УДК 511. 178

01.00.00 Физико-математические науки

КОМБИНАТОРНЫЙ МЕТОД ФАКТОРИЗАЦИИ ЧИСЕЛ

Бредихин Борис Андреевич
кандидат технических наук, профессор
РИНЦ SPIN-код: 9984-6650

Проблема, имеющая элементарную формулировку, побуждает искать наиболее простое её решение. Именно такой попыткой является изложенный в работе комбинаторный метод факторизации натуральных чисел. Комбинаторный метод обладает простым алгоритмом, приводящим непосредственно к цели – отысканию всех факторизаций и установлению всех простых чисел на любом интервале натурального ряда. Простые числа никакой информации о себе, кроме собственной величины, не несут. Составные числа, обладая свойством делимости, дают возможность подобрать ключи к закону их распределения. Достижение этой цели однозначно и полно решает и проблему отыскания закона распределения простых чисел

Ключевые слова: КОМБИНАТОРНЫЙ МЕТОД, ФАКТОРИЗАЦИЯ ЧИСЕЛ

Doi: 10.21515/1990-4665-123-122

UDC 511. 178

Phys - Math. sciences

COMBINATORY METHOD OF NUMBERS′ FACTORIZATION

Bredikhin Boris Andreevich
Candidate of Engineering sciences, professor
RSCI SPIN - code: 9984-665

Problem having elementary formulation makes us look for its easier solution. So the combinatorial method of positive integer's factorization is an attempt to do it. The combinatory method possesses simple algorithm, leading immediately to finding out all the factorizations and identification of all prime numbers on any interval of the positive integers. Prime numbers don't carry any information except their own magnitude. Composite numbers, possessing divisibility properties provide possibility to discover the law of their distribution. The achievement of this purpose also completely solves the problem of finding out the law of prime numbers' distribution

Keywords: COMBINATORY METHOD, FACTORIZATION OF NUMBERS

СОДЕРЖАНИЕ

1. Введение

Достоинство самой науки требует, чтобы все возможные средства были исследованы для решения проблемы разложения составных чисел в их факторы, проблемы столь изящной и настолько знаменитой.

Карл Фридрих Гаусс

Проблема, имеющая элементарную формулировку, побуждает искать возможно более простое её решение. Именно такой попыткой является изложенный в работе комбинаторный метод факторизации натуральных чисел.

Выбор комбинаторного метода обусловлен не только характером проблемы, но также возможностями комбинаторики. По образному выражению Лейбница комбинаторика должна заниматься одинаковым и различным, похожим и непохожим, абсолютным и относительным, в то время как обычная математика занимается большим и малым, единицей и многим, целым и частью. Лейбниц предвидел широкую сферу применения комбинаторики в наше время.

Комбинаторный метод обладает простым алгоритмом, приводящим непосредственно к цели – отысканию всех факторизаций и установлению всех простых чисел на любом интервале натурального ряда.

Простые числа никакой информации о себе, кроме собственной величины, не несут. Составные числа, обладая свойством делимости, дают возможность подобрать ключи к закону их распределения. Достижение этой цели однозначно и полно решает и проблему отыскания закона распределения простых чисел.

2. Алгоритм построения графов сочетаний простых делителей

В основе комбинаторного метода факторизации лежит идея отыскания канонических разложений натуральных чисел некоторого промежутка $x \le x_m$ в виде сочетаний простых делителей $p_1 \le p_i \le p_m$. Ясно, что множество всевозможных сочетаний этих делителей (с повторами делителей в группе) содержит в себе полное и бесповторное множество канонических разложений чисел промежутка $x \le x_m$, если $x_m = p_1 p_m$.

Это множество целесообразно разбить на подмножества по числу делителей s в разложении : $\bar{C}_m^2$, $\bar{C}_m^3$, …, $\bar{C}_m^{Sm}$. Здесь полка означает повторность делителей в группе, а s_m – максимально возможное число делителей в разложениях чисел интервала $x \le x_m$.

Значение s_m определяется из условия $p_1^{Sm} \le x_m$. Из него следует: $s_m = \left|\frac{\ln x_m}{\ln p_1}\right|$. При выборе $x_m = p_1 p_m$ значение $s_m = \left|1 + \frac{\ln p_m}{\ln p_1}\right|$. При выборе $x_m = p_1^{Sm}$ значение s_m задано и, следовательно, $p_m \le p_1^{Sm-1}$.

В итоге, для решения поставленной выше задачи необходимо задать интервал простых делителей $p_1 \le p_i \le p_m$, установить границу x_m интервала $x \le x_m$, вычислить значение s_m и составить подмножества $\bar{C}_m^s$.

Далее исключением тех чисел x на интервале $x \le x_m$, для которых получены канонические разложения, установить подмножество простых чисел интервала. Последнее состоит из заданной последовательности $p_1 \le p_i \le p_m$ и вновь обнаруженных на этом интервале простых чисел $p_m < p_i < x_m$.

В общем случае отыскание сочетаний подмножества $\bar{C}_m^s$ затруднений не вызывает. Однако в данной задаче возникает проблема отбора только тех сочетаний, для которых выполняется условие $X \leq X_m$.

Эту проблему предлагается решить применением алгоритма, позволяющего упорядочить процесс составления сочетаний и осуществить их отбор по условию $X \leq X_m$.

Суть предлагаемого алгоритма состоит в следующем. Полнота и бесповторность сочетаний на множестве $\bar{C}_m^s$ будет обеспечена, если в процессе образования каждая предыдущая группа делителей сочетается только со старшим по сравнению с последним делителем группы или сочетается с равным ему.

Эту версию составления сочетаний будем именовать первой. Её сочетания будем изображать в виде линейно упорядоченных групп с неубывающими индексами делителей. Ниже для наглядности изложения приведена таблица всевозможных сочетаний $\bar{C}_5^2$ (рисунок 1). В этой таблице делители p_i представлены своими индексами.

p_i	p_1	p_2	p_3	p_4	p_5
p_1	1·1	1·2	1·3	1·4	1·5
p_2	2·1	2·2	2·3	2·4	2·5
p_3	3·1	3·2	3·3	3·4	3·5
p_4	4·1	4·2	4·3	4·4	4·5
p_5	5·1	5·2	5·3	5·4	5·5

Рисунок 1. Таблица возможных сочетаний $\bar{C}_5^2$.

Правая часть таблицы вместе с диагональю содержит бесповторное множество сочетаний вида $\bar{C}_5^2$, в которых индексы делителей возрастают.

Однако можно показать, что приведенное выше условие достижения полноты и бесповторности применимо при любом числе элементов в группе.

На множестве групп $\bar{C}_m^{s+1}$, образованных по данному алгоритму из какой-либо группы множества $\bar{C}_m^s$, повторов быть не может, так как новые группы отличаются друг от друга присоединяемым элементом. Любые два таких множества $\bar{C}_m^{s+1}$ не пересекаются, так как образованы на основе разных исходных групп.

Что касается полноты множества $\bar{C}_m^{s+1}$, то данный алгоритм образования упорядоченных групп не оставляет возможности для появления иных групп. Ясно также, что включение в число присоединяемых делителя, равного последнему в исходной группе, не меняет выводов,сделанных выше.

Все сказанное выше верно и для варианта, когда каждая предыдущая группа делителей сочетается только с младшими, по сравнению с последним делителем группы, или сочетается с равным ему. Эти сочетания составляют левую часть таблицы вместе с её диагональю. Версию их составления будем именовать второй.

Полнота сочетаний на множестве $\bar{C}_m^s$ обеспечена полнотой возможных значений параметров

$2 \leq s \leq s_m$ и $p_1 \leq p_l \leq p_m$.

Множество сочетаний $\bar{C}_m^s$ при s =const удобно представить в виде древовидной структуры (графа), имеющей уровни n = 1, 2, …, s .

Введём следующую терминологию и символику.

Порядок графа: s ($2 \leq s \leq s_m$).

Уровни графа : n ($1 \leq n \leq s$).

Последовательность делителей p_i на уровне n графа порядка s будем обозначать символом p_{i_n}.

Последовательности p_{i_n} будем называть кронами уровня n, а последовательность делителей $p_{i_1}. . p_{i_{n-1}}$ – стволом соответствующей кроны. По необходимости уместно применять термин многоуровневая крона с указанием её ствола, а граф, построенный для ствола p_{i_1}, называть частичным графом первого уровня.

3. Структура графов первой версии

В графах присутствуют канонические разложения чисел $X \le X_m$ Для их исключения необходимо на всех уровнях всех графов установить предел для присоединяемых p_{i_n} из условия $X \le X_m$. Предельное значение p_{i_n} будем обозначать p_{k_n}.

Для графа второго порядка ограничение на первом уровне определяется из условия $p_{k_1}^2 \le x_m$, $p_{k_1} \le \sqrt{x_m}$.

На втором уровне ограничения находятся из условия

$$p_{i_1} p_{k_2} \le x_m, \quad p_{k_2}(p_{i_1}) \le \frac{x_m}{p_{i_1}}.$$

Заметим, что p_{k_2} определяется для каждого делителя первого уровня

$$p_1 \le p_{i_1} \le p_{k_1}.$$

Для графа третьего порядка ограничения определяются из следующих условий.

$$n = 1: \; p_{k_1}^3 \le x_m; \; p_{k_1} \le \sqrt[3]{x_m};$$

$$n = 2:\ p_{i_1} p_{k_2}^2 \le x_m;\ \ p_{k_2}(p_{i_1}) \le \sqrt{\frac{x_m}{p_{i_1}}};$$

$$n = 3:\ p_{i_1}\, p_{i_2}\, p_{k_3} \le x_m;\ \ p_{k_2}(p_{i_1}, p_{i_2}) \le \frac{x_m}{p_{i_1} p_{i_2}}.$$

Заметим, что p_{k_2} определяется для каждого сочетания делителей p_{i_1}, p_{i_2}, полученного на втором уровне.

Для графа произвольного порядка s ограничения на его уровнях выражаются формулами:

$$p_{k_1} \le \sqrt[s]{x_m},\ p_{k_2} \le \sqrt[s-1]{\frac{x_m}{p_{i_1}}},\ p_{k_3} \le \sqrt[s-2]{\frac{x_m}{p_{i_1} p_{i_2}}}, \ldots\ldots\ldots,$$

$$p_{k_n} \le \sqrt[s-(n-1)]{\frac{x_m}{p_{i_1} \cdots\cdots p_{i_{n-1}}}},\ p_{k_s} \le \frac{x_m}{p_{i_1} \cdots\cdots p_{i_{n-1}}}.$$

На уровнях $n \ge 1$ ограничения p_{k_n} определяются для каждого сочетания делителей p_{i_1}, p_{i_2}, …, $p_{i_{n-1}}$. Значения p_{k_n}, полученные по этим формулам, будем называть оценками.

Ограничение p_{k_n} в любой кроне следует ставить в соответствие стволу p_{i_1}, p_{i_2},.., $p_{i_{n-1}}$, а граф с таким стволом и кроной на уровнях от n до s называть частичным графом уровня n - 1.

Ниже в качестве примера составлены графы первой версии с ограничениями для интервала $x \le x_m = 249$.

Максимальный делитель графа: $p_m \le \frac{x_m}{p_1} = 83 = p_{22}$

Максимальный порядок графа: 83

$$s_m \le \left|1 + \frac{\ln p_m}{\ln p_1}\right| = \left|1 + \frac{\ln 83}{\ln 3}\right| = \left|1 + \frac{4{,}42}{1{,}09}\right| = 5.$$

Интервал порядка графов: $2 \le s \le 5$.

Граф $s = 2$.

Уровень $n = 1$: $p_{k_1} \le \sqrt{x_m} = \sqrt{249} = 15,8$; $p_{k_1} = 13 = p_5$. Крона первого уровня: $p_1 \le p_{i_1} \le p_5$.

Уровень $n = 2$: $p_{k_2} p_{i_1} \le x_m$, $p_{k_2}(p_{i_1}) \le \frac{x_m}{p_{i_1}}$.

$p_{k_2}(p_1) = 83 = p_{22}$, крона $p_1 \le p_{i_2} \le p_{22}$;

$p_{k_2}(p_2) = 47 = p_{14}$, крона $p_2 \le p_{i_2} \le p_{14}$;

$p_{k_2}(p_3) = 31 = p_{10}$, крона $p_3 \le p_{i_2} \le p_{10}$;

$p_{k_2}(p_4) = 19 = p_7$, крона $p_4 \le p_{i_2} \le p_7$;

$p_{k_2}(p_5) = 19 = p_7$, крона $p_5 \le p_{i_2} \le p_7$.

Граф $s = 2$ показан на рисунке 2 в виде совокупности частичных графов со стволами $p_1 \le p_{i_1} \le p_5$.

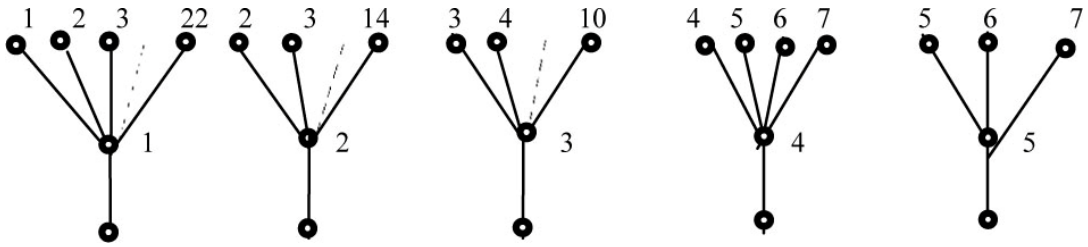

Рисунок 2. Граф $s = 2$, $x \le 249$.

Граф $s = 3$.

Уровень $n = 1$: $p_{k_1} \le \sqrt[3]{x_m} = \sqrt[3]{249} = 6,29$, $p_{k_1} = 5 = p_2$.

Крона первого уровня: $p_1 \le p_{i_1} \le p_2$.

Уровень $n = 2$: $p_{k_2}^2 p_{i_1} \le x_m$, $p_{k_2}(p_1) \le \sqrt{\frac{x_m}{p_{i_1}}}$.

$p_{k_2}(p_1) = 7 = p_3$, крона $p_1 \le p_{i_2} \le p_3$;

$p_{k_2}(p_2) = 7 = p_3$, крона $p_2 \le p_{i_2} \le p_3$.

Уровень $n = 3$: $p_{k_3}(p_{i_1}, p_{i_2}) \le \frac{x_m}{p_{i_1} p_{i_2}}$.

$p_{k_3}(p_1, p_1) = 23 = p_8$, крона $p_1 \le p_{i_3} \le p_8$;

$p_{k_3}(p_1, p_2) = 13 = p_5$, крона $p_2 \le p_{i_3} \le p_5$;

$p_{k_3}(p_1, p_3) = 11 = p_4$. крона $p_3 \le p_{i_3} \le p_4$. ;

$p_{k_3}(p_2, p_2) = 7 = p_3$. крона $p_2 \le p_{i_3} \le p_3$;

$p_{k_3}(p_2, p_3) = 7 = p_3$. крона $p_{i_3} = p_3$.

Граф $s = 3$ показан на рисунке 3 в виде совокупности двух частичных графов со стволами p_1 и $_2$.

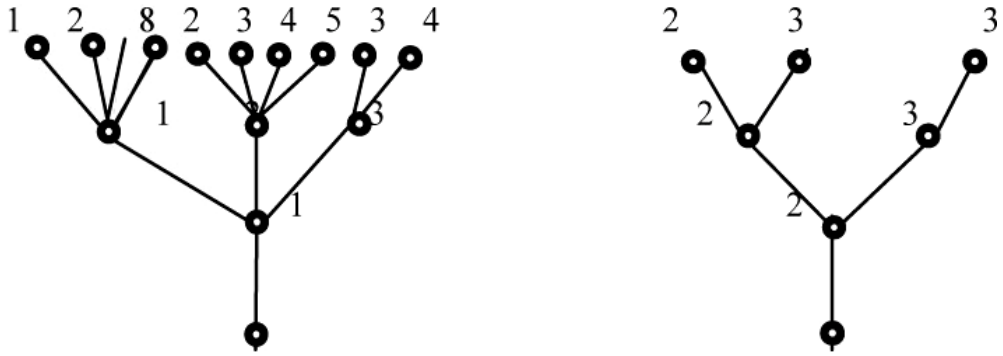

Рисунок 3. Граф $s = 3$, $x \le 249$.

Граф $s = 4$.

Уровень $n = 1$: $p_{k_1} \le \sqrt[4]{x_m} = \sqrt[4]{249} = 3,97$, $p_{k_1} = 3 = p_1$.

Крона первого уровня содержит только делитель p_1.

Уровень $n = 2$: $p_{k_2}(p_1) \le \sqrt[2]{\frac{x_m}{p_{i_1}}}$, $p_{k_2}(p_1) = 3 = p_1$.

Крона второго уровня содержит только делитель p_1.

Уровень $n = 3$: $p_{k_3}(p_{i_1}, p_{i_2}) \le \sqrt{\frac{x_m}{p_{i_1} p_{i_2}}}$.

$p_{k_3}(p_1, p_1) = p_2$, крона $p_1 \le p_{i_3} \le p_2$.

Уровень $n = 4$: $p_{k_4} \le \frac{x_m}{p_{i_1} p_{i_2} p_{i_3}}$.

$p_{k_4}(p_1, p_1, p_1) = 7 = p_3$, крона $p_1 \le p_{i_4} \le p_3$.

$p_{k_4}(p_1, p_1, p_2) = 5 = p_2$, крона $p_{i_4} = p_2$.

Граф $s = 4$ показан на рисунке 4.

Граф $s = 5$.

Расчёт ограничений p_{k_n} в кронах графа $s = 5$ даёт следующие результаты: на всех уровнях графа $s = 5$ ограничение $p_{k_n} = p_1$, то есть на всех уровнях крона содержит только делитель p_1.

Граф $s = 5$ показан на рисунке 4.

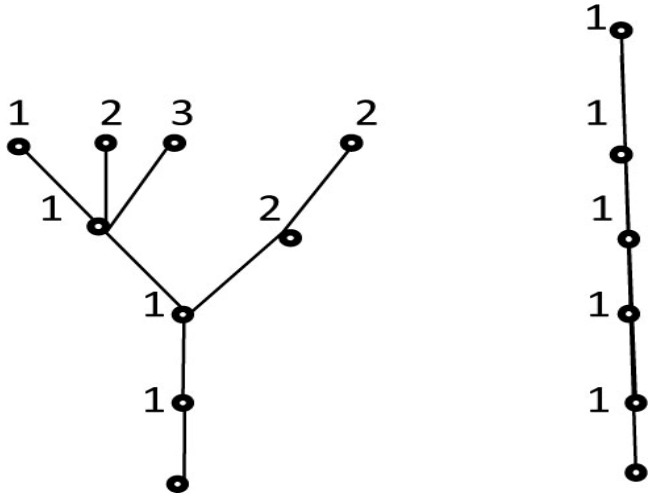

Рисунок 4. Графы $s = 4$ и $s = 5$, $x \le 249$.

Древовидная структура графа сочетаний простых делителей (рисунки 2. 2, 2. 3) обладает следующим свойством. Если на любом уровне

$1 \le n \le s$ отобрать две любые ветви, изображающие делители p_i данного уровня, и достроить их во всех остальных уровнях, то получатся две структуры, не пересекающиеся между собой. Это свойство графа позволяет выделить из него частичные графы любого уровня $1 \le n \le s$

Так, например, граф порядка s можно представить как совокупность частичных графов, построенных на отдельных ветвях, изображающих делители первого уровня $p_1 \le p_{i_1} \le p_{k_1}$. Ветви p_{i_1} будем называть стволами частичных графов первого уровня, а надстройку над ними – кроной частичного графа первого уровня.

Аналогично можно выделить из графа порядка s структуру, опирающуюся на ствол p_{i_1}, p_{i_2},.. , p_{i_n} ($1 \le n \le s$), и назвать её частичным графом уровня n, имеющим крону во всех вышележащих уровнях.

Кстати, при $n = s - 1$ крону частичного графа составляют ветви $p_{i_{s-1}} \le p_{i_s} \le p_{k_s}$, то есть крона графа располагается в одном уровне $n = s$.

У частичного графа уровня $n = s$ крона отсутствует, а его ствол $p_{i_1} \ldots p_{i_s}$ изображает разложение единственного числа $x = p_{i_1} p_{i_2} \cdots p_{i_s}$.

Представление графов первой версии в табличной форме

Представление множества сочетаний простых делителей p_i в виде древовидной структуры (графа) при больших x_m приводит к непреодолимым трудностям. Логично, в таком случае, применить табличный способ записи множества сочетаний.

Алгоритм составления таблицы идентичной графу со стволом p_{i_1} не зависит ни от ствола, ни от порядка графа. Это следует из принципа

построения структуры графа. Таблица, идентичная частичному графу порядка s со стволом p_{i_1} имеет следующий вид. Число строк таблицы равно s +1.

Нижние s строк содержат делители p_i соответствующих уровней графа $1 \le n \le s$. Число, равное произведению делителей p_i какой-либо колонки таблицы, записывается на пересечении данной колонки и верхней строки. Левая колонка на всех уровнях $1 \le n \le s$ заполняется делителем p_{i_1} (ствол графа). В верхней строке колонка содержит составное число $x = p_{i_1}^s$.

Далее в очередной колонке на уровне $n = s$ вписывается p_{i_s} с индексом на единицу большим. В верхней строке записывается $x = p_{i_1}^{s-1} p_{i_s}$. Процесс повышения индекса i_s в следующих колонках продолжается до тех пор, пока выполняется условие $x = p_{i_1}^{s-1} p_{i_s} \le x_m$. Старший делитель p_{i_s} признаётся конечным и обозначается p_{k_s}.Все колонки, содержащие на уровне $n = s$ делители $p_{i_1} \le p_{i_s} \le p_{k_s}$, содержат на остальных уровнях делитель p_{i_1}. Верхняя строка заполняется числами $x = p_{i_1}^{s-1} p_{i_s}$.

Затем в очередной колонке на уровне $n = s - 1$ вписывается делитель $p_{i_{s-1}}$ с очередным после p_{i_1}. индексом (то есть p_{i_1+1}). Этот же делитель вписывается и на уровне $n = s$, то есть в данной колонке $p_{i_s} = p_{i_{s-1}} = p_{i_1+1}$. На остальных уровнях $1 \le n \le s - 2$ этой колонки в качестве делителя p_{i_n} остаётся p_{i_1}. В верхней строке колонка содержит число $x = p_{i_1}^{s-2} p_{i_{s-1}}^2$.

Далее варьируется значение делителя p_{i_s} в пределах $p_{i_{s-1}} \le p_{i_s} \le p_{k_s}$. Делитель p_{k_s} находится из условия $x = p_{i_1}^{s-2} p_{i_{s-1}} p_{k_s} \le x_m$. При этом на уровнях $1 \le n \le s - 2$ сохраняются делители $p_{i_n} = p_{i_1}$, а на уровне $n = s - 1$

делители $p_{i_{s-1}} = p_{i_1+1}$.

В очередной (после достижения p_{k_s}) колонке индекс делителя опять возрастёт на единицу и устанавливается $p_{i_{s-1}} = p_{i_s} = p_{i_1+2}$. Индекс $s-1$ будет повышаться на единицу после каждого события $p_{i_s} = p_{k_s}$ до достижения значения $p_{k_{s-1}}$ из условия $x = p_{i_1}^{s-2} p_{k_{s-1}}^2 \le x_m$.

В очередной колонке (после достижения $p_{k_{s-1}}$) на уровне $n = s - 2$ делитель $p_{i_n} = p_{i_1}$ должен быть заменён на очередной - $p_{i_{s-2}} = p_{i_1+1}$. На уровнях $n = s-1$ и $n = s$ устанавливается тот же делитель, то есть

$$p_{i_s} = p_{i_{s-1}} = p_{i_{s-2}} = p_{i_1+1}$$

Событие $p_{i_s} = p_{k_s}$, $p_{i_{s-1}} = p_{k_{s-1}}$, $p_{i_{s-2}} = p_{k_{s-2}}$ приведёт к возрастанию на единицу индекса делителя на уровне $n = s - 3$ и установке его на остальных уровнях.

По описанному выше алгоритму можно представить в виде таблицы частичный граф любого уровня со стволом p_{i_1}, p_{i_2}, … p_{i_n}, где $n < s$. Крона такого графа развивается на уровнях от $n + 1$ до $n = s$, а на уровнях, лежащих ниже n , делители ствола сохраняются постоянными.

4. Структура графов второй версии

Особенности структуры графов, кроны которых составлены по условию $p_{i_n} \le p_{i_1}$, рассмотрим на примере графов интервала $x \le x_m = 249$, $p_m = 83$, $s_m = 5$.

Граф $s = 2$.

Уровень n = 1: $p_{k_1} \le \frac{x_m}{p_1^{s-1}} = \frac{249}{3} = 83$, $p_{k_1} = 83 = p_{22}$.

Крона первого уровня : $p_1 \le p_{i_1} \le p_{22}$.

Уровень n = 2: $p_{k_2}(p_{i_1}) \le \frac{x_m}{p_{i_1}}$, $p_{i_1}^* < p_{i_1} \le p_{k_1}$, где $p_{i_2}^* \le \sqrt[s]{x_m}$, $p_{i_1}^* = p_5$.

Для наименьшего ствола $p_{i_2} = p_6$: $p_{k_2}(p_6) = p_5$. Ограничение $p_{k_2} = p_5$ будет действовать до ствола p_{i_1} включительно, определяемого формулой

$p_{i_2}(p_5) \le \frac{x_m}{p_5} = \frac{249}{13} = 19,1$, $p_{i_2}(p_5) \le p_7 = 19$.

Далее, задаваясь последовательно $p_{k_2} < p_5$, следует определять значения p_{i_1} по формуле $p_{i_1}(p_{k_2}) \le \frac{x_m}{p_{k_2}}$.

$p_{i_1}(p_4) \le p_7 = 19$. Ограничение $p_{k_2} \le p_4$ возможно только при $p_{i_1} \le p_7$, но при $p_{i_1} = p_7$ действует менее жёсткое ограничение $p_{k_2} = p_5$.

$p_{i_1}(p_3) \le p_{10} = 31$. Ограничение $p_{k_2} = p_3$ действует в графах $p_7 < p_{i_1} \le p_{10}$.

$p_{i_1}(p_2) \le p_{14} = 47$. Ограничение $p_{k_2} = p_2$, действует в графах $p_{10} < p_{i_1} \le p_{14}$.

$p_{i_1}(p_1) \le p_{22} = 83$. Ограничение $p_{k_2} = p_1$ действует в графах $p_{14} < p_{i_1} \le p_{22}$.

Граф s = 2 показан на рисунке 5.

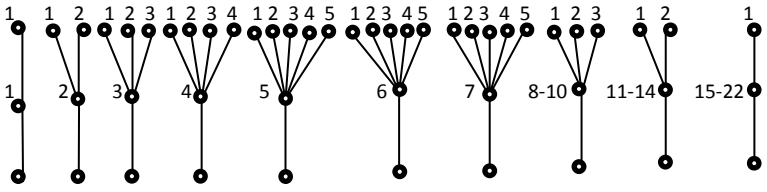

Рисунок 5. Граф s = 2, x ≤ 249.

Граф s = 3.

Уровень n = 1: $p_{k_1} \le \frac{x_m}{p_1^{s-1}} = \frac{249}{3^2} = 27,6$, $p_{k_1} = 2\,3 = p_8$. Крона первого уровня: $p_1 \le p_{i_1} \le p_8$.

Уровень n = 2: $p_{k_2}(p_{i_1}) \le \frac{x_m}{p_{i_1} p_1^{s-2}}$, где $p_{i_1}^* < p_{i_1} \le p_{k_1}$. Здесь $p_{i_1}^* \le \sqrt[3]{x_m} = \sqrt[3]{249} = 6,29$, $p_{i_1}^* = p_2$. Ограничения есть в графах со стволами $p_2 < p_{i_1} \le p_8$. На уровне n = 2 ограничений нет в графах $p_{i_1} \le p_{i_1}^*$, где $p_{i_1}^{*2} p_1 \le x_m$, $p_{i_1}^* \le \sqrt{\frac{x_m}{p_1}} = \sqrt{\frac{249}{3}} = 9,11$, $p_{i_1}^* = 7 = p_3$. Ограничения на n = 2 имеют место в графах со стволами $p_3 < p_{i_1} \le p_8$. Для $p_{i_1} = p_4$: $p_{k_2}(p_4) = 7 = p_3$.

Для $p_{k_2} = p_2$ из условия $p_{i_1} p_{k_2} p_1 \le x_m$ определяется $p_{i_1}(p_2) \le p_5 = 13$. Ограничение $p_{k_2} = p_2$ имеет место только в стволе $p_{i_1} = p_5$. В стволах $p_6 \le p_{i_1} \le p_8$ будет $p_{k_2} = p_1$.

Уровень n = 3: $p_{k_3}(p_{i_1}, p_{i_2}) \le \frac{x_m}{p_{i_1} p_{i_2}}$, $p_{i_1}^* < p_{i_1} \le p_{k_1}$, где $p_{i_1}^* \le \sqrt[s]{x_m} = \sqrt[3]{249} = 6,29$, $p_{i_1}^* = 5 = p_2$. На уровне n = 3 ограничений нет в стволах $p_{i_1} \le p_{i_1}^*$.

$p_{k_3}(p_3, p_3) = p_2$, $p_{k_3}(p_3, p_2) = p_2$, $p_{k_3}(p_4, p_3) = p_1$, $p_{k_3}(p_4, p_2) = p_1$, $p_{k_3}(p_5, p_2) = p_1$.

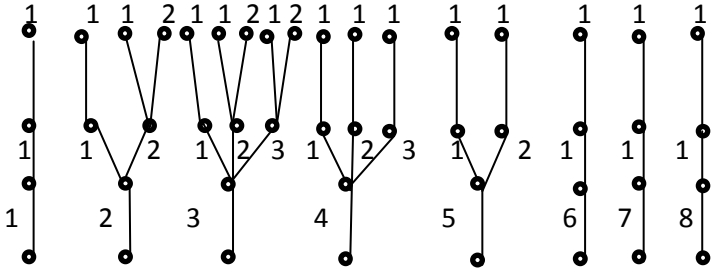

Рисунок 6. Граф s = 3, $x \le 249$.

Граф s = 4.

Уровень n = 1: $p_{k_1} \le \frac{x_m}{p_1^{s-1}} = \frac{249}{3^3} = 9,22$, $p_{k_1} = 7 = p_3$.

Крона первого уровня $p_1 \le p_{i_1} \le p_3$.

Уровень n = 2: $p_{k_2}(p_{i_1}) \le \frac{x_m}{p_{i_1} p_1^2}$, $p_{i_1}^* < p_{i_1} \le p_{k_1}$, где

$p_{i_1}^* \le \sqrt[4]{x_m} = \sqrt[4]{249} = 3,97$, $p_{i_1}^* = 3 = p_1$. Ограничения на n = 2: $p_{k_2}(p_2) = 5 = p_2$, $p_{k_2}(p_3) = 3 = p_1$.

Уровень n = 3. Ограничения возможны только в графе со стволом p_2, p_2: $p_{k_3}(p_2, p_2) = 3 = p_1$.

Уровень n = 4. Все стволы частичных графов вида $p_{i_1} p_{i_2} p_{i_3}$ имеют $p_{i_3} = p_1$. Согласно структуре графа все p_{i_4} тоже равны p_1. Граф s = 4 показан на рисунке 7.

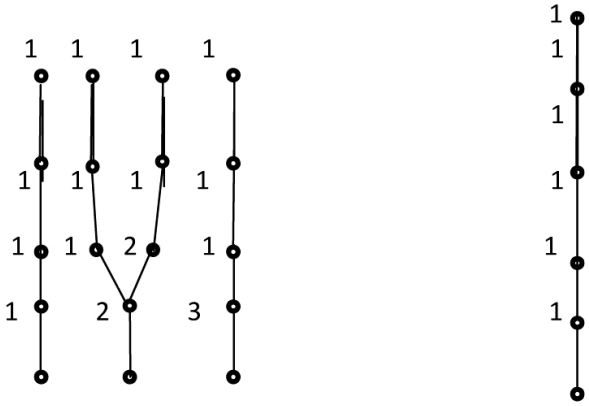

Рисунок 7. Графы s = 4 и s = 5, $x \le 249$.

Граф s = 5.

Уровень n = 1: $p_{k_1} \le \frac{x_m}{p_1^{s-1}} = \frac{249}{81} = 3,07$, $p_{k_1} = 3 = p_1$.

Согласно структуре графа на всех уровнях $p_{k_n} = p_{k_1}$.

Граф s = 5 показан на рисунке 7.

Полный граф порядка s с такой структурой кроны факторизует числа $p_1^s \le x \le p_{k_1} \dots p_{k_s}$. Здесь p_{k_s} определяется из условия $p_{k_s} p_{k_1} \dots p_{i_{s-1}} \le x_m$.

Частичный граф со стволом p_{i_1} факторизует числа $p_{i_1} p_1^{s-1} \le x \le p_{i_1} p_{k_2} .. p_{k_s}$, если $p_{i_1}^s > x_m$. Делитель p_{k_s} подбирается по условию $p_{k_s} p_{i_1} \dots p_{k_{s-1}} \le x_m$.

Левые границы частичных графов со стволами $p_1 \le p_{i_1} \le p_{k_1}$ факторизуют числа $x = p_{i_1} p_1^{s-1}$, а правые – числа $p_{i_1}^s$ или близкие к x_m, если $p_{i_1}^s > x_m$.

Представление графов второй версии в табличной форме

В основе алгоритма составления таблиц графов второй версии лежат следующие положения.

В связи с обособленностью структуры графов со стволами $p_1 \le p_{i_1} \le p_{k_1}$ (s) таблицу следует составлять для каждого графа поочерёдно. Значения ствола p_{i_1} и порядка графа не влияют на содержание алгоритма и сказываются лишь на объёме таблицы.

Для графа любого порядка с конкретным стволом нижняя строка таблицы содержит во всех колонках делитель p_{i_1}. Вторая строка будет заполняться делителями $p_1 \le p_{i_2} \le p_{i_1}$ поочерёдно по мере составления колонок слева направо. На втором уровне при любом p_{i_1} первым делителем будет p_1.

Частичный граф со стволом p_{i_1}, p_1 также является обособленной структурой и может быть записан в виде отдельной таблицы. Все кроны всех уровней в этом графе содержат согласно требованию структуры $p_{i_n} \le p_{i_{n-1}}$ только один делитель $p_{i_n} = p_1$.

Таблица графа состоит из одной колонки, в которой факторизуется число $x = p_{i_1} p_1^{s-1}$. Заметим, что именно событие $p_{i_s} = p_1$ завершает составление таблицы графа со стволом p_{i_1}, p_1. Далее необходимо рассматривать граф со стволом p_{i_1}, p_2, так как делитель p_2 отвечает условию $p_2 \le p_{i_1}$.

Таблица графа со стволом p_{i_1}, p_2 содержит $s-1$ колонок, поскольку на всех уровнях кроны содержат по условию структуры делители $p_{i_n} = p_1$ и $p_{i_n} = p_2$.

Таблица графа со стволом p_{i_1}, p_2 заканчивается после наступления события $p_{i_s} = p_2$ колонкой, факторизующей число $x = p_{i_1} p_2^{s-1}$. Последнее означает необходимость установить очередной делитель $p_{i_2} = p_3$.

Для графов со стволами $p_{i_2} > p_2$ возникает необходимость в кронах уровней $n > 2$ многократно назначать очередной делитель согласно условию $p_{i_n} \le p_{i_2}$.

Условием такого назначения на любом уровне является событие $p_{i_s} = p_{i_n}$, где p_{i_n} есть предыдущий делитель $p_{i_n} \le p_{i_2}$.

5. Алгоритм построения графов первой версии для произвольного интервала .

На любом интервале $x \le x_m$ в канонических разложениях его чисел присутствуют все делители $p_1 \le p_i \le p_m$. В кронах уровня s присутствуют числа, близкие к x_m, так как p_{k_s} подбирается по условию $x \le x_m$.

В связи с этим алгоритм составления графов интервала $x_1 < x \le x_2$ состоит в последовательном выделении частичных графов со стволами вида $p_{i_1} \cdots p_{i_n}$, содержащих в своих кронах на уровне s только числа интервала $x_1 < x \le x_2$. Правая граница крон интервала $x \le x_i \ (i = 1,2)$ определяется формулой:

$$p_{k_n}(x_i) \le \sqrt[s-(n-1)]{\frac{x_i}{p_{i_1}, \cdots, p_{i_{n-1}}}} \ .$$

Крона любого уровня графа порядка s для интервала $x_1 < x \le x_2$ имеет вид $p_{k_n}(x_1) < p_{i_n} \le p_{k_n}(x_2)$.

Построение графа порядка s целесообразно выполнять от уровня $n = 1$ до уровня $n = s$.

Последовательность действий при отыскании частичных графов интервала $x_1 < x \le x_2$ заключается в следующем:

1. Устанавливаются $p_{k_1}(x_1)$ и $p_{k_1}(x_2)$ и выделяется интервал стволов частичных графов первого уровня: $p_{k_1}(x_1) < p_{i_1} \le p_{k_1}(x_2)$.

2. В частичных графах первого уровня со стволами $p_1 \le p_{i_1} \le p_{k_1}(x_1)$ для каждого ствола p_{i_1} вычисляются $p_{k_2}(x_1)$ и $p_{k_2}(x_2)$ и выделяются частичные графы второго уровня со стволами вида p_{i_1}, p_{i_2}, в которых

$p_1 \le p_{i_1} \le p_{k_1}(x)$ и $p_{k_2}(x_1) < p_{i_2} \le p_{k_2}(x_2)$.

3. В частичных графах со стволами p_{i_1}, p_{i_2}, в которых $p_{i_1} \le p_{i_2} \le p_{k_2}(x_1)$, выделяются части крон $p_{k_s}(x_1) < p_{i_s} \le p_{k_s}(x_2)$ и соответствующие им графы третьего уровня со стволами вида p_{i_1}, p_{i_2}, p_{i_s}.

4. В графах третьего уровня со стволами $p_{i_1}, p_{i_2}, p_{i_s}$, в которых $p_1 \le p_{i_1} \le p_{k_1}(x_1)$, $p_{i_1} < p_{i_2} \le p_{k_2}(x_1)$, $p_{i_2} < p_{i_s} \le p_{k_s}(x_1)$ вычисляются и сравниваются $p_{k_4}(x_1)$ и $p_{k_4}(x_2)$.

В итоге выделяются графы четвертого уровня по условию $(x_1) < p_{i_4} \le p_{k_4}(x_2)$. Процесс выделения частичных графов заканчивается на уровне $n = s - 1$. Выделяются графы со стволами p_{i_1}, p_{i_2}, . . $p_{i_{s-1}}$ и кронами $p_{k_s}(x_1) < p_{i_s} \le p_{k_s}(x_2)$. Ясно, что все выделенные графы достраиваются до уровня $n = s$ по условию $x \le x_2$. Левые границы крон в процессе достройки определяются структурой графа, то есть не зависят более от значения x_1.

Описанный выше алгоритм построения графов применим для интервала с любыми границами x_1 и x_2, в том числе как угодно близкими. Графы порядков $2 \le s \le 5$ интервала $87 < x \le 249$ показаны на рисунках 8 – 11.

6. Алгоритм построения графов второй версии для произвольного интервала

Пусть заданы $x_m = x_1$ и $x_m = x_2$ и требуется построить графы для интервала $x_1 < x \le x_2$, и пусть построены графы всех порядков для интервала $x \le x_2$ со стволами $p_1 \le p_{i_1} \le \dfrac{x_1}{p_1^{s-1}}$ и кронами, составленными по условию $p_{i_n} \le p_{i_1}$.

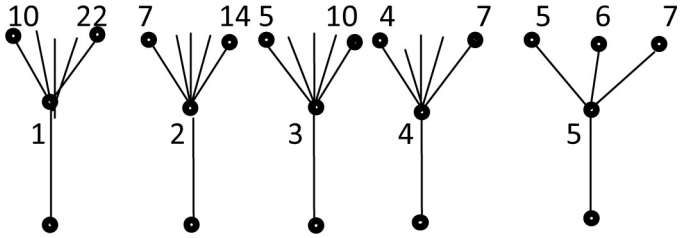

Рисунок 8. Граф $s = 2$, $87 < x \le 249$.

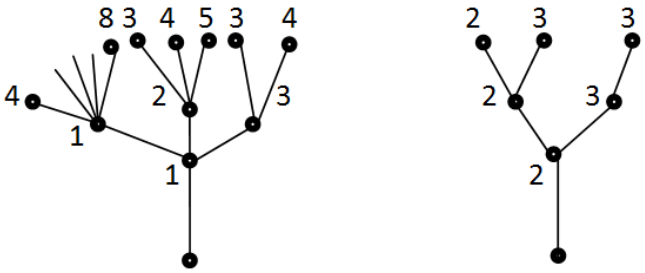

Рисунок 9. Граф $s = 3$, $87 < x \le 249$.

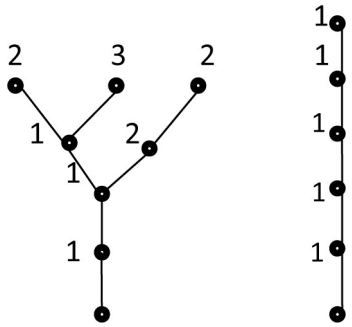

Рисунок 10. Графы $s = 4$ и $s = 5$, $87 < x \le 249$.

Ясно, что частичные графы любого порядка s со стволами, отвечающими условию $p_{i_1}^s \le x_1$, не содержат чисел интервала $x_1 < x \le x_2$ и должны быть исключены из дальнейшего рассмотрения.

Частичные графы со стволами, отвечающими условию $p_{i_1} > \frac{x_1}{p_1^{s-1}}$, содержат только числа $x_1 < x \le x_2$ и должны быть полностью приписаны этому интервалу.

Что касается частичных графов со стволами, отвечающими условию $\sqrt[s]{x_1} < p_{i_1} \le \frac{x_1}{p_1^{s-1}}$, то из них следует исключить числа $x \le x_1$. Для этого левые границы крон на всех уровнях, установленные согласно структуре графа для $x \le x_2$,должны быть заменены значениями p_{k_n} из условия $x \le x_1$. В таком виде графы будут содержать только числа интервала $x_1 < x \le x_2$.

В итоге алгоритм построения графа любого порядка для произвольно заданного промежутка состоит в следующем:

1.Установить p_{k_1} по условию $p_{k_1} \le \frac{x_1}{p_1^{s-1}}$ - границу, до которой ещё сохраняются $x \le x_1$.

2. Установить $p_{i_1} \le \sqrt[s]{x_1}$ - границу, за которой появятся числа $x > x_1$.

3. Исключить из рассмотрения графы со стволами $p_1 \le p_{l_1} \le \sqrt[s]{x_1}$.

4. Построить графы со стволами $\sqrt[s]{x_1} < p_{i_1} < \frac{x_1}{p_1^{s-1}}$. При этом правые границы крон на всех уровнях определить по условию $x \le x_2$, а левые – по условию $x > x_1$: $p_{i_1} \dots p_{l_{n-1}} p_{k_n} p_1^{s-n} \le x_2$, $p_{i_1} \dots p_{i_{n-1}} p_{k_n} p_1^{s-n} \le x_1$,

$$p_{k_n}(x_1) < p_{i_n} \le p_{k_n}(x_2).$$

Ясно, что операция по отысканию левых границ крон усложняет расчёты незначительно.

5. Построить частичные графы со стволами $\frac{x_1}{p_1^{s-1}} < p_{i_1} \le \frac{x_2}{p_1^{s-1}}$, определив правые границы крон по условию $x \le x_2$. Левые границы крон определяются структурой графа.

Следует особо заметить, что для достаточно малых интервалов кроны на нижних уровнях стягиваются каждая в одну ветвь p_{i_n}, которая становится частью ствола в частичных графах более высокого уровня. В процессе расчета это реализуется в виде событий $p_{k_n}(x_1) = p_{k_n}(x_2)$ или события $p_{k_n}(x_2) = p_{i_{n-1}}$.

Практически задача построения графов для промежутка $x_1 < x \le x_2$ решается по алгоритму для $x \le x_2$ с той лишь разницей, что в графах со стволами $\sqrt[s]{x_1} < p_{i_1} \le \frac{x_1}{p_1^{s-1}}$ кроны на всех уровнях строятся по условию $p_{k_n}(x_1) < p_{i_n} \le p_{k_1}(x_2)$, а в графах со стволами $\frac{x_1}{p_1^{s-1}} < p_{i_1} \le p_{k_1}(x_2)$, согласно структуре графа, по условию $p_{i_{n-1}} \le p_{i_n} \le p_{k_n}$.

Графы со стволами $p_{i_1} \le \sqrt[s]{x_1}$ не рассматриваются, так как факторизуют числа $x < x_1$.

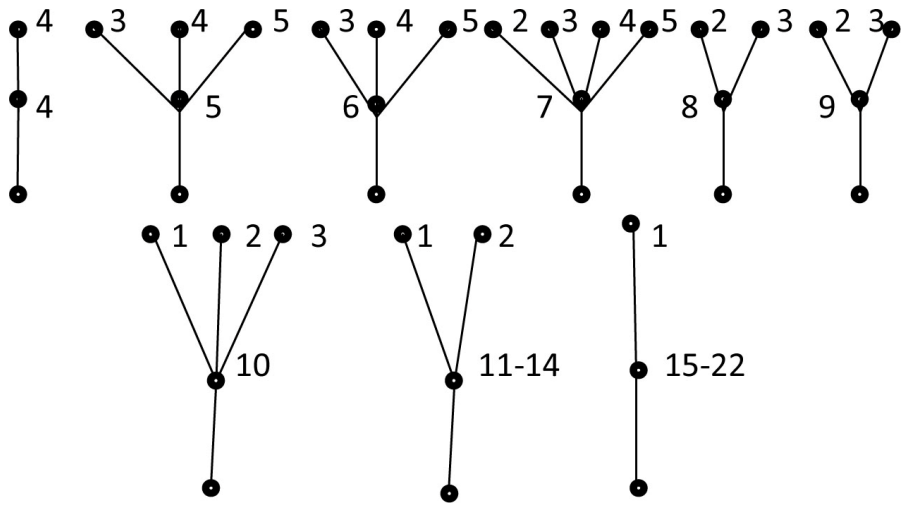

Рисунок 11. Граф $s = 2$, $p_4 \le p_{i_1} \le p_{22}$, $87 < x \le 249$.

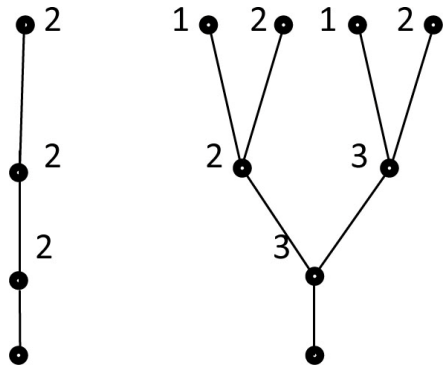

Рисунок 12. Граф $s = 3$, $p_2 \le p_{i_1} \le p_3$, $87 < x \le 249$.

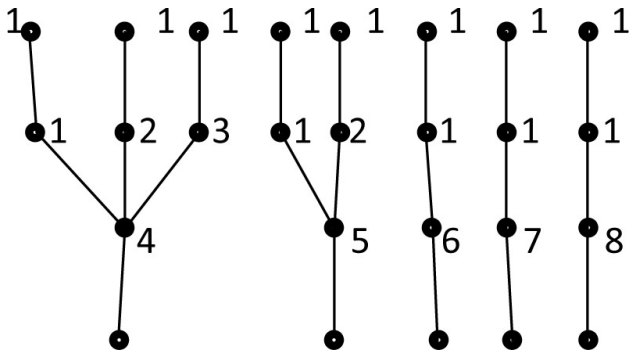

Рисунок 13. Граф $s = 3$, $p_4 \le p_{i_1} \le p_8$, $87 < x \le 249$.

7. Факторизация чётных чисел

Каждый частичный граф первой версии со стволом p_{i_1} содержит на всех уровнях кроны делители $p_{i_n} \ge p_{i_1}$. Делители $p_i < p_{i_1}$ в этом графе и в последующих отсутствуют. Это следует непосредственно из закона построения графа $p_{i_n} \ge p_{i_{n-1}}$, то есть на следующем уровне делитель не меньше предыдущего.

С другой стороны, делитель ствола p_{i_1} входит в разложение всех чисел, определяемых данным частичным графом. Это обстоятельство позволяет выделить чётные числа на заданном интервале $x \le x_m$.

Для этого достаточно включить в задаваемую последовательность p_i делитель $p_0 = 2$, то есть задать интервал $p_0 \le p_{i_1} \le p_m$.

В этом случае частичные графы всех порядков со стволами $p_{i_1} = p_0$ будут определять разложения только чётных чисел интервала $x \le x_m$ Остальные частичные графы со стволами $p_{i_1} > p_0$ чётных чисел не содержат.

Добавление p_0 в заданную последовательность простых делителей приводит в графах всех порядков к возникновению частичного графа со стволом $p_{i_1} = p_0$. Эти графы, и только они, содержат чётные числа.

Введение нового минимального делителя p_0 требует увеличения p_m по условию $p_0 p_m \le x_m$. Кроме того, в связи с заменой делителя p_1 на p_0 возрастает максимальный порядок графа согласно условию $p_0^{s_m} \le x_m$.

Можно утверждать, что графы вновь возникших порядков имеют на первом уровне только один ствол $p_{i_1} = p_0$, потому что для этих графов $p_{i_1}^s > x_m$, если $p_{i_1} > p_0$.

Поскольку все чётные числа интервала $x \le x_m$ собраны в заведомо известных графах со стволами $p_{i_1} = p_0$,то рассматривать крону первого уровня и строить графы со стволами $p_{i_1} > p_0$ нет необходимости. Для факторизации чётных чисел интервала $x \le x_m$ достаточно найти s_m из условия $p_0^{s_m} \le x_m$ и построить частичные графы всех порядков со ствола- ми $p_{i_1} = p_0$.

Графы со стволами $p_{i_1} = p_0$ для интервалов $x \le x_m$ и $x_1 < x \le x_2$ а также их таблицы строятся по алгоритмам, описанным ранее.

Заключение

Существующие методы факторизации чисел по своей сути являются методами последовательных испытаний. Комбинаторный метод с помощью простого и прозрачного алгоритма приводит непосредственно к цели. При этом весь объём вычислений выполняется с привлечением только простых чисел из заданной последовательности.

Эффективность комбинаторного метода обусловлена простотой его алгоритма, и однородностью исходных данных, простой закономерностью формирования стволов. Все вычислительные операции по построению графов однозначны и порождают однозначные следствия.

Алгоритм комбинаторного метода по своей сути является таблицей генетических кодов составных чисел, которую следует записать в границах исследуемого интервала.

Одним из значимых следствий комбинаторной факторизации является возможность разложить интервал чисел на подмножества по числу делителей в них. Это позволяет при исследовании какого-либо из подмножеств ограничиться построением только одного графа.

Другим значимым следствием комбинаторной факторизации является возможность выделить подмножества чисел интервала, кратных какому-либо простому делителю.

Именно это следствие дало возможность выделить факторизацию чётных чисел в отдельную проблему и результат представить в виде совокупности частичных графов всех порядков со стволами $p_{i_1} = p_0 = 2$.

Число графов, связанное логарифмической зависимостью с границей интервала факторизуемых чисел, с повышением границы растёт медленно, а скорость его роста стремится к нулю.

Число операций по построению графа с повышением его порядка быстро уменьшается и стремится к единице.

В интервалах натурального ряда множество факторизаций определяется только условием $\mathbf{X} \leq \mathbf{X}_{m.}$ Любое соотношение, позволяющее установить множество факторизаций на любом (как угодно малом) отрезке натурального ряда, есть закон распределения простых чисел.

Точки $\mathbf{x}_m = p_1 p_i$ являются границами спектра делителей. Делитель p_i в этой точке появляется в разложениях чисел впервые и остаётся максимально возможным (p_m) в интервалах с правой границей $\mathbf{x}_m < p_1 p_{i+1}$. Максимально возможное число делителей $\mathbf{s}_m$ остается в этих интервалах постоянным.

Однако интервалы $\mathbf{x}_m$ с постоянным p_m очень малы, а переход к новому его значению меняет весь процесс составления множества сочетаний и, следовательно, его результат. Иначе говоря, процесс составления сочетаний носит спонтанный характер, то есть обусловлен только внутренними причинами и не зависит от внешних.

Спонтанность процесса, а также высокая частота и нерегулярность смены p_m позволяют утверждать, что какой-либо обозримой закономерности распределения p_i с ростом $\mathbf{x}_m$ не существует. Однако в любом промежутке натурального ряда (в том числе как угодно малом) можно выделить все простые числа.

Последовательность результатов, полученных на множестве смежных и достаточно малых промежутков натурального ряда, и выражает собой закон распределения простых чисел. Комбинаторный метод позволяет утверждать, что эта форма закона является единственно возможной.

Комбинаторный метод не конкурирует с существующими методами в решении других проблем. Однако не исключено, что его алгоритм будет востребован при дальнейшей разработке существующих методов.

При составлении таблиц факторизаций с оптимальным выбором шага соотношение числа факторизаций и числа потребных операций получается очень выгодным. В этой своей роли комбинаторный метод, весьма вероятно, вне конкуренции.

Основным преимуществом комбинаторного метода является возможность составления таблиц факторизаций на любом отрезке натурального ряда и установление закона распределения составных и, следовательно, простых чисел.

Литература

1. Бредихин Б. А. Факторизация чисел. Комбинаторный метод/ Б. А. Бредихин. - Краснодар : Издательский Дом – Юг, 2016. –184 с.

2. Прикладная комбинаторная математика. Сборник статей/под редакцией Э. Беккенбаха. – М. : Мир, 1968. -365 с.

3. Гельфонд А. О. Элементарные методы в теории чисел / А. О. Гельфонд, Ю. В. Линник. - М. : Физматгиз, 1962. - 272 с.

4. Ишмухаметов Ш. Т. Методы факторизации натуральных чисел: учебное пособие/ Ш. Т. Ишмухаметов. - Казань: Казанский ун. , 2011. – 190 с.

5. Сергеев Э. А. Элементы теории чисел/ Э. А. Сергеев. - Краснодар: КГУ, 1998. – 175 с.

References

1. Bredihin B. A. Faktorizacija chisel. Kombinatornyj metod/ B. A. Bredihin. - Krasnodar : Izdatel'skij Dom – Jug, 2016. –184 s.

2. Prikladnaja kombinatornaja matematika. Sbornik statej/pod redakciej Je. Bekkenbaha. – M. : Mir, 1968. -365 s.

3. Gel'fond A. O. Jelementarnye metody v teorii chisel / A. O. Gel'fond, Ju. V. Linnik. - M. : Fizmatgiz, 1962. - 272 s.

4. Ishmuhametov Sh. T. Metody faktorizacii natural'nyh chisel: uchebnoe posobie/ Sh. T. Ishmuhametov. - Kazan': Kazanskij un. , 2011. – 190 s.

5. Sergeev Je. A. Jelementy teorii chisel/ Je. A. Sergeev. - Krasnodar: KGU, 1998. – 175 s.