $r$ простому числу $\hat{p}$ следует что $\hat{p} \le r < M_k$, а $P_{n(k)}$ по определению отображения $n$ и есть множество простых чисел меньших $M_k$.

Тогда согласно основной теореме арифметики [12] представим $r$ в виде:

$$r = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} \cdot p_{k+1}^{\beta_{k+1}} \cdot \ldots \cdot p_{n(k)-1}^{\beta_{n(k)-1}} \cdot p_{n(k)}^{\beta_{n(k)}}, \beta_i \in N \cup \{0\}, i = \overline{1, n(k)} \quad (2)$$

Покажем теперь, что $(\forall i = \overline{1,k})(\beta_i = 0)$. Предположим противное, а именно, что $(\exists i = \overline{1,k})(\beta_i \neq 0)$. Тогда $r$ будет кратно $p_i$, но и $M_k$ кратно $p_i$ по определению. Следовательно, $(l \cdot M_k + r)$ кратно $p_i$ или $p$ кратно $p_i$. Но так как $p$ и $p_i$ простые числа, то из их кратности следует, что $p = p_i$. Вместе с тем $p_i < M_k$ по определению $M_k$ для $\forall k > 1$, а $p > M_k$ по условию теоремы. Получили противоречие. Следовательно, наше предположение неверно. То есть $\beta_i = 0$ или $p_i^{\beta_i} = 1, \forall i = \overline{1,k}$.

Переобозначим степени в (2), заменив $\beta_{k+j}, j = \overline{1, n(k)-k}$ на $a_j$. Члены произведения (2) со степенями $\beta_i, i = \overline{1,k}$ равны 1 и могут быть опущены. Тогда выражение (2) принимает вид:

$$r = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \ldots \cdot p_{n(k)}^{\alpha_{n(k)-k}}, a_j \in N \cup \{0\}, j = \overline{1, n(k)-k} \quad (3)$$

Выражение (3) и ранее показанное неравенство $r < M_k$ однозначно доказывают то, что $r \in G_k$ по определению этого множества.

Утверждение теоремы, сформулированное на языке «эпсилон-дельта», можно перефразировать следующим образом: для любого $M_k, k > 1$, остаток от деления любого большего $M_k$ простого числа на $M_k$ принадлежит $G_k$.

**Следствие.** Пусть $p \in P_\infty, M_k < p < M_{k+1}$. Тогда $\exists l = \overline{1, p_{k+1}-1}$ и $r \in G_k$, такие, что $p = l \cdot M_k + r$.

*Доказательство*. Согласно теореме из условия данного следствия непосредственно следует, что $\exists l \in N$ и $r \in G_k$ такие, что $p = l \cdot M_k + r$. Осталось показать, что $l < p_{k+1}$. Предположим противное: $l \ge p_{k+1}$. Тогда $p = l \cdot M_k + r > l \cdot M_k \ge p_{k+1} \cdot M_k = M_{k+1}$ или $p > M_{k+1}$, что противоречит условию следствия. Наше предположение неверно. Следствие доказано.

Это следствие крайне важно для данной работы. По сути, в статье предлагается разбить ряд натуральных чисел, больших 6 на полуинтервалы вида: $[M_2, M_3), [M_3, M_4), [M_4, M_5), \ldots$

после чего построить на каждом полуинтервале $[M_k, M_{k+1}), k \in N, k > 2$ элементы вида $l \cdot M_k + r, l = \overline{1, p_{k+1} - 1}, r \in G_k$ и искать среди этих элементов простые числа.

Оценим мощность множества $G_k$ для произвольного числа $k \in N \backslash \{1\}$. Для этого докажем следующее утверждение.

**Утверждение 1**. $|G_k| = \prod_{i=1}^{k}(p_i - 1)$

*Доказательство*. Для доказательства данного утверждения покажем, что $G_k$ является множеством чисел, взаимно простых с $M_k$ в диапазоне от 1 до $M_k$.

1) Пусть $m$ – взаимно простое число с$M_k$и $m < M_k$, тогда, в силу основной теоремы арифметики [12] и того факта, что все простые делители $m$меньше $M_k$, верно равенство:

$$m = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_k^{\beta_k} \cdot p_{k+1}^{\beta_{k+1}} \cdot \ldots \cdot p_{n(k)-1}^{\beta_{n(k)-1}} \cdot p_{n(k)}^{\beta_{n(k)}}, \beta_i \in N \cup \{0\}, i = \overline{1, n(k)}$$

Теперь докажем, что $(\forall i = \overline{1, k})(\beta_i = 0)$. Для этого предположим противное:$(\exists i = \overline{1, k})(\beta_i \neq 0)$. Тогда $m$кратно $p_i$, но и $M_k$ по определению кратно $p_i$. Другими словами $p_i$ – общий делитель $m$и $M_k$. Следовательно, НОД$(m, M_k) \geq p_i$, где НОД$(\cdot,\cdot)$– функция формализующая нахождение наибольшего общего делителя двух натуральных чисел. Полученное неравенство противоречит тому, что $m$и $M_k$– взаимно простые числа, для которых наибольший общий делитель равен 1по определению. Что и требовалось доказать. Из того что $(\forall i = \overline{1, k})(\beta_i = 0)$, следует, что $(\forall i = \overline{1, k})(p_i^{\beta_i} = 1)$, а значит $m = p_{k+1}^{\beta_{k+1}} \cdot \ldots \cdot p_{n(k)-1}^{\beta_{n(k)-1}} \cdot p_{n(k)}^{\beta_{n(k)}} \cdot$ Обозначим$\beta_{k+i} = \alpha_i, \forall i = \overline{1, n(k) - k}$и вспомним, что $m < M_k$. Получим:$m = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \ldots \cdot p_{n(k)}^{\alpha_{n(k)-k}}, a_i \in N \cup \{0\}, i = \overline{1, n(k) - k}, m < M_k$, то есть $m \in G_k$ по определению.

1) Пусть $m \in G_k$, тогда по определению $G_k$ имеем:

$$m = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \ldots \cdot p_{n(k)}^{\alpha_{n(k)-k}}$$

или

$$m = p_1^0 \cdot p_2^0 \cdot \ldots \cdot p_k^0 \cdot \ldots \cdot p_{k+1}^{\alpha_1} \cdot p_{k+1}^{\alpha_2} \cdot p_{k+1}^{\alpha_3} \cdot \ldots \cdot p_{n(k)}^{\alpha_{n(k)-k}} \quad (4)$$

При этом согласно обозначению:

$$M_k = p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

или

$$M_k = p_1 \cdot p_2 \cdot \ldots \cdot p_k \cdot p_{k+1}^0 \cdot p_{k+2}^0 \cdot \ldots \cdot p_{n(k)}^0 \quad (5)$$

На основе формулы вычисления НОД факторизованных чисел [4] и в силу (4) и (5) получаем:

$$\text{НОД}(m, M_k) = p_1^{\min(0,1)} \cdot p_2^{\min(0,1)} \cdot \ldots \cdot p_k^{\min(0,1)} \cdot p_{k+1}^{\min(\alpha_1,0)} \cdot p_{k+2}^{\min(\alpha_2,0)} \cdot \ldots \cdot p_{n(k)}^{\min(\alpha_{n(k)-k},0)} = p_1^0 \cdot p_2^0 \cdot \ldots \cdot p_k^0 \cdot p_{k+1}^0 \cdot p_{k+2}^0 \cdot \ldots \cdot p_{n(k)}^0 = 1,$$

что по определению означает взаимную простоту $m$ и $M_k$.

Итак, с одной стороны показано, что для произвольного числа $m < M_k$ если $m$ и $M_k$– взаимно простые числа, то $m \in G_k$, а с другой, что еслипроизвольное натуральное число $m \in G_k$, то $m$ и $M_k$ – взаимно простые числа. Из этих двух доказанных утверждений следует, что множества взаимно простых чисел с $M_k$ из диапазона от 1 до $M_k$ и $G_k$– совпадают.

Тогда $|G_k| = \phi(M_k)$, согласно определению. Тогда значение функции Эйлера в силу вида $M_k$ можно представить в виде [4]:

$$\varphi(M_k) = M_k(1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdot \ldots \cdot (1 - \frac{1}{p_k})$$

или

$$|G_k| = p_1 \cdot (1 - \frac{1}{p_1}) \cdot p_2 \cdot (1 - \frac{1}{p_2}) \cdot \ldots \cdot p_k \cdot (1 - \frac{1}{p_k})$$

или

$$|G_k| = \prod_{i=1}^{k} (p_i - 1) \quad (6)$$

Что и требовалось доказать.

Обозначим $\prod_{i=1}^{k}(p_i - 1)$ через $M_k^*$.

Отметим, что вычисление мощности $M_k$, базировалось на доказательстве того, что $G_k$ ни что иное, как множество чисел меньших $M_k$ и взаимно простых с ним.

**Утверждение 2**. Пусть $\tilde{p} = l \cdot M_k + r, l = \overline{1, p_{k+1} - 1}, r \in G_k, r = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \ldots p_{n(k)}^{\alpha_{n(k)-k}}$. Тогда верно, что если $\alpha_i \neq 0$, то $\tilde{p}$ не кратно $p_{k+i}$ , $\forall i = \overline{1, n-k}$.

*Доказательство*. Предположим противное: $\exists i = \overline{1, n(k) - k} | \alpha_i \neq 0$ и $\tilde{p}$ кратно $p_{k+i}$. Из последнего условия в предположении следует, что $\exists t \in N$, такое, что $\tilde{p} = t p_{k+i}$ или

$$l \cdot M_k + r = t \cdot p_{k+i}$$

или

$$l \cdot M_k + p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_{n-k}} = t \cdot p_{k+i}$$

или

$$l \cdot M_k = t \cdot p_{k+i} - p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \ldots \cdot p_{n(k)}^{\alpha_{n(k)-k}} \quad (7)$$

Очевидно, что правая часть (7) кратна $p_{k+i}$ при $\alpha_i \neq 0$. В то время как левая часть (7) состоит из произведения чисел $l$ и $M_k$. Причём $l < p_{k+1} \leq p_{k+i}, \forall i = \overline{1, n(k) - k}$, следовательно, $l$ не кратно $p_{k+i}$. $M_k$ же представляет собой произведение простых чисел от $p_1$ до $p_k$ включительно и поэтому также не кратно $p_{k+i}$,$\forall i = \overline{1, n-k}$. Это означает, что и произведение $l \cdot M_k$ не кратно $p_{k+i}$.

Итак, было показано, что левая часть (7) не кратна $p_{k+i}$, в то время как правая – кратна. Получили противоречие. Следовательно, наше предположение неверно. Что и требовалось доказать.

Утверждение 2 не является ключевым для построения последовательности, среди элементов которой будем искать простые числа. Как, впрочем, и верхняя оценка $n(k)$, найденная ранее. Вместе с тем дополнительные знания о введённых в рассмотрение отображениях, множествах и последовательностях могут помочь при дальнейших исследованиях, в том числе при непосредственном проектировании алгоритма поиска простых чисел.

Вернёмся теперь к, заявленной ранее, неограниченно расширяющейся надпоследовательности ряда простых чисел. Для её построения введём в рассмотрение ещё одно семейство множеств. Возьмём и зафиксируем некоторое произвольное $k \in N \backslash \{1\}$, найдем число $M_k$ и построим множество $G_k = \{g_1^k, g_2^k, g_3^k, \ldots, g_{M_k^*}^k\}$. Без ограничения общности будем считать, что $g_i^k < g_j^k, \forall i, j | i < j$ и $i, j = \overline{1, M_k^*}$, где согласно утверждению 1 $M_k^* = \prod_{i=1}^{k}(p_i - 1)$. Построим множество $X_k = \{x_1^k, x_2^k, \ldots, x_{M_{k+1}^*}^k\}$, где

$$x_i^k = l \cdot M_k + g_j^k, i = \overline{1, M_{k+1}^*}, l = \overline{1, p_{k+1} - 1}, j = \overline{1, M_k^*}. \quad (8)$$

Корректность последнего индекса данного построения следует из того, что согласно принятым обозначениям $M_{k+1}^* = M_k^* \cdot (p_{k+1} - 1)$, поэтому $M_{k+1}^*$ или $|X_k|$ и есть число всех возможных $x_i^k$ при заданных ограничениях: $l = \overline{1, p_{k+1} - 1}$ и $j = \overline{1, M_k^*}$.

Кроме того, зададим последовательность индексирования в $X_k$ следующей формулой:

$$x_i^k = l_i^k \cdot M_k + g_{j_i^k}^k, \tag{9}$$

где

$$l_i^k = \left\lfloor \frac{i-1}{M_k^*} \right\rfloor + 1, \text{ а } M_k^* + 1, \tag{10}$$

причём $\lfloor \quad \rfloor$ – обозначает целую часть выражения, $mod$– остаток от деления, а $i$ изменяется в полуинтервале от 1 до $M_{k+1}^*$.

Выражения (9-10) сложны для восприятия, так как содержат довольно много индексов и обозначений. На самом деле, они призваны задать последовательность индексирования $X_k$ таким образом, чтобы элементы располагались по возрастанию. Ниже это будет доказано. Вместе с тем поясним, что данная индексация позволяет расположить элементы в следующем порядке:
$x_1^k = M_k + g_1^k$, $x_2^k = M_k + g_2^k$, $x_3^k = M_k + g_3^k$, …, $x_{M_k^*}^k = M_k + g_{M_k^*}^k$,$x_{M_k^*+1}^k = 2M_k + g_1^k$,$x_{M_k^*+2}^k = 2M_k + g_2^k$, $x_{M_k^*+3}^k = 2M_k + g_3^k$, …, $x_{2M_k^*}^k = 2M_k + g_{M_k^*}^k$, … , $x_{(i-1)M_k^*+1}^k = iM_k + g_1^k$, $x_{(i-1)M_k^*+2}^k = iM_k + g_2^k$, $x_{(i-1)M_k^*+3}^k = iM_k + g_3^k$, …,$x_{iM_k^*}^k = iM_k + g_{M_k^*}^k$,…,$x_{(p_{k+1}-2)M_k^*+1}^k = (p_{k+1} - 1)M_k + g_1^k$, $x_{(p_{k+1}-2)M_k^*+2}^k = (p_{k+1} - 1)M_k + g_2^k$, $x_{(p_{k+1}-2)M_k^*+3}^k = (p_{k+1} - 1)M_k + g_3^k$, …,$x_{(p_{k+1}-1)M_k^*}^k = (p_{k+1} - 1)M_k + g_{M_k^*}^k$.

То есть построение $X_k$ в соответствииспредложенной индексацией происходит по следующему алгоритму: берём $M_k$ и добавляем к нему последовательно каждый элемент $G_k$. Потом берём $2M_k$ и повторяем процесс, потом $3M_k$ и так далее до $(p_k\text{-}\,1)M_k$. С точки зрения программной реализации построение $X_k$ осуществляется элементарным алгоритмом с двумя вложенными циклами: внутренний по $G_k$, а внешний от 1 до $p_k$- 1.

Предложим алгоритм построения $X_k$ и назовём его алгоритм ***A***.

Алгоритм ***A***. Построение упорядоченного множества $X_k$.

**Шаг 1**. На входе имеем $G_k$, $M_k$ и $p_{k+1}$. Устанавливаем переменные $LM$ и *Counter* равными 0. Устанавливаем $X_k = \emptyset$.

**Шаг 2**. $LM$ присваиваем $LM + M_k$. Увеличиваем $Counter$ на единицу. Проходим по упорядоченному множеству $G_k$. Пусть $g$ – текущий элемент $G_k$ на каждой итерации цикла. На каждом шаге вычисляем $LM + g$ иполученное значение добавляем конец $X_k$.

**Шаг 3**. Если $Counter$ равен $p_{k+1} - 1$, то конец алгоритма, в противном случае переходим к **шагу 2**.

Значения $G_k$, $M_k$ и $p_{k+1}$ могут храниться в переменных целочисленного типа, коими являются также $LM$ и $Counter$. В качестве структуры данных для формализации $X_k$ подойдёт любая конструкция для хранения коллекции элементов с заданным порядком, например линейный список.

Так как $M_k$, добавляющееся к $LM$ на втором шаге, больше любого элемента множества $G_k$ по определению, а в последнем элементы располагаются по порядку, то элементы $X_k$ алгоритм также находит в порядке возрастания.

Докажем два утверждения о множестве $X_k$.

**Утверждение 3**. $(\forall i = \overline{1, M_{k+1}^*})(M_k < x_i^k < M_{k+1})$

*Доказательство*. Из (8) непосредственно следует, что $M_k < x_i^k$ для $\forall i = \overline{1, M_k^*}$. Осталось показать, что $M_{k+1} > x_i^k$ для $\forall i = \overline{1, M_{k+1}^*}$. Для этого достаточно доказать, что

максимальный элемент ($x_{max}()$) множества $X_k$ меньше $M_{k+1}$. В силу неотрицательности всех членов в равенстве (8) имеем:

$$x_{max} = (p_{k+1} - 1)M_k + g^k_{M^*_k} \quad (11)$$

Известно, что $g^k_{M^*_K} \in G_k$ и, следовательно, по условию, наложенному на элементы $G_k$ при его задании $g^k_{M^*_k} < M_k$, тогда, согласно (11), максимальный элемент $X_k$ правомерно оценить как:

$$x_{max} = p_{k+1}M_k - M_k + g^k_{M^*_k} = M_{k+1} - \left(M_k - g^k_{M^*_k}\right) < M_{k+1},$$

что и требовалось доказать.

Утверждение 3 доказывает, что все элементы $X_k, \forall k \in N, k > 2$ лежат в полуинтервале $[M_k, M_{k+1})$, для которого в следствии к теореме было показано, что простые числа из этого полуинтервала представимы как раз таки в том же виде, что и члены последовательности $X_k$.

Докажем теперь строго, что предложенная в (9-10) индексация членов $X_k$, нумерует их по возрастанию.

**Утверждение 4**. $\left(\forall i = \overline{1, M^*_{k+1} - 1}\right)\left(x^k_i < x^k_{i+1}\right)$

*Доказательство*. Возьмем и зафиксируем некоторое $i = \overline{1, M^*_{k+1} - 1}$. Согласно (9) $x_i$ и $x_{i+1}$ распишем в виде:

$$\begin{cases} x^k_i = l^k_i \cdot M_k + g^k_{j^k_i}, \\ x^k_{i+1} = l^k_{i+1} \cdot M_k + g^k_{j^k_{i+1}}; \end{cases}.$$

Рассмотрим два случая.

1) $l^k_i < l^k_{i+1}$. Известно, что $g^k_{j^k_j} < M_k$ по условию, наложенному на элементы множества $G_k$. Тогда

$$x^k_i = l^k_i \cdot M_k + g^k_{j^k_i} < l^k_i \cdot M_k + M_k = (l^k_i + 1) \cdot M_k \le l^k_{i+1} \cdot M_k < l^k_{i+1} \cdot M_k + g^k_{j^k_{i+1}} = x^k_{i+1}.$$

Собрав начало и конец данного неравенства, получим:

$$x^k_i < x^k_{i+1}.$$

2) $l^k_i = l^k_{i+1}$. Если $l^k_i = l^k_{i+1}$, то, согласно (10), $\left\lfloor \frac{i-1}{M^*_k} \right\rfloor = \left\lfloor \frac{i}{M^*_k} \right\rfloor$. Тогда на основе обозначений, принятых в (10) для $x_i$ и $x_{i+1}$, верно, что

$$\begin{cases} i - 1 = (l^k_i - 1)M^*_k + j^k_i - 1, \\ i = (l^k_{i+1} - 1)M^*_k + j^k_{i+1} - 1; \end{cases}.$$

Очевидно, что левая часть данных равенств отличается на 1. Таким образом, добавив 1 к левой и правой частям первого из рассматриваемых равенств, приравняем их правые части и заменим $l^k_{i+1}$ на равное, в рассматриваемом случае, ей $l^k_i$. В результате получим:

$$(l^k_l - 1)M^*_k + j^k_i = (l^k_l - 1)M^*_k + j^k_i - 1$$

или

$$j^k_{i+1} = j^k_j + 1$$

Тогда $x^k_i = l^k_i M_k + g^k_{j^k_i} < l^k_i M_k + g^k_{j^k_i + 1} = l^k_{i+1} M_k + g^k_{j^k_{i+1}} = x^k_{i+1}$, или $x^k_i < x^k_{i+1}$.

Заметим, что ситуации $l^k_i > l^k_{i+1}$. быть не может в силу (10). А в обоих оставшихся рассмотренных возможных случаях получим $x^k_i < x^k_{i+1}$. Что и требовалось доказать.

Упорядоченность множества $X_k$ является крайне важной, так как именно на основе этого множества будет осуществлено построение надпоследовательности простых чисел.

Для решения данной задачи разобьем множество натуральных чисел $N$на полуинтервалы $[M_k, M_{k+1}), k \in N\backslash\{1\}$. Построим для каждого такого полуинтервала множество$X_k$. Дополним полученное семейство множеством $X_1 = \{2,3,5\}$. Отметим, что из утверждения 3 следует, что $X_k \subset [M_k, M_{k+1}), \forall k \in N\backslash\{1\}$.

Рассмотрим множество $X = \bigcup_{k=1}^{\infty} X_k$. Докажем, что множество простых чисел является подмножеством $X$.

**Утверждение 5**. $P_\infty \subset X$.

*Доказательство*. Возьмем произвольный $p \in P_\infty$ и покажем, что $p \in X$. Это и будет означать истинность утверждения по определению подмножества. Если $p \in \{2,3,5\}$, то $p \in X_1 \subset X$ и, следовательно, $p \in X$. В противном случае, так как множество $N$, начиная с числа $M_2 = 6$ было разбито на полуинтервалы вида $[M_k, M_{k+1})$, то $(\exists k \in N\backslash\{1\})(p \in [M_k, M_{k+1}))$. Найдем и зафиксируем это $k$, а также заметим, что $p \neq M_k$, так как $M_k$ для $k > 2$ составное число по определению. То есть $M_k < p < M_{k+1}$. Тогда в силу следствия из теоремы $\exists l = \overline{1, p_{k+1} - 1}$и $r \in G_k$, такие, что $p = lM_k + r$, т. е. $p$ представимо в виде (8). Следовательно, $p \in X_k \subset X$ или$p \in X$. Что и требовалось доказать.

Важно отметить, что одним из следствий утверждения 5 является бесконечная мощность множества $X$, в силу аналогичной мощности $P_\infty$. А построение данного множества заключается в последовательном построении $X_k$ с помощью алгоритма $\boldsymbol{A}$. Поэтому множество $X$ будем также рассматривать как последовательность. Обозначим члены данной последовательности $x_1$, $x_2$, … тогда утверждение 5 говорит о том, что последовательность простых чисел является подпоследовательностью $X$ или $X$ является надпоследовательностью ряда простых чисел. Именно $X$ является последовательностью, заявленной ранее, в том числе в названии статьи, среди элементов которой будем искать простые числа. Рассмотрим некоторые свойства последовательности $X$ и множеств её составляющих.

**Утверждение 6**. $(\forall x \in X_k)\left(\forall i = \overline{1, k}\right)$ ($x$ не кратно $p_i \in P_k$)

*Доказательство*. Предположим противное: $(\exists x \in X_k)(\exists i = \overline{1, k})$($x$ кратно $p_i$). Так как $x \in X_k$, то он представим в виде (8), то есть:

$$x = lM_k + g, l = \overline{1, p_{k+1} - 1}, g \in G_k.$$

Тогда:

$$g = x - lM_k. \tag{12}$$

По нашему предположению $x$ кратно $p_i$, но и $lM_k$ кратно $p_i$ по построению. Тогда из (12) следует, что $g$ кратно $p_i$, но это противоречит общему виду элемента $G_k$, который представляет собой произведение степеней простых чисел с порядковым номером большим $k$и, согласно утверждению 1, является взаимно простым с $M_k$, а, следовательно, не может быть кратен $p_i i = \overline{1, k}$. Получили противоречие. Наше предположение неверно. Утверждение доказано.

Покажем теперь, что последовательность $X$неограниченно расширяется на множестве натуральных чисел.

**Утверждение 7**. $(\forall m \in N)(\exists i \in N | x_{i+1} - x_i > m)$

*Доказательство*. Предположим противное: $(\exists m \in N)(\forall i \in N | x_{i+1} - x_i \leq m)$. Выберем произвольное $m$, удовлетворяющее данному условию. В качестве$x_i$ возьмем $M_{m+1} + 1$. Заметим, что именно такой вид имеет первый элемент $X_{m+1}$. Действительно, как уже было ранее упомянуто для $\forall k \in N\backslash\{1\}$ элемент $g_1$ равен 1. Это тот случай, когда все степени в произведении простых чисел равны 0-лю.

Тогда по нашему предположению $x_{i+1} - M_{m+1} - 1 \leq m$.

С другой стороны, $x_{i+1} > x_i = M_{m+1} + 1$. Соберём из полученных неравенств одно:

$$M_{m+1} + 1 < x_{i+1} \leq M_{m+1} + (m+1).$$

Тогда $\exists j = \overline{2,(m+1)}$, такое, что $x_{i+1} = M_{m+1} + j$. Пусть $p$ – наименьший простой делитель $j => p \leq j \leq m+1$, а значит, что $p$ входит в произведение $M_{m+1}$, то есть $M_{m+1}$ кратно $p$.

Тогда и $x_{i+1}$ кратно $p$, как сумма двух кратных $p$ чисел ($M_{m+1}$ и $j$), что противоречит утверждению 6. Получили противоречие. Утверждение доказано.

Данное утверждение показывает, что плотность $X$ниже соответствующей плотности множества натуральных чисел, что верно и для ряда простых чисел. Вместе с тем, тот факт, что $P_\infty \subset X$ (утверждение 5) говорит оплотности $X$, как не превышающей соответствующую плотность $P_\infty$.

Покажем, что элементы $X_k$ не кратны друг другу.

**Утверждение 8**. $(\forall k \in N)(\forall \overset{\wedge}{x}, \overset{\vee}{x} \in X_k \left| \overset{\wedge}{x} \neq \overset{\vee}{x}\right.)(\overset{\wedge}{x}$не кратно $\overset{\vee}{x})$

*Доказательство.* Предположим противное $(\exists k \in N)(\exists \overset{\wedge}{x}, \overset{\vee}{x} \in X_k \left| \overset{\wedge}{x} \neq \overset{\vee}{x}\right.)(\overset{\wedge}{x}$ кратно $\overset{\vee}{x})$.

Высказывание $\overset{\wedge}{x}$ кратно $\overset{\vee}{x}$ по определению означает, что $\exists t \in N$, такое, что

$$\overset{\wedge}{x} = t \cdot \overset{\vee}{x} \tag{13}$$

Заметим, что $1 < t < p_{k+1}$. Действительно, $\overset{\wedge}{x}, \overset{\vee}{x} \in X_k$, а это значит, согласно утверждению 3, $M_k < \overset{\wedge}{x}, \overset{\vee}{x} < p_{k+1} \cdot M_k$. Тогда, если предположить, что $t \geq p_{k+1}$, то $M_{k+1} = p_{k+1} \cdot M_k \leq t \cdot M_k < t \cdot \overset{\vee}{x} = \overset{\wedge}{x}$, или $M_{k+1} < \overset{\wedge}{x}$, что противоречит утверждению 3. С другой стороны, $\overset{\wedge}{x}, \overset{\vee}{x}$ положительные и$\overset{\wedge}{x} \neq \overset{\vee}{x}$, что означает $t > 1$.

Итак, мы показали, что$1 < t < p_{k+1}$. Но тогда$t$имеет простой делитель из $P_k$ (возможно сам себя, если является простым). То есть $(\exists i = \overline{1,k})(t$ кратно $p_i)$. Тогда $t \cdot \overset{\vee}{x}$также кратно $p_i$. Следовательно, в силу (13) $\overset{\wedge}{x}$ кратно $p_i$, что противоречит утверждению 6. Следовательно, наше предположение неверно. Утверждение доказано.

Для упрощения дальнейших теоретических построений введём в рассмотрение два множества. Множество простых чисел из заданного интервала $P_{k+1}^k = \{p \in P_\infty | M_k < p < M_{k+1}\}$ и множество $Z_k = \{z \in U_k | M_k < z < M_{k+1}\}$. Поясним, что $P_{k+1}^k$ – это просто множество простых чисел из интервала $(M_k, M_{k+1})$, а $Z_k$ – это числа по своей природе аналогичные $G_k$, с тем лишь отличием, что элементы $G_k$ принадлежат интервалу $(0, M_k)$, а $Z_k$ – интервалу $(M_k, M_{k+1})$. Отметим, что использование интервалов не противоречит ранее предложенному разбиению числового ряда на полуинтервалы вида $[M_k, M_{k+1})$, так как элементы множеств $P_\infty$, $U_k$, $G_k$ не могут совпадать с $M_k$ по природе построения.

**Следствие**. $(X_k = Z_k \cup P_{k+1}^k)$и $(Z_k \cap P_{k+1}^k = \emptyset)$

*Доказательство*. То, что $Z_k \cap P_{k+1}^k = \emptyset$ легко заметить, обратив внимание на построение данных множеств. Действительно, произвольный элемент $z$ из множества $Z_k$ имеет вид $p_{k+1}^{a_1} \cdot p_{k+2}^{a_2} \cdot \ldots \cdot p_{n(k)}^{a_{n(k)-k}}$, где $a_i \in N \cup \{0\}, \forall i = \overline{1, n(k)-k}$. Согласно заданию отображения $n$ и множества $P_k$ имеет место неравенство $p_{k+1}^{a_1} < p_{k+2}^{a_2} < \ldots < p_{n(k)}^{a_{n(k)-k}} < M_k$. Вместе с тем множество $P_{k+1}^k$ состоит из простых чисел больших $M_k$. Это означает, что в факторизации любой пары элементов из $Z_k$ и $P_{k+1}^k$ не будет не одного совпадающего сомножителя (факторизация элемента из $P_{k+1}^k$ и есть он сам). То есть, просто нет ни одного совпадающего элемента. Поэтому любая пара элементов из этих множеств не только не совпадает, но ещё и взаимно проста.

Покажем теперь, что $X_k = Z_k \cup P_{k+1}^k$. Пусть $x \in X_k$, тогда, если $x$ – простое число, то в силу утверждения 5 и задания $P_{k+1}^k$ верно, что $x \in P_{k+1}^k$. В противном случае, согласно

основной теореме арифметики [4], $x$ разлагается на простые делители, среди которых не могут быть $p_i, i = \overline{1,k}$ согласно утверждению 6, и элементы $P_{k+1}^k \subset X_k$, согласно утверждению 8. Тот факт, что $P_{k+1}^k$ является подмножеством $X_k$, напрямую следует из утверждения 5 и построения данных множеств.

Таким образом, в качестве простых делителей $x$ могут выступать только $p_{k+1}, p_{k+2}, \dots, p_{n(k)}$. Поэтому либо$x$– простое число и принадлежит $X_k$, либо $x = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \dots \cdot p_{n(k)}^{\alpha_{n(k)-k}} \alpha_i \in N \cup \{0\}, i = \overline{1, n(k)-k}$, то есть $x \in Z_k$. Что и требовалось доказать.

Заметим также, что $\{p_{n(k)+1}, p_{n(k)+2}, \dots, p_{n(k+1)}\}$ и есть множество $P_{k+1}^k$. Действительно, по определению отображения $n$, $p_{n(k)}$ – самое большое простое число меньше $M_k$, следовательно $p_{n(k)+1}$ – первое простое число больше $M_k$, аналогично, $p_{n(k+1)}$ – самое большое простое число меньше $M_{k+1}$.То есть рассматриваемое множество – это совокупность простых чисел между $M_k$ и $M_{k+1}$, чем по определению и является $P_{k+1}^k$.

Кроме того, из данного следствия легко заключить, что $P_{k+1}^k = X_k \backslash Z_k$, то есть простые числа в интервале $(M_k, M_{k+1})$ можно найти исключив из множества $X_k$ элементы множества $Z_k$. Именно этот подход представляется крайне интересным с точки зрения построения алгоритма поиска простых чисел среди членов последовательности $X$.

**Утверждение 9**. $G_{k+1} = \{g \in G_k \cup X_k | g$ *не кратно* $p_{k+1}\}$

*Доказательство*. В силу следствия к утверждению 8 $G_k \cup X_k = G_k \cup Z_k \cup P_{k+1}^k$.

Рассмотрим некоторое число $h = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \dots \cdot p_{n(k)}^{\alpha_{n(k)-k}} \cdot p_{n(k)+1}^{\gamma_1} \cdot p_{n(k)+2}^{\gamma_2} \cdot \dots \cdot p_{n(k+1)}^{\gamma_{n(k+1)-n(k)+k}}$, причём $h < M_{k+1}, \alpha_i, \gamma_j \in N \cup \{0\}, \forall i = \overline{1, n(k)-k}, \forall j = \overline{1, (k+1)-n(k)}$. Заметим, что согласно способу задания и наложенным ограничениям $h \in G_{k+1}$, при условии, что $\alpha_1 = 0$.

Предположим, что $h$ не принадлежит $G_k \cup Z_k$, тогда $(\exists j = \overline{1, n(k+1)-n(k)+k} | (\gamma_j \neq 0)$. Другими словами хотя бы одна степень у сомножителей из множества $P_{k+1}^k$ не равна 0. Тогда, если хотя бы ещё одна степень $\alpha_i$ или $\gamma_t (t \neq j)$ не равна 0 или $\gamma_j > 1$, то $h > p_{k+1} \cdot p_{n(k)+j}$. Но $p_{n(k)+j} \in P_{k+1}^k$, а значит, удовлетворяет неравенству $M_k < p_{n(k)+j} < M_{k+1}$. Тогда верно, что $h > p_{k+1} \cdot p_{n(k)+j} > p_{k+1} \cdot M_k = M_{k+1}$., то есть $h > M_{k+1}$. Но $h < M_{k+1}$, следовательно, наше предположение неверно и $\gamma_j$ будет равным 1 только при условии, что остальные простые сомножители входят в $h$ с нулевой степенью.

Итак, было взято $h = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \dots \cdot p_{n(k)}^{\alpha_{n(k)-k}} \cdot p_{n(k)+1}^{\gamma_1} \cdot p_{n(k)+1}^{\gamma_2} \cdot \dots \cdot p_{n(k)+1}^{\gamma_{m(k+1)-n(k)}}$ и показано, что если $h$ не принадлежит $G_k \cup Z_k$, то оно принадлежит $P_{k+1}^k$. Таким образом, переобозначив $\gamma$ через $\alpha$с соответствующими индексами, получаем, что для любого элемента $g = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \dots \cdot p_{n(k+1)}^{\alpha_{n(k+1)-k}} \Big| g < M_{k+1}; \alpha_i \in N \cup \{0\}, i = \overline{1, n(k)-k}$ верно, что $g \in G_k \cup Z_k \cup P_{k+1}^k$.

Покажем теперь, что произвольный элемент $g \in G_k \cup Z_k \cup P_{k+1}^k$ можно представить в виде $g = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \dots \cdot p_{n(k+1)}^{\alpha_{n(k+1)-k}} \Big| g < M_{k+1}; \alpha_i \in N \cup \{0\}, i = \overline{1, n(k)-k}$.

Рассмотрим 2 случая: $g \in G_k \cup Z_k$ и $g \in P_{k+1}^k$. Согласно следствию из утверждения 8 эти случаи взаимно исключающиеся.

1) $g \in G_k \cup Z_k$. Отметим, что $G_k = \{g \in U_k | \ g < M_k\}, Z_k = \{z \in U_k | M_k < z < M_{k+1}\}$, а множество $U_k = \left\{u = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \dots \cdot p_{n(k)}^{\alpha_{n(k)-k}} | a_i \in N \cup \{0\}, \forall i = \overline{1, n(k)-k}\right\}$. Следовательно

$$G_k \cup Z_k = \left\{g = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \dots \cdot p_{n(k)}^{\alpha_{n(k)-k}} \ | g < M_{k+1}; \alpha_i \in N \cup \{0\}, \forall i = \overline{1, n(k)-k}\right\}$$

или

$$G_k \cup Z_k = \left\{ g = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \ldots \cdot p_{n(k)}^{\alpha_{n(k)-k}} \cdot p_{n(k)+1}^{0} \cdot p_{n(k)+2}^{0} \cdot \ldots \cdot p_{n(k+1)}^{0} \middle| g < M_{k+1}; \alpha_i \in N \cup \{0\}, \forall i = \overline{1, n(k)-k} \right\}. \quad (14)$$

2) $g \in P_{k+1}^k$. Тогда $\left( \exists j, j = \overline{n(k)+1, n(k+1)} \middle| g = p_j \right.$, в силу чего $P_{k+1}^k$ можно представить в виде:

$$P_{k+1}^k = \left\{ g = p_{k+1}^{0} \cdot p_{k+2}^{0} \cdot \ldots \cdot p_{n(k)}^{0} \cdot p_{n(k)+1}^{0} \cdot \ldots \cdot p_j^1 \cdot \ldots \cdot p_{n(k+1)}^{0} \middle| g < M_{k+1}; \alpha_i \in N \cup \{0\}, \forall i = \overline{1, n(k)-k} \right\}. \quad (15)$$

Из (14) и (15) видно, что если $g \in G_k \cup Z_k \cup P_{k+1}^k$, то его можно представить в виде $g = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \ldots \cdot p_{n(k+1)}^{\alpha_{n(k+1)-k}} \Big| g < M_{k+1}; \alpha_i \in N \cup \{0\}, i = \overline{1, n(k)-k}$.

Таким образом, было показано, что

$$G_k \cup Z_k \cup P_{k+1}^k = \left\{ g = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \ldots \cdot p_{n(k+1)}^{\alpha_{n(k+1)-k}} \middle| g < M_{k+1}; \alpha_i \in N \cup \{0\}, i = \overline{1, n(k)-k} \right\}.$$

Преобразуем полученное множество, исключив из него элементы, кратные $p_{k+1}$:

$$\{ g \in G_k \cup Z_k \cup P_{k+1}^k | g \text{ не кратно } p_{k+1} \} = \{ g = p_{k+2}^{\alpha_2} \cdot \ldots \cdot p_{n(k+1)}^{\alpha_{n(k+1)-k}} | g < M_{k+1};$$

$$\alpha_i \in N \cup \{0\}, i = \overline{1, n(k)-k} \}.$$

Легко видеть, что правая часть равенства представляет собой множество $G_{k+1}$. То есть $G_{k+1} = \{ g \in G_k \cup Z_k \cup P_{k+1}^k | g \textit{ не кратно } p_{k+1} \}$. Что и требовалось доказать.

Утверждение 9 крайне важно для построения алгоритма поиска простых чисел среди элементов множества (последовательности) $X$. Одним из шагов этого алгоритма будет построение $X_k$. На этом шаге сразу можно будет проверять кратность каждого нового элемента $p_{k+1}$, что, вкупе с тем фактом, что построение $X_k$ предполагает неоднократное прохождение элементов множества $G_k$, говорит о возможности на этом же шаге построить $G_{k+1}$. Такой подход обеспечивает итеративное, не влияющее на асимптотическую сложность алгоритма построение $G_{k+1}$на основе $G_k$ и $X_k$.

С учётом утверждения 9, разработана диаграмма (рис. 1), демонстрирующая взаимосвязь между элементами ключевых введённых множеств в соотношении с числовой прямой.

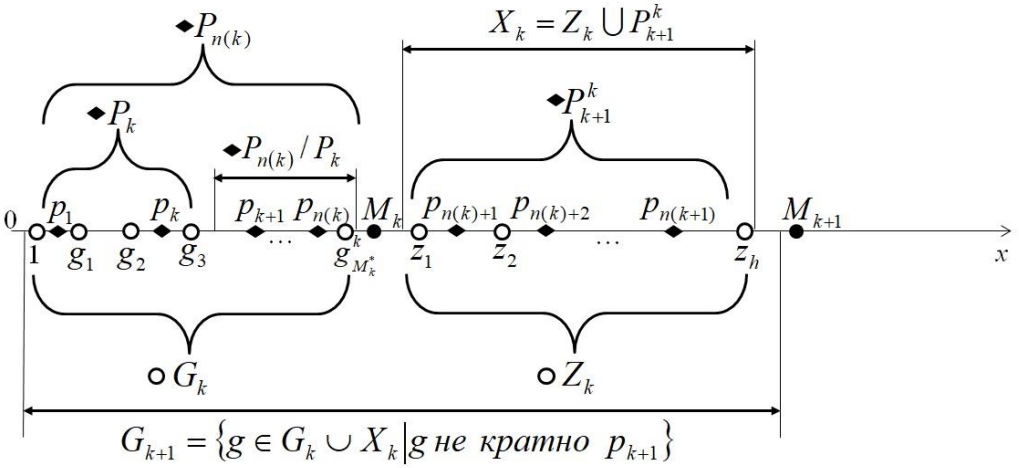


*Рис. 1. Взаимосвязь между множествами $P_k$, $P_{n(k)}$, $P_{k+1}^k$, $G_{k+1}$, $X_k$, $G_k$, и числами$M_k$ и $M_{k+1}$ в контексте числовой прямой*

Так как точки некоторых множеств перемешаны, принадлежность тому или иному множеству на Рисунке 1 показана формой точек. Для понимания того, какому множеству

точки какой формы принадлежат у соответствующих множеств присутствует значок в форме точек, обозначающих элементы этого множества.

**Утверждение 10**. $(\forall k \in N\backslash\{1\})\left(p_{k+1} \cdot g_{M_k^*}^k \in Z_k\right)$

*Доказательство*. Так как $g_{M_k^*}^k \in G_k$, то его можно представить в виде:

$$g_{M_k^*}^k = p_{k+1}^{\alpha_1} p_{k+2}^{\alpha_2} \cdot \ldots \cdot p_{n(k)}^{\alpha_{n(k)-k}} \tag{16}$$

и верно неравенство

$$g_{M_k^*}^k < M_k. \tag{17}$$

Из (16) следует, что

$$p_{k+1} \cdot g_{M_k^*}^k = p_{k+1}^{\alpha_1+1} p_{k+2}^{\alpha_2} \cdot \ldots \cdot p_{n(k)}^{\alpha_{n(k)-k}}, \tag{18}$$

А умножив обе части (17) на $p_{k+1}$ получим:

$$p_{k+1} \cdot g_{M_k^*}^k < M_{k+1},. \tag{19}$$

Из выражений (18) и (19) видно, что $p_{k+1} \cdot g_{M_k^*}^k$ является членом множества $G_k \cup Z_k$. Вместе с тем $g_{M_k^*}^k$ – максимальный элемент $G_k$ по определению. Но$p_{k+1} \cdot g_{M_k^*}^k$ будет больше всех элементов $G_k$, начиная с $k = 2$. Это означает, что $p_{k+1} \cdot g_{M_k^*}^k \in Z_k$. Что и требовалось доказать.

**Следствие 1**. $(\forall k \in N\backslash\{1\})(\forall g \in G_k)(g \cdot p_{k+1} \in G_k) \vee (g \cdot p_{k+1} \in Z_k)$.

Действительно, равенства (18) и (19) верны не только для $g_{M_k^*}^k$, но и для любого элемента $G_k$. Следовательно, $g \in G_k \cup Z_k$, что равносильно условию следствия.

**Следствие 2**. $(\forall k \in N\backslash\{1\})(\forall g \in G_k | g > M_{k-1})(gp_{k+1} \in Z_k)$.

В силу следствия 1 из утверждения 10 достаточно показать, что $gp_{k+1} \notin G_k$.Действительно, $g > M_{k-1}$, следовательно, $gp_{k+1} > M_{k-1}p_{k+1} > M_{k-1}p_k = M_k$.А это означает, что $g \cdot p_{k+1} \notin G_k$, согласно построению последнего ($G_k$задаётся как множество элементов $U_k$меньших $M_k$).

Рассмотрим ещё одно утверждение, проливающее свет на природу $Z_k$.

**Утверждение 11**. $(\forall k \in N\backslash\{1\})(\forall z \in Z_k)\left(\exists p \in P_{n(k)}\backslash P_k\right)$ такое, что $z$ кратно$p$ и $z/p \in G_k$.

*Доказательство*. Так как $z \in Z_k$, то выполняется неравенство $M_k < z < M_{k+1}$. Вместе с тем все простые числа в интервале $(M_k; M_{k+1})$ по определению принадлежат множеству $P_{k+1}^k$ и, согласно следствию к утверждению 8, не могут принадлежать $Z_k$. Следовательно, $z$ является составным числом.

Пусть $p$ – простой делитель $z$. Благодаря тому, что $z \in Z_k$ известен общий вид факторизации $z$. Из этого вида можно заключить, что $p \in P_{n(k)}\backslash P_k$. и, как следствие, $p \geq p_{k+1}$.

Так как $z \in Z_k$, верно неравенство

$$z < M_{k+1}$$

или

$$z < p_{k+1} \cdot M_k.$$

Разделим обе части неравенства на $p \in P_{n(k)}\backslash P_k$и получим

$$z/p < p_{k+1} \cdot M_k/p \leq p_{k+1} \cdot M_k/p_{k+1} = M_k$$

или

$$^{z}/_{p} < M_k.$$

С другой стороны, так как $p \in P_{n(k)} \backslash P_k$, $^{z}/_{p} \in U_k$. Тогда $^{z}/_{p} \in G_k$ по определению множества $G_k$.

Заметим, что в ходе доказательства утверждения 11 был взят произвольный простой делитель $z$. Таким образом, для любого простого делителя $p$ произвольного числа $z \in Z_k$ верно, что $^{z}/_{p} \in G_k$.

Кроме того, из утверждения 11 вытекает метод построения множества $Z_k$ как произведений элементов множеств $P_{n(k)}/P_k$ и $G_k$. Разумеется, не каждая пара элементов этих множеств принадлежит $Z_k$. Часть из них будет также принадлежать $G_k$, а часть будет больше $M_{k+1}$. С точки зрения построения $Z_k$ алгоритм нахождения всех пар элементов $P_{n(k)}/P_k$ и $G_k$, вычисление их произведения и отсеивания принадлежащих $G_k$ и больших $M_{k+1}$ представляется асимптотически и вычислительно крайне сложным.

Вместе с тем, благодаря утверждению 10 и его следствиям представляется возможным построение алгоритма, который на каждом шаге будет обрабатывать только те элементы $P_{n(k)}/P_k$ и $G_k$, произведение которых даёт элемент $Z_k$.

При этом само $Z_k$ допустимо задать, как $Z_k = \{z = gp | g \in G_k, p \in P_{n(k)} \backslash P_k, z \in G_k, z < M_{k+1}\}$.

Докажем ещё одно утверждение, которое дополнит картину взаимосвязей между элементами рассмотренных множеств. Для этого возьмём и зафиксируем произвольный элемент $z \in Z_k$.Согласно следствию к утверждению 8, $Z_k \subset X_k$, из чего следует, что $z = l \cdot M_k + g$, причём $l, g \in N, l < p_{k+1}, g \in G_k$.

**Утверждение 12**. Числа$z$и $g$ – взаимно просты.

Предположим противное. А именно НОД$(z, g) > 1$.

В силу того, что $z \in Z_k$, а $g \in G_k$ их факторизацию можно представить в виде:

$$z = p_{k+1}^{\alpha_1} \cdot p_{k+2}^{\alpha_2} \cdot \ldots \cdot p_{n(k)}^{\alpha_{n(k)-k}},$$

а

$$g = p_{k+1}^{\beta_1} \cdot p_{k+2}^{\beta_2} \cdot \ldots \cdot p_{n(k)}^{\beta_{n(k)-k}},$$

где $\alpha_i, \beta_i \in N \cup \{0\}, \forall i = \overline{1, n(k)-k}$.

Тогда, известно [4], что

$$\text{НОД}(z, g) = p_{k+1}^{min(\alpha_1, \beta_1)} \cdot p_{k+2}^{min(\alpha_2, \beta_2)} \cdot \ldots \cdot p_{n(k)}^{min(\alpha_{n(k)-k}, \beta_{n(k)-k})}.$$

Согласно сделанному предположению $\exists i = \overline{1, n(k)-k}$ такое что $min(\alpha_i, \beta_i) \neq 0$. Следовательно, $z$кратно $p_{k+i}$ и $g$ кратно $p_{k+i}$. Но тогда $z - g = l \cdot M_k$ кратно $p_{k+i}$, что невозможно, так как в силу известного вида факторизации $M_k$ и того факта, что $l < p_{k+1}$, все простые делители $l \cdot M_k$ меньше $p_{k+1} \leq p_{k+i}, \forall i = \overline{1, n(k)-k}$.

Таким образом, было показано, что наше предположение неверно. Следовательно, утверждение доказано.

Рассмотренные и доказанные теорема, утверждения и следствия позволяют спроектировать алгоритм поиска простых чисел в заданном диапазоне на основе полученных теоретических результатов. Идея алгоритма состоит в том, чтобы последовательно находить простые числа из интервалов $(M_k; M_{k+1})$ для каждого $k \in N \backslash \{1\}$. Для того, чтобы найти простые числа в интервале $(M_k; M_{k+1})$ достаточно построить $X_k$, посредством алгоритма ***A***. После чего, удобно воспользоваться следствием из утверждения 8, которое говорит, что $X_k = Z_k \cup P_{k+1}^k$ и $Z_k \cap P_{k+1}^k = \emptyset$, а это значит, что $P_{k+1}^k = X_k \backslash Z_k$. То есть, для получения искомого

$P_{k+1}^{k}$, достаточно построить $Z_k$, исключая его элементы из $X_k$. Для построения этих множеств требуется перестраивать вспомогательные множества. Например, на каждом шаге нам понадобиться перестраивать $G_k$ для нового, увеличенного на 1 значения $k$. Для решения этой задачи, как было ранее отмечено, целесообразно воспользоваться утверждением 9.

**Выводы и заключение**

В данной работе предложена и рассмотрена последовательность, для которой доказывается, что все простые числа являются её членами. Кроме того, показано, что, как и для ряда простых чисел, расстояние между членами построенной последовательности неограниченно возрастает. То есть плотность данной последовательности меньше плотности ряда натуральных чисел. Дальнейшие исследования планируется посвятить разработке алгоритмов построения последовательности простых чисел и быстрой факторизации на основе предложенных теоретических выкладок с асимптотической сложностью соответствующей плотности $X$ относительно натурального числового ряда. Кроме того, интерес представляет дальнейшее исследование природы множеств $G_k$ и $Z_k$, а также возможности их более быстрого построения.

**Список литературы**


1. Бараш Л. Алгоритм AKS проверки чисел на простоту и поиск констант генераторов псевдослучайных чисел: Безопасность информационных технологий. // Черноголовка: Институт теоретической физики им. Л. Д. Ландау. 2005. С. 27-38.
2. Василенко О. Н. Теоретико-числовые алгоритмы в криптографии. М.: МЦНМО, 2003.
3. Ландау Э. Основы анализа. М.: ИЛ, 1947.
4. Матысик О. В., Трофимук А. А. Теория чисел. Брест: Изд-во БрГУ, 2013.
5. Шеврин Л. Н. Общая алгебра. Глава IV. Полугруппы. М.: Наука, 1991. Т. 2.
6. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: Триумф, 2002.
7. Chen J.R. On the Distribution of Almost Primes in an Interval // Sci.: Sinica18, 1975. 611-627.
8. Guy R. Unsolved Problems in Number Theory: Pseudoprimes. Euler Pseudoprimes. Strong Pseudo-primes. //New York: Springer-Verlag. 1994. 28-29.
9. Lawrence C. Elliptic Curves: Number Theory and Cryptography. Washington: Chapman & Hall/CRC. 2003.
10. Miller G. L. Riemann's hypothesis and tests for primality. // Journal of Computer and Systems Sci-ences. 1976. 300-317.
11. Montgomery H., Vaughan R. The exceptional set of Goldbach's problem // Poland, Poznan, Institute of Mathematics of the Polish Academy of Sciences: Actaarithmetica, 1975. 353-370.
12. Strassen V., Solovay R. A Fast Monte-Carlo Tests for Primality // SIAM Journal on Computing. 1977. №6(1). 84-85.

# AN APPROACH FOR SEARCHING PRIME NUMBERS AMONG MEMBERS OF CONSTRUCTED IN SPECIAL WAY SUBSE-QUENCE OF INTEGERS

**D. V. Polyakov**
Cand. Sci. (Technical)
dimadress@mail.ru
Tambov
**A. I. Popov**
Cand. Sci. (Pedagogical),
associate professor
olimp_popov@mail.ru
Tambov
**A. N. Tolmacheva**
a.tolma4yova@yandex.ru
Tambov

Tambov State Technical University

**Abstract.** The article deals with the problem of finding Prime numbers from a given range and factorizing large numbers. The relevance of the research is due to the spread of asymmetric cryptographic algorithms as methods for ensuring a secure session in the global network, which causes the need for additional research that clarifies the properties of a number of Prime numbers. Mechanisms for searching for Prime numbers are in demand by cryptology both to improve the security of the global network, and to develop new methods of attacks on asymmetric cryptographic encryption systems. In this paper, we consider a sequence of numbers for which a series of Prime numbers is a subsequence. To construct this sequence, we propose to divide a series of natural numbers into semi-intervals whose boundaries are products of a certain number of first primes. It is shown that on each such half-interval there is a set of a special type, which, among other things, belongs to the primes that fall into the corresponding half-interval. This set is interesting because its density is lower than the density of the natural series. This means that it is possible to construct this set using an algorithm with relatively low asymptotic complexity. The paper presents and proves a number of statements and their consequences, which shed light on the properties of the sequence obtained from the Union of sets of a special type. It is shown in the language of set theory that a possible iterative construction of the sequence under study is possible, as well as that a series of primes is a subsequence for it. The obtained theoretical results allow us to design an algorithm for searching for Prime numbers in a given range, and also create a Foundation for building fast algorithms for factorization of large numbers.

**Keywords:** prime numbers, arithmetic, searching for prime numbers, building a series of prime numbers.

## References

1. Barash, L. (2005) AKS algorithm for checking numbers for simplicity and searching for constants of pseudo-random number generators: information technology Security. [*Algoritm AKS proverki chisel na prostotu i poisk constant generatorov psevdosluchajnyh chisel*]. Chernylovka: Landau Institute of theoretical physics. 27-38.
2. Chen J.R. (1975) On the Distribution of Almost Primes in an Interval.

3. Guy R. (1994). Unsolved Problems in Number Theory: Pseudoprimes. Euler Pseudoprimes. Strong Pseudoprimes. New York: Springer-Verlag. 28-29.
4. Landau, E. (1947) Fundamentals of analysis [*Osnovy analiza*]. Moscow: IL.
5. Lawrence C. (2003) Elliptic Curves: Number Theory and Cryptography. Washington: Chapman & Hall.
6. Matysik, O. V., Trofimuk, A.A. (2013) Number Theory [*Teoriya chisel*]. Brest.
7. Miller G.L. (1976) Riemann's hypothesis and tests for primality. // Journal of Computer and Systems Sciences. 300-317.
8. Montgomery H., Vaughan R. (1975) The exceptional set of Goldbach's problem. Poland, Poznan, Institute of Mathematics of the Polish Academy of Sciences: Actaarithmetica. 353-370.
9. Schneier, B. (2002). Applied cryptographyProtocols, algorithms, source texts in C. [*Prikladnaya kriptografiya. Protokoly, algoritmy, iskhodnye teksty na yazyke C*]. Moscow.
10. Shevrin, L. N. (1991) General algebra Chapter IV. Semigroups [*Obshchaya algebra*] Moscow: Nauka. 2.
11. Strassen V., Solovay R. (1977) A fast Monte-Carlo Tests for Primality. SIAM Journal on Computing. 6(1). 84-85.
12. Vasilenko, O. N. (2003) Theoretical and numerical algorithms in cryptography [*Teoretiko-chislovye algoritmy v kriptografii*]. Moscow.