УДК 511. 178

01.00.00 Физико-математические науки

ОЦЕНКА СЛОЖНОСТИ КОМБИНАТОРНОГО МЕТОДА ФАКТОРИЗАЦИИ ЧИСЕЛ

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

Статья посвящена оценке вычислительной сложности комбинаторного метода факторизации чисел. Сущность комбинаторного метода изложена в одноимённой статье журнала в ноябре 2016 года. Предполагается, что читатель в необходимой мере ознакомлен с её содержанием и владеет основными понятиями теории вычислительной сложности алгоритмов. В статье изложены следующие результаты исследования поставленной задачи. Алгоритм комбинаторного метода допускает параллельные вычисления. Граф любого порядка является обособленной структурой, так как его исходные данные устанавливаются независимо от других графов. Таким образом, вычислительная сложность задачи о факторизации чисел на заданном интервале натурального ряда определяется сложностью наиболее трудоёмкого графа. Анализ структуры графов позволяет утверждать, что таким является граф третьего порядка. В любом графе две ветви первого уровня порождают обособленные структуры – частичные графы первого уровня с независимыми входными данными. Таким образом, вычислительная сложность полного графа определяется максимальной сложностью графа первого уровня. Вычислительная сложность графов произвольно заданного интервала натурального ряда остаётся неизменной, если рассматривается последовательность смежных интервалов. В итоге установлено, что оценка вычислительной сложности комбинаторного метода, как и других ныне существующих методов факторизации чисел, является экспоненциальной. В этом плане комбинаторный метод не конкурирует с существующими. Однако при оценке научной значимости алгоритма определяющим фактором является не вычислительная сложность, а его новизна, позволяющая объяснить (если не открыть) какие-либо свойства натурального ряда. В заключении статьи приведены преимущества комбинаторного метода, позволяющие оценить степень его научной новизны

Ключевые слова: КОМБИНАТОРНЫЙ МЕТОД, ФАКТОРИЗАЦИЯ ЧИСЕЛ, СЛОЖНОСТЬ АЛГОРИТМА

UDC 511. 178

Phys - Math. Sciences

THE ASSESSMENT OF COMPLEXITY OF COMBINATORY METHOD OF NUMBERS' FACTORIZATION

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

This article is devoted to the assessment of the calculating complexity of combinatory method of numbers' factorization. The content of combinatory method is explained in the article of the same name published in the journal issued in November 2016. The author supposes that the reader has learnt its content and knows the basic notions of theory of calculating complexity of the algorithms. The following results of the learning of the given task are expounded in this article. The algorithm of combinatory method permits to accomplish the parallel calculations. Graph of any order is the separate structure, because its initial data are determined independently from the other graphs. So, the calculating complexity of the task about the factorization of numbers in the predetermined interval of the positive integers is defined by the complexity of the most laborious graph. The analysis of the graphs' structure allows to state that it's the graph of the third order. In any graph both branches of the first level give the separate structures- partitive graphs of the first level with independent input data. So, the calculating complexity of the graph complete is determined by the maximal complexity of the graph of the first level. The givenat random interval of positive integers stays without changes, if we observe the sequence of the adjacent intervals. In the results it's stated that the assessment of complexity of combinatory method as well other present methods of numbers'factorization is exponential. In this aspect the combinatory method doesn't compete with other actual methods. However, evaluating the scientific significance of the algorithm, the decisive factor is not the calculating complexity, but its originality, which permits to explain (if not to discover) any properties of the positive integers. In the conclusion of the article the author describes the advantages of combinatory method, permitting to appreciate the degree of its scientific novelty

Keywords: COMBINATORY METHOD, FACTORIZATION OF NUMBERS, COMPLEXITY OF ALGORITHM

Doi: 10.21515/1990-4665-134-006

СОДЕРЖАНИЕ

Введение

Бог создал натуральные числа, всё
остальное – дело рук человеческих.
Леопольд Кронекер.

Комбинаторный метод допускает параллельные вычисления и в поставленной задаче и в её фрагментах. Граф любого порядка является обособленной структурой с независимыми от других графов входными данными. Вычислительная сложность построения графа адекватна его структуре, которая определяет и сложность вычисления делителей, ограничивающих кроны, и их число на каждом уровне. Таким образом, сложность решения задачи о факторизации чисел $X \leq X_m$ определяется сложностью наиболее трудоёмкого графа.

Сравнительный анализ структуры графов позволяет считать наиболее трудоёмким граф $S = 3$ при любом X_m .Снижение трудоёмкости графа с ростом его порядка обусловлено снижением длины входа по закону

$k_1 = \frac{s\sqrt[s]{x_m}}{\ln x_m}$. Влияние этого фактора на сложность построения графа не компенсируется ростом числа уровней в графе. Этот вывод следует из анализа структуры графа.

Структура графа любого порядка имеет следующую особенность. Две ветви графа, выбранные на первом уровне, порождают обособленные структуры – частичные графы первого уровня с независимыми входными данными. Это даёт возможность построить эти графы параллельно. Следовательно, вычислительная сложность построения полного графа определяется максимальной сложностью частичного графа первого уровня.

Две ветви графа, произвольно выбранные на уровне n, порождают на уровне $n + 1$ обособленные структуры – частичные графы уровня n со стволами p_{i_1}, p_{i_2}, …, p_{i_n}. Входные данные для каждого частичного графа устанавливаются в процессе построения крон на предыдущих уровнях, однако это не исключает применение параллельных вычислений.

После построения кроны уровня n и оформления стволов p_{i_1}, p_{i_2}, …, p_{i_n} все части кроны уровня $n + 1$ могут быть построены параллельно. Например, граф со стволом p_{i_1}после построения кроны второго уровня можно разложить на графы второго уровня со стволами вида $p_{i_1} p_{i_2}$, где $p_{i_1} = const$, $p_{i_1} \le p_{i_2} \le p_{k_2}(p_{i_1})$. Эти графы можно построить параллельно.

При изменении левой границы интервала чисел x вычислительная сложность графа остаётся неизменной, если последовательно рассматриваются смежные интервалы. В этом случае ограничения крон слева известны из предыдущего расчёта.

Всё изложенное выше в равной мере относится к алгоритмам графов обеих версий. Кроме того алгоритм графа второй версии даёт возможность

выделить на каждом уровне интервалы стволов, несущих одинаковые кроны, и , следовательно, уменьшить число потребных операций для построения графа.

1. Пошаговая процедура построения графов

Оценка сложности построения графа любого порядка выполняется обособленно, то есть по независимым входным данным и адекватно его структуре, которая определяет и сложность вычисления p_{k_n} и их число на каждом уровне. В связи с этим сложность решения задачи о факторизации чисел $x \leq x_m$ определяется сложностью наиболее трудоёмкого графа. Для оценки трудоёмкости любого графа целесообразно представить его алгоритм в виде пошаговой процедуры построения графа.

Рассматривается ряд нечётных чисел x. Задаётся последовательность простых делителей : $p_1 \leq p_i \leq p_m$, $i = 1, 2, .., m$, $p_1 = 3$.

Устанавливается множество нечётных чисел $x \leq x_m$, в которых простые делители не превышают p_m, если принять $x_m = p_1 p_m$,

Множество $x \leq x_m$ разбивается по определённому алгоритму на подмножества сочетаний: $\bar{C}_m^2$,$\bar{C}_m^3$ ... , $\bar{C}_m^s$... , $\bar{C}_m^{Sm}$, $2 \leq s \leq s_m$. Здесь s-число простых делителей в факторизациях, а $s_m = \left|1 + \frac{\ln p_m}{\ln p_1}\right|$ - их максимально возможное число, определяемое по условию $p_1^{Sm} \leq x_m$.

Каждое подмножество $\bar{C}_m^s$ представляется древовидной структурой – графом порядка s. Крона графа порядка s имеет уровни $1 \leq n \leq s$. На каждом уровне $n > 1$ крона состоит из отдельных частей по числу ветвей в кроне предыдущего уровня.

Построение графа порядка s требует вычисления только делителей, ограничивающих части крон. Кроны графов первой версии построены по

условию $p_{i_n} \geq p_{i_1}$, а их ограничивающие делители вычисляются по формуле $p_{k_n} \leq \sqrt[s-(n-1)]{\frac{x_m}{p_{i_1} p_{i_2} \ldots\ldots p_{i_{n-1}}}}$, $1 \leq n \leq s$. Кроны графов второй версии построены по условию $p_{i_n} \leq p_{i_1}$, а их ограничивающие делители вычисляются по формуле $p_{k_n} \leq \frac{x_m}{p_{i_1} \ldots p_{i_{n-1}} p_1^{s-n}}$, $1 \leq n \leq s$. Эти формулы дают оценку параметра p_{k_n}, по которой он выбирается из последовательности $p_1 \leq p_i \leq p_m$.

Таким образом, вычислительная сложность построения графа определяется сложностью отыскания параметров p_{k_n} и их числом. Следует иметь в виду, что эта задача решается отдельно для графа любого порядка адекватно его структуре. Кроме того, эта задача решается поочерёдно для частичных графов со стволами p_{i_1}.

Ниже показаны графы $s = 4$ и $s = 5$ для интервала $x_m = 3981$. Делители p_{k_n}, ограничивающие кроны, представлены на графах своими индексами.

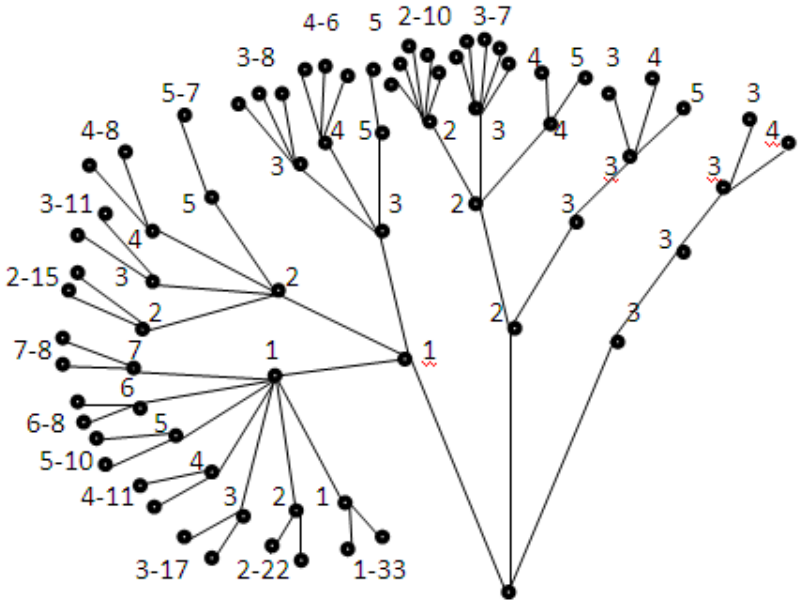

Рис. 1. Граф $s=4$, $p_{i_n} \geq p_{i_1}$.

Кроны графа построены по условию $p_{i_n} \geq p_{i_1}$. Граф содержит 150 факторизаций .Для его построения требуется 29 операций по вычислению p_{k_n}.

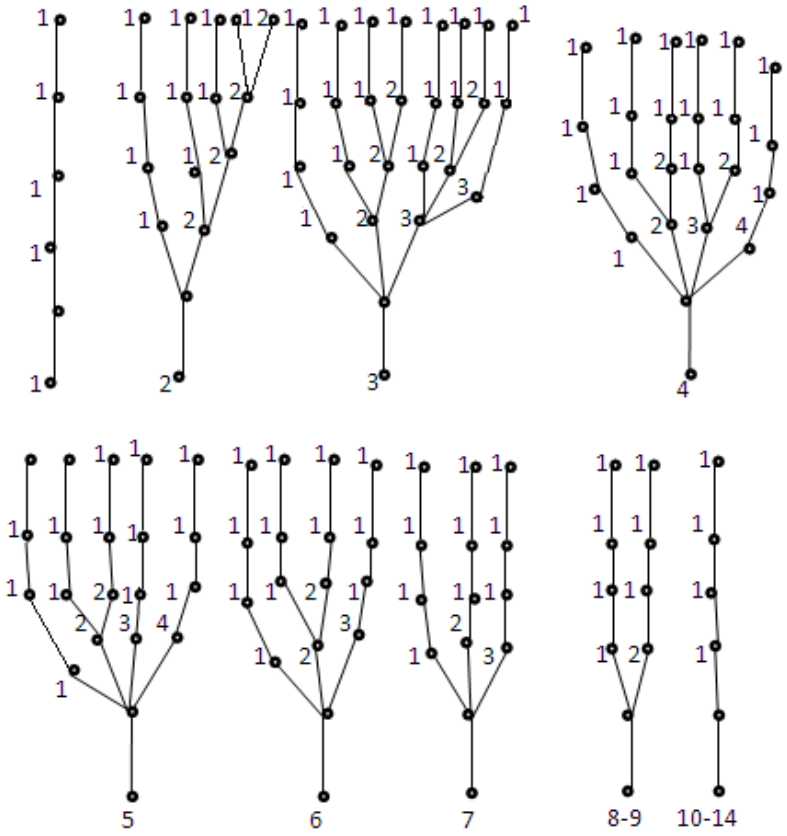

Рис. 2. Граф $s=5$, $p_{i_n} \leq p_{i_1}$.

Кроны графа построены по условию $p_{i_n} \leq p_{i_1}$. Граф содержит 41 факторизацию. Для его построения требуется 12 операций по вычислению p_{k_n}.

2. Оценка сложности алгоритма построения графов первой версии

Задано: $p_1 \leq p_i \leq p_m$, $i=1, 2,.., m$, $p_1 = 3$. Установлено $x_m = p_1 p_m$, $2 \leq s \leq s_m$, $s_m = \left|\frac{\ln x_m}{\ln p_1}\right|$. Кроны графов построены по условию $p_{i_n} \geq p_{i_1}$.

Граф $s = 2$.

Уровень $n = 1$.

Применяется формула $p_{k_1} \le \sqrt{x_m}$, с последующим отбором p_{k_1} из интервала $p_1 \le p_i \le p_m$. Эта операция выполняется однократно.

Уровень $n = 2$.

Применяется формула $p_{k_2}(p_{i_1}) \le \frac{x_m}{p_{i_1}}$ для каждого p_{i_1} из интервала $p_1 \le p_{i_1} \le p_{k_1}$ с последующим отбором p_{k_2} по его оценке $p_{k_2}(p_{i_1})$ из интервала $p_1 \le p_i \le p_m$. Число таких операций равно индексу k_1. При достаточно больших значениях x_m можно принимть $k_1 = \frac{p_{k_1}}{\ln p_{k_1}} = \frac{2\sqrt{x_m}}{\ln x_m}$.

Операция по отысканию оценки $p_{k_2}(p_{i_1})$ имеет вычислительную сложность $T(n) = O(\log^2 n)$. Сложность построения кроны графа $s = 2$ в стандартных обозначениях будет равна: $T(n) = O\left(n^{1/2}\log n\right)$. Под n понимается длина входного параметра x_m.

В частичном графе $s = 2$ со стволом p_{i_1} для построения его кроны $p_{i_1} \le p_{i_2} \le p_{k_2}(p_{i_1})$ операция $p_{k_2}(p_{i_1})$ выполняется однократно.

Граф $s = 3$.

Уровень $n = 1$.

Применяется формула $p_{k_1} \le \sqrt[3]{x_m}$, с последующим отбором p_{k_1} из интервала $p_1 \le p_i \le p_m$ по его оценке. Эта операция является единственной.

Уровень $n = 2$.

Применяется формула $p_{k_2}(p_{i_1}) \le \sqrt{\frac{x_m}{p_{i_1}}}$, для каждого p_{i_1} из интервала $p_1 \le p_{i_1} \le p_{k_1}$ с последующим отбором p_{k_2} из интервала $p_1 \le p_i \le p_m$ по его оценке .Число операций по отысканию $p_{k_2}(p_{i_1})$ равно индексу k_1 .При достаточно больших значениях x_m можно принимать $k_1 = \frac{p_{k_1}}{\ln p_{k_1}} = \frac{3\sqrt[3]{x_m}}{\ln x_m}$.

Операция по отысканию $p_{k_2}(p_{i_1})$ имеет вычислительную сложность $T(n) = O(\log^2 n)$. Сложность построения кроны второго уровня в стандартных обозначениях будет равна: $T(n) = O\left(n^{1/3}\log n\right)$.

Уровень $n = 3$.

Применяется формула $p_{k_3}(p_{i_1}\, p_{i_2}) \le \frac{x_m}{p_{i_1} p_{i_2}}$ с последующим отбором p_{k_3} из интервала $p_1 \le p_i \le p_m$. Значения делителей в сочетаниях $p_{i_1}\, p_{i_2}$ лежат в пределах : $p_1 \le p_{i_1} \le \sqrt[3]{x_m}$, $p_1 \le p_{i_2} \le \sqrt{p_m}$, то есть не превышают $\sqrt{p_m}$ и, следовательно, выполняется $p_{i_1}\, p_{i_2} < x_m$. В итоге операция по отысканию $p_{k_3}(p_{i_1}, p_{i_2})$ имеет вычислительную сложность $T(n) = O(\log^2 n)$.

Согласно структуре графа число делителей p_{k_3} равно ω_2 – числу ветвей на втором уровне:

$$\lambda_3 = \omega_2 = \sum_{i_1=1}^{k_1} [k_2(i_1)\text{-}(i_1\text{-}1)].$$

$$\text{Сумма} \sum_{i_1=1}^{k_1} (i_1\text{-}1) = \frac{k_1}{2}(k_1\text{-}1)$$

как сумма k_1 членов арифметической прогрессии.

$$\text{Сумма} \sum_{i_1=1}^{k_1} k_2(i_1) = \frac{k_1}{2}(k_2(1) + k_1),$$

если считать её суммой k_1 членов арифметической прогрессии с первым членом $k_2(1)$ и последним k_1. В итоге

$$\omega_2 = \frac{k_1}{2}(k_2(1) + 1).$$

Такой подход , как показывают расчёты, даёт небольшую ошибку даже при малых x_m, не занижая при этом оценку сложности алгоритма.

Для достаточно больших x_m можно принимать

$$k_1 = \frac{3\sqrt[3]{x_m}}{\ln x_m}\ ,\ k_2(1) = \frac{2\sqrt{x_m}}{\sqrt{3}\ln x_m}\ .$$

Тогда число операций по отысканию $p_{k_3}(p_{i_1}, p_{i_2})$ определяется формулой

$$\lambda_3 = \frac{\sqrt{3}\sqrt{x_m}\sqrt[3]{x_m}}{\ln^2 x_m} + \frac{3\sqrt[3]{x_m}}{2\ln x_m}.$$

После исключения постоянных коэффициентов и слагаемых меньшего порядка

$$\lambda_3 = \frac{\sqrt{x_m}\sqrt[3]{x_m}}{\ln^2 x_m} = \frac{{x_m}^{5/6}}{\ln x_m}.$$

В итоге вычислительная сложность построения кроны третьего уровня графа $s = 3$ обусловлена применением формулы $p_{k_3}(p_{i_1}, p_{i_2})$, выполняемой λ_3 раз с последующим отбором p_{k_3} из интервала $p_1 \le p_i \le p_m$. Сложность построения кроны третьего уровня и графа $s = 3$ в стандартных обозначениях будет равна: $T(n) = O(n^{5/6})$.

В частичном графе $s = 3$ со стволом p_{i_1} для построения кроны второго уровня $p_{i_1} \le p_{i_2} \le p_{k_2}(p_{i_1})$ выполняется однократно операция

$p_{k_2}(p_{i_1}) \le \sqrt{\frac{x_m}{p_{i_1}}}$. Для построения кроны третьего уровня для каждого p_{i_2} из интервала $p_{i_1} \le p_{i_2} \le p_{k_2}(p_{i_1})$ выполняется операция $p_{k_3}(p_{i_1} p_{i_2}) \le \frac{x_m}{p_{i_1} p_{i_2}}$. Сложность операции: $T(n) = O(\log^2 n)$. Число операций равно $k_2(i_1) = \frac{2\sqrt{x_m}}{\sqrt{p_{i_1}} \ln x_m}$. Сложность построения кроны третьего уровня и графа со стволом p_{i_1} равна: $T(n) = O\left(n^{1/2} \log n\right)$.

3. Оценка сложности алгоритма построения графов первой версии в произвольном интервале чисел

Заданы последовательности простых чисел $p_1 \le p_i \le p_{m_1}$, $p_1 \le p_i \le p_{m_2}$. Установлено: $x_1 = p_1 p_{m_1}$, $x_2 = p_1 p_{m_2}$,

$$S_{m_1} = \left|\frac{\ln x_1}{\ln p_1}\right|, \quad S_{m_2} = \left|\frac{\ln x_2}{\ln p_1}\right|.$$

Граф любого порядка для интервала $x_1 < x \le x_2$ строится, начиная с первого уровня. Во всех частях кроны каждого уровня устанавливаются делители $p_{k_n}(x_1)$ и $p_{k_n}(x_2)$, определяемые по формуле

$$p_{k_n}(x_t) \le \sqrt[s-(n-1)]{\frac{x_t}{p_{i_1}, \cdots, p_{i_{n-1}}}}, (t = 1,2).$$

Оба расчёта выполняются одновременно для одного и того же ствола вида $p_{i_1}, \cdots, p_{i_{n-1}}$, их результаты связаны следующим соотношением:

$$p_{k_n}(x_1) = p_{k_n}(x_2) \sqrt[s-(n-1)]{\frac{x_1}{x_2}}.$$

В этой формуле корень есть величина постоянная для каждого уровня в графе порядка S на данном интервале Δx .

Граф $S = 2$.

Уровень $n = 1$.

Вычисляются $p_{k_1}(x_1) \le \sqrt{x_1}$ и $p_{k_1}(x_2) \le \sqrt{x_2}$ с последующим отбором p_{k_1} из интервала $p_1 \le p_i \le p_m$. Эти операции выполняются однократно

Уровень $n = 2$.

Применяются формулы

$$p_{k_2}(x_1) \le \frac{x_1}{p_{i_1}} \text{ и } p_{k_2}(x_2) \le \frac{x_2}{p_{i_1}}$$

с последующим отбором делителей p_{k_2} из интервала $p_1 \le p_i \le p_m$.

Если рассматриваются смежные интервалы Δx , то делители $p_{k_2}(x_1)$ известны из предыдущего расчета, в котором они были правой границей кроны и обозначались $p_{k_2}(x_2)$. В этом случае оценки вычислительной сложности построения графа $S = 2$ на интервалах Δx и $x \le x_2$ совпадают.

При рассмотрении интервала Δx впервые в частичных графах интервала $p_1 \le p_{i_1} \le p_{k_1}(x_1)$ вычисляются делители

$$p_{k_2}(x_2) \le \frac{x_2}{p_{i_1}} \text{ и } p_{k_2}(x_1) = p_{k_2}(x_2)\ \frac{x_1}{x_2}$$

с последующим их отбором из интервала $p_1 \le p_i \le p_m$ по их оценкам. Кроны второго уровня в этих графах имеют вид $p_{k_2}(x_1) < p_{i_2} \le p_{k_2}(x_2)$.

В частичных графах интервала $p_{k_1}(x_1) < p_{i_1} \le p_{k_1}(x_2)$ выполняются операции только по отысканию $p_{k_2}(x_2)$ с последующим их отбором из интервала $p_1 \le p_i \le p_m$ по их оценкам. Кроны второго уровня в этих графах имеют вид $p_{i_1} < p_{i_2} \le p_{k_2}(x_2)$.

В итоге вычислительная сложность построения графа $s = 2$ будет обусловлена сложностью $T(n) = O(\log^2 n)$ операций по вычислению $p_{k_2}(x_1)$ и $p_{k_2}(x_2)$, повторенных k_1 раз, где $k_1 = \frac{2\sqrt{x_2}}{\ln x_2}$. В стандартных обозначениях она будет равна: $T(n) = O\left(n^{1/2} \log n\right)$.

Граф $s = 3$.

Уровень $n = 1$.

Вычисляются $p_{k_1}(x_1) \le \sqrt[3]{x_1}$ и $p_{k_1}(x_2) \le \sqrt[3]{x_2}$ с последующим отбором p_{k_1} из интервала $p_1 \le p_i \le p_m$. Эти операции выполняются однократно.

Уровень $n = 2$.

Применяются формулы

$$p_{k_2}(x_2) \le \sqrt{\frac{x_2}{p_{i_1}}} \quad \text{и} \quad p_{k_2}(x_1) = p_{k_2}(x_2)\sqrt{\frac{x_1}{x_2}}$$

для всех p_{i_1} из интервала $p_1 \le p_{i_1} \le p_{k_2}(x_1)$ с последующим отбором p_{k_2} из интервала $p_1 \le p_i \le p_m$ по их оценкам. Сложность операций равна: $T(n) = O(\log^2 n)$. Если рассматриваются смежные интервалы Δx, то делители $p_{k_2}(x_1)$ известны из предыдущего расчёта. При рассмотрении интервала Δx впервые вычислительная сложность построения кроны второго уровня будет обусловлена сложностью операций по вычислению $p_{k_2}(x_1)$ и

$p_{k_2}(x_2)$, повторенных k_1 раз, где $k_1 = \frac{3\sqrt[3]{x_2}}{\ln x_2}$. В стандартных обозначениях она будет равна: $T(n) = O(n^{1/3}\log n)$.

Уровень $n = 3$.

Применяются формулы $p_{k_3}(x_2) \le \frac{x_2}{p_{i_1} p_{i_2}}$ и $p_{k_3}(x_1) = p_{k_3}(x_2)\frac{x_1}{x_2}$ с последующим отбором p_{k_3} из интервала $p_1 \le p_i \le p_{m_2}$ по их оценкам. В этой формуле $p_1 \le p_{i_1} \le \sqrt[3]{x_2}$, $\sqrt[3]{x_2} \le p_{i_2} \le \sqrt{p_{m_2}}$, то есть делители p_{i_1} и p_{i_2} не превышают корня из p_{m_2} и, следовательно, выполняется $p_{i_1} p_{i_2} < x_m$.

Если рассматриваются смежные интервалы Δx, то делители $p_{k_3}(x_1)$ и $p_{k_2}(x_1)$ известны из предыдущего расчета. В этом случае оценки вычислительной сложности построения графа $s = 3$ на интервалах Δx и $x \le x_2$ совпадают.

При рассмотрении интервала Δx впервые вычислительная сложность построения кроны третьего уровня графа $s = 3$ будет обусловлена сложностью $T(n) = O(\log^2 n)$ операций по вычислению $p_{k_3}(x_1)$ и $p_{k_3}(x_2)$, повторенных λ_3 раз, где λ_3 равно ω_2-числу ветвей на втором уровне графа.

$$\lambda_3 = \frac{\sqrt{3}\sqrt{x_2}\sqrt[3]{x_2}}{\ln^2 x_2} + \frac{3\sqrt[3]{x_2}}{2\ln x_2}.$$

После исключения постоянных коэффициентов и слагаемых меньшего порядка сложность построения кроны третьего уровня и графа $s = 3$ в стандартных обозначениях будет равна $T(n) = O(n^{5/6})$. Таким образом, произвольное изменение левой границы интервала Δx не усложняет задачу.

4. Оценка сложности алгоритма построения графов второй версии

Задано: $p_1 \le p_i \le p_m$, $i = 1, 2, .., m$, $p_1 = 3$. Установлено: $x_m = p_1 p_m$, $2 \le s \le s_m$, $s_m = \left|\frac{\ln x_m}{\ln p_1}\right|$. Кроны графов построены по условию $p_{i_n} \le p_{i_1}$.

Граф $s = 2$.

Уровень $n = 1$.

Применяется формула $p_{k_1} \le \frac{x_m}{p_1}$, с последующим отбором p_{k_1} из интервала $p_1 \le p_i \le p_m$ по его оценке. Эта операция является единственной.

Уровень $n = 2$.

Применяется формула $p_{i_1}(p_{k_2}) \le \frac{x_m}{p_{k_2}}$ для каждого p_{k_2} из интервала $p_1 \le p_{k_2} \le p^*_{i_1}(2)$ с последующим отбором p_{i_1} из интервала $p_1 \le p_i \le p_m$ по его оценке $p_{i_1}(p_{k_2})$. Сложность операции $p_{i_1}(p_{k_2})$ равна: $T(n) = O(\log^2 n)$. Здесь $p^*_{i_1}(2) \le \sqrt{x_m}$ - максимальное значение p_{k_2}, допускаемое структурой графа. При достаточно больших x_m можно принимать $i_1^*(2) = i_2^m = \frac{2\sqrt{x_m}}{\ln x_m}$. Число операций $p_{i_1}(p_{k_2})$ равно индексу i_2^m.

В итоге вычислительная сложность построения графа $s = 2$ обусловлена применением формулы $p_{i_1}(p_{k_2})$, выполняемой i_2^m раз с последующим отбором p_{i_1} из интервала $p_1 \le p_i \le p_m$. Операция по отысканию $p_{i_1}(p_{k_2})$ имеет вычислительную сложность $T(n) = O(\log^2 n)$. Сложность построения графа $s = 2$ в стандартных обозначениях будет равна: $T(n) = O\left(n^{1/2} \log n\right)$.

Граф $s = 3$.

Уровень $n = 1$.

Применяется формула $p_{k_1} \le \frac{x_m}{p_1^2}$, с последующим отбором p_{k_1} из интервала $p_1 \le p_i \le p_m$ по его оценке. Эта операция является единственной.

Уровень $n = 2$.

Применяется формула $p_{i_1}(p_{k_2}) \le \frac{x_m}{p_{k_2} p_1}$ для каждого p_{k_2} из интервала $p_2 \le p_{k_2} \le p^*_{i_1}(2)$ с последующим отбором p_{i_1} из интервала $p_1 \le p_i \le p_m$ по его оценке $p_{i_1}(p_{k_2})$. Здесь $p^*_{i_1}(2) \le \sqrt{\frac{x_m}{p_1}} = \sqrt{p_m}$ – максимальное значение p_{k_2}, допускаемое структурой графа. При достаточно больши x_m можно принимать $i^*_1(2). = i_2^m = \frac{2}{\sqrt{3}} \frac{\sqrt{x_m}}{\ln x_m}$. Число операций $p_{i_1}(p_{k_2})$ равно индексу i_2^m.

В итоге вычислительная сложность построения кроны второго уровня графа $s = 3$ обусловлена применением формулы $p_{i_1}(p_{k_2})$, выполняемой i_2^m раз с последующим отбором p_{i_1} из интервала $p_1 \le p_i \le p_m$.

Операция по отысканию $p_{i_1}(p_{k_2})$ имеет вычислительную сложность $T(n) = O(\log^2 n)$. Сложность построения кроны второго уровня в стандартных обозначениях будет равна: $T(n) = O\left(n^{1/2} \log n\right)$.

Уровень $n = 3$.

Применяется формула $p_{i_1}(p_{k_3}) \le \frac{x_m}{p_{k_3} p_{i_2}}$ с последующим отбором $p_{i_1}(p_{k_3})$ из интервала $p_1 \le p_i \le p_m$ по его оценке. Число операций равно числу допускаемых структурой графа сочетаний $p_{i_2}\ p_{k_3}$. Значения сочетающихся делителей лежат в пределах $p_2 \le p_{i_2} \le p^*_{i_1}(2)$, $p_2 \le p_{k_3} \le p^*_{i_1}(3)$ Здесь

$p^*_{i_1}(3) \le \sqrt[3]{x_m}$ – максимальное значение p_{k_3}, допускаемое структурой графа. Для достаточно больших x_mможно принимать: $i_1^*(3). = i_3^m = \frac{3\sqrt[3]{x_m}}{\ln x_m}$.

Число сочетаний вида p_{i_2} p_{k_3}в интервале $2 \le i_2 \le i_3^m$ можно представить суммой арифметической прогрессии:

$$\sum_{i_2=2}^{i_3^m}(i_2\text{-}1) = \frac{1 + i_3^m\text{-}1}{2}(i_3^m - 1) = \frac{1}{2}((i_3^m)^2\text{-}i_3^m).$$

В интервале $i_3^m < i_2 \le i_2^m$ число сочетаний зависит от условия $x \le x_m$

и в обозримом виде не выражается. Однако ему можно дать оценку, не снижающую сложность алгоритма. Для этого достаточно считать число сочетаний следующей суммой арифметической прогрессии:

$$S = \frac{i_3^m + 1}{2}(i_2^m\text{-}i_3^m) = \frac{1}{2}\left(i_2^m i_3^m + i_2^m\text{-}i_3^m\text{-}(i_3^m)^2\right).$$

Опуская постоянные множители и члены меньшего порядка в суммах прогрессий , можно оценку числа сочетаний выразить формулой

$$\lambda_3 = i_2^m \cdot i_3^m = \frac{\sqrt{x_m}\sqrt[3]{x_m}}{\ln^2 x_m}.$$

В итоге вычислительная сложность построения кроны третьего уровня графа $s = 3$ обусловлена применением формулы $p_{i_1}(p_{k_3})$,выполняемой λ_3 раз с последующим отбором p_{i_1} из интервала $p_1 \le p_i \le p_m$.

Операция по отысканию $p_{i_1}(p_{k_3})$ имеет сложность $T(n) = O(\log^2 n)$. Сложность построения кроны третьего уровня и графа $s = 3$ в стандартных обозначениях будет равна: $T(n) = O(n^{5/6})$.

5. Оценка сложности алгоритма построения графов второй версии в произвольном интервале чисел

Заданы последовательности простых чисел: $p_1 \le p_i \le p_{m_1}$,

$p_1 \le p_i \le p_{m_2}$, где $p_1 = 3$. Установлено: $x_1 = p_1 p_{m_1}$, $x_2 = p_1 p_{m_2}$,

$$S_{m_1} = \left|\frac{\ln x_1}{\ln p_1}\right|, \quad S_{m_2} = \left|\frac{\ln x_2}{\ln p_1}\right|.$$

Граф $s = 2$.

Уровень $n = 1$.

Применяются формулы $p_{k_1} \le \frac{x_1}{p_1}$ и $p_{k_1} \le \frac{x_2}{p_1}$ с последующим отбором p_{k_1} из интервала $p_1 \le p_i \le p_m$. Эти операции выполняются однократно.

Уровень $n = 2$.

Применяется формула $p_{i_1}(p_{k_2}) \le \frac{x_1}{p_{k_2}}$ для каждого p_{k_2} из интервала $p_1 \le p_{k_2} \le p^*_{i_1}(x_1)$ и формул$p_{i_1}(p_{k_2}) \le \frac{x_2}{p_{k_2}}$для каждого p_{k_2} из интервала $p_1 \le p_{k_2} \le p^*_{i_1}(x_2)$ с последующим отбором p_{i_1} из интервала $p_1 \le p_i \le p_m$ по их оценкам. Здесь $p^*_{i_1}(x_1) \le \sqrt{x_1}$ и $p^*_{i_1}(x_2) \le \sqrt{x_2}$ – максимальные значения p_{k_2}, допускаемые структурой графа на соответствующем интервале чисел.

Их индексы равны: $i_2^m(x_1). = i_1^*(x_1). = \frac{2\sqrt{x_1}}{\ln x_1}$, $i_2^m(x_2). = i_1^*(x_2). = \frac{2\sqrt{x_2}}{\ln x_2}$.

В итоге сложность построения графа на интервале Δx складывается из сложности операции $p_{i_1}(p_{k_2}) \le \frac{x_1}{p_{k_2}}$, повторенной $i_2^m(x_1)$ раз и операции

$p_{i_1}(p_{k_2}) \le \frac{x_2}{p_{k_2}}$, повторенной $i_2^m(x_2)$ раз. Сложность операций $p_{i_1}(p_{k_2})$ равна: $T(n) = O(\log^2 n)$. При достаточно малом Δx оба интервала p_{k_2}, допускаемых структурой, можно считать совпадающими, а числа операций равными.

Если рассматриваются смежные интервалы Δx, то делители $p_{k_3}(x_1)$ и $p_{k_2}(x_1)$ известны из предыдущего расчёта, в котором они были правой границей кроны и обозначались $p_{k_3}(x_2)$ и $p_{k_2}(x_2)$. В итоге оценка вычислительной сложности построения графа $s = 2$ на интервале Δx равна: $T(n) = O\left(n^{1/2}\log n\right)$ и совпадает с оценкой на интервале $x \le x_2$.

Граф $s = 3$.

Уровень $n = 1$.

Применяются формулы $p_{k_1} \le \frac{x_1}{p_1^2}$ и $p_{k_1} \le \frac{x_2}{p_1^2}$ с последующим отбором p_{k_1} из интервала $p_1 \le p_i \le p_m$ по их оценкам. Эти операции выполняются однократно.

Уровень $n = 2$.

Применяется формула $p_{i_1}(p_{k_2}) \le \frac{x_1}{p_{k_2} p_1}$ для каждого p_{k_2} из интервала $p_2 \le p_{k_2} \le p_{i_1}^*(x_1)$ и формула $p_{i_1}(p_{k_2}) \le \frac{x_2}{p_{k_2} p_1}$ для каждого p_{k_2} из интервала $p_2 \le p_{k_2} \le p_{i_1}^*(x_2)$ с последующим отбором p_{i_1} из интервала $p_1 \le p_i \le p_m$ по их оценкам $p_{i_1}(p_{k_2})$. Здесь $p_{i_1}^*(x_1) \le \sqrt{\frac{x_1}{p_1}}$, $p_{i_1}^*(x_2) \le \sqrt{\frac{x_2}{p_1}}$ – максимальные значения p_{k_2}, допускаемые структурой графа на соответствующем интервале чисел. Их индексы равны:

$$i_2^m(x_1) = i_1^*(x_1) = \frac{2}{\sqrt{3}}\frac{\sqrt{x_1}}{\ln x_1}, \quad i_2^m(x_2) = i_1^*(x_2) = \frac{2}{\sqrt{3}}\frac{\sqrt{x_2}}{\ln x_2}$$

Таким образом, вычислительная сложность построения кроны второго уровня графа $s = 3$ на интервале Δx складывается из сложности операции $p_{i_1}(p_{k_2}) \le \frac{x_1}{p_{k_2} p_1}$, выполняемой $i_2^m(x_1)$ раз и операции $p_{i_1}(p_{k_2}) \le \frac{x_2}{p_{k_2} p_1}$, выполняемой $i_2^m(x_2)$ раз. Сложность операций $p_{i_1}(p_{k_2})$ равна: $T(n) = O(\log^2 n)$. При достаточно малом Δx оба интервала делителей p_{k_2}, допускаемых структурой, можно считать совпадающими, а *числа* операций $i_2^m(x_1)$ и $i_2^m(x_2)$ равными.

Если рассматриваются смежные интервалы Δx, то делители $p_{k_2}(x_1)$ известны из предыдущего расчёта, в котором они были правой границей кроны и обозначались $p_{k_2}(x_2)$. В итоге оценка вычислительной сложности построения кроны второго уровня графа $s = 3$ на интервале Δx равна: $T(n) = O\left(n^{1/2}\log n\right)$ и совпадает с оценкой на интервале $x \le x_2$.

Уровень $n = 3$.

Применяется формула $p_{i_1}(p_{k_3}) \le \frac{x_2}{p_{k_3} p_{i_2}}$. Число операций следует считать равным числу возможных сочетаний $p_{i_2} p_{k_3}$ на интервале $x \le x_2$:

$$\lambda_3(x_2) = \frac{2\sqrt{3}\sqrt{x_2}\sqrt[3]{x_2}}{\ln^2 x_2}.$$

Применяется формула $p_{i_1}(p_{k_3}) \le \frac{x_1}{p_{k_3} p_{i_2}}$. Число операций следует считать равным числу возможных сочетаний $p_{i_2} p_{k_3}$ на интервале $x \le x_1$:

$$\lambda_3(x_1) = \frac{2\sqrt{3}\sqrt{x_1}\sqrt[3]{x_1}}{\ln^2 x_1}.$$

При достаточно малом Δx числа операций $\lambda_3(x_2)$ и $\lambda_3(x_1)$ совпадают.

Таким образом, вычислительная сложность построения кроны третьего уровня графа $S = 3$ на интервале Δx складывается из сложности операции $p_{i_1}(p_{k_3}) \le \frac{x_2}{p_{k_3} p_{i_2}}$, выполняемой $\lambda_3(x_2)$ раз и операции $p_{i_1}(p_{k_3}) \le \frac{x_1}{p_{k_3} p_{i_2}}$, выполняемой $\lambda_3(x_1)$ раз. Сложность операций $p_{i_1}(p_{k_3})$ равна: $T(n)=O(\log^2 n)$.

Если рассматриваются смежные интервалы Δx, то делители $p_{k_3}(x_1)$ и $p_{k_2}(x_1)$ известны из предыдущего расчёта. В этом случае оценки вычислительной сложности построения графа $S = 3$ на интервалах Δx и $x \le x_2$ совпадают.

При рассмотрении интервала Δx впервые вычислительная сложность построения кроны третьего уровня графа $S = 3$ будет обусловлена сложностью обеих операций $p_{i_1}(p_{k_3})$, повторенных λ_3 раз, где $\lambda_3 = \omega_2$ - числу ветвей на втором уровне графа.

После исключения постоянных коэффициентов и слагаемых меньшего порядка сложность построения кроны третьего уровня и графа $S = 3$ в стандартных обозначениях будет равна: $T(n) = O(n^{5/6})$. Таким образом, произвольное изменение левой границы интервала Δx не усложняет задачу.

6. Оценка сложности алгоритма составления таблиц факторизаций

Пусть подлежит составлению таблица частичного графа порядка S со стволом p_{i_1}, крона которого построена по условию $p_{i_n} \ge p_{i_1}$. Алгоритм составления таблицы, идентичной графу со стволом p_{i_1}, не зависит ни от ствола ни от порядка графа. Это следует из анализа структуры графа.

Рассматривается ряд нечётных чисел x. Задаётся последовательность простых делителей : $p_1 \le p_i \le p_m$, $i = 1, 2, .., m$, $p_1 = 3$. Устанавливается

интервал чисел $x \le x_m = p_1 p_m$, в которых простые делители не превышают p_m и интервал порядка графов $2 \le s \le S_m$, где $S_m = \left| \frac{\ln x_m}{\ln p_1} \right|$.

В левой колонке таблицы на уровнях $1 \le n \le s-1$ записывается делитель p_{i_1}. На уровне $n=s$ записывается делитель p_{k_s}, отобранный из интервала $p_1 \le p_i \le p_m$ по его оценке $p_{k_s} \le \frac{x_m}{p_{i_1}^{s-1}}$.

В очередной колонке на уровне $n= s-1$ записывается делитель p_{i_1+1}, а на нижележащих уровнях сохраняется делитель p_{i_1}. На уровне $n = s$ записывается делитель p_{k_s}, отобранный из интервала $p_1 \le p_i \le p_m$ по его оценке $p_{k_s} \le \frac{x_m}{p_{i_1}^{s-2} p_{i_1+1}}$.

Делитель p_{k_s}, записанный на уровне $n = s$, следует считать изображающим крону $p_{i_{s-1}} \le p_{i_s} \le p_{k_s}$, опирающуюся на ствол вида $p_{i_1}, \dots, p_{i_{s-1}}$. В таком виде таблица имеет существенно меньший объём. Однако при необходимости она может быть развёрнута повторением этого ствола для всех p_{i_s} данной кроны.

Индекс делителя $p_{i_{s-1}}$ следует повышать после каждого события $p_{i_s} = p_{k_s}$ до наступления события $p_{k_s} < p_{i_{s-1}}$. Это означает, что последнее повышение индекса на уровне $n = s-1$ недопустимо из-за нарушения условия $x \le x_m$. Предыдущие индекс и делитель p_{k_s} сохраняются.

В очередной колонке на уровне $n=S-2$ и выше устанавливается делитель $p_{i_{1+1}}$, то есть $p_{i_{s-2}} = p_{i_{s-1}} = p_{i_{1+1}}$. На нижележащих уровнях сохраняется делитель p_{i_1}.

Описанный выше цикл по отысканию p_{k_s} для возрастающих значений $p_{i_{s-1}}$ выполняется вплоть до наступления события $p_{k_s} < p_{i_{s-1}}$. Последнее влечёт за собой установку делителей $p_{i_{s-2}} = p_{i_{s-1}} = p_{i_1+2}$ и выполнение очередного цикла. Индекс делителя $p_{i_{s-2}}$ следует повышать до наступления события $p_{k_s} < p_{i_{s-1}}$, что означает недопустимость последнего повышения из-за нарушения условия $x \le x_m$. Это повышение отменяется, сохраняется предыдущее и соответствующий ему делитель p_{k_s}.

Следующим этапом построения таблицы будет выполнение всего цикла отыскания p_{k_s} для ствола, в котором $p_{i_{s-3}} = p_{i_{s-2}} = p_{i_{s-1}} = p_{i_1+1}$. Понижение уровня вариаций делителями ствола заканчивается наступлением события $p_{k_s} < p_{i_{s-1}}$ при очередной замене делителя p_{i_2} на уровне $n=2$.

Далее, согласно алгоритму, необходимо варьировать делители на уровне $n=1$. Это означает переход к следующему частичному графу со стволом $p_{i_{1+1}}$. Его таблица может быть построена по тому же алгоритму.

При программировании алгоритма составления таблицы следует иметь в виду следующие его особенности.

1. В основе процесса составления таблицы лежит операция по непрерывному вычислению оценок делителей p_{k_s} и их отбору из заданной последовательности p_i. Операция выполняется при каждой смене опорного делителя $p_{i_{s-1}}$. При этом произведение делителей ствола целесообразно

вычислять умножением базового значения $p_{i_1}^{s-2}$ на очередное значение делителя $p_{i_{s-1}}$.

2. Событие $p_{k_s} < p_{i_{s-1}}$, наступившее при очередном повышении делителя на любом уровне n, означает неприемлемость данного значения p_{i_n} по условию $x \le x_m$ и необходимость ввести в ствол очередное значение делителя на уровне $n-1$. Это значение устанавливается на всех вышележащих уровнях данного ствола.

Таблица для интервала $x_1 < x \le x_2$ строится по алгоритму для $x \le x_2$, но для каждого ствола вида $p_{i_1}, \dots, p_{i_{s-1}}$ вычисляются одновременно делители $p_{k_s}(x_1)$ и $p_{k_s}(x_2)$.

Событие $p_{k_s}(x_2) = p_{k_s}(x_1)$ означает, что крона ствола имеет вид $p_{i_{s-1}} < p_{i_s} \le p_{k_s}(x_1)$, то есть не содержит чисел $x > x_1$ и поэтому исключается из таблицы вместе со стволом.

Событие $p_{k_s}(x_2) > p_{k_s}(x_1)$ означает наличие у данного ствола кроны $p_{k_s}(x_1) < p_{i_s} \le p_{k_s}(x_2)$, которая содержит только числа интервала $x_1 < x \le x_2$. Эта крона существует в стволах с $p_{i_{s-1}} \le p_{k_s}(x_1)$.

Событие $p_{k_s}(x_1) < p_{i_{s-1}}$ означает, что крона данного ствола имеет вид $p_{i_{s-1}} < p_{i_s} \le p_{k_s}(x_2)$ и сохраняет его до события $p_{k_s}(x_2) < p_{i_{s-1}}$, которое влечёт за собой введение в ствол очередного значения $p_{i_{s-2}}$ и установку его на всех вышележащих уровнях. Далее повторяется весь описанный выше цикл.

Таким образом, таблица на уровне $n=s$ в стволах с опорным делителем $p_{i_{s-1}} \le p_{k_s}(x_1)$ наряду с $p_{k_s}(x_2)$ содержит левую границу кроны $p_{k_s}(x_1)$.

В остальных стволах левой границей кроны согласно структуре графа служит опорный делитель $p_{i_{s-1}}$.

Изложенная выше пошаговая процедура составления таблицы графа произвольного порядка позволяет оценить вычислительную сложность её реализации. В процессе составления таблицы применяется только одна формула $p_{k_s} \leq \frac{x_m}{p_{i_1} \ldots\ldots\ldots p_{i_{s-1}}}$. Опорные делители в стволе $p_{i_1} \ldots p_{i_{s-1}}$ замещаются последовательно при переходе к очередному уровню. Это обстоятельство вместе с фактом $p_{i_1} \ldots p_{i_{s-1}} < x_m$ позволяет считать оценкой сложности этой операции $T(n) = O(\log^2 n)$. Число таких операций равно числу параметров p_{k_s} плюс число переходов на нижележащий уровень, когда расчёт p_{k_s} приводит к событию $p_{k_s} < p_{i_{s-1}}$. Ясно, что число переходов равно числу параметров p_{k_n} на уровнях $2 \leq n \leq s-1$.

Таким образом, число параметров p_{k_n}, определяемых при построении графа, сохраняется при составлении таблицы. Однако в алгоритме составления таблицы нет операций по извлечению корней степени до $s-1$ включительно. Этот факт вместе с фактом сохранения числа операций позволяет считать сложность алгоритма составления таблицы равной в первои приближении сложности построения графа: $T(n) = O(n^{5/6})$.

Более точный анализ реализации алгоритма составления таблицы может привести к снижению этой оценки. В связи с этим следует отдать предпочтение применению табличной формы графа.

Заключение

Алгоритмы факторизации в зависимости от сложности делятся на экспоненциальные и субэкспоненциальные. Вычислительная сложность пер-

вых экспоненциально зависит от длины входного параметра, то есть от длины числа в бинарном представлении. Вторые работают за сверх полиномиальное время, но менее чем за экспоненциальное.

Наиболее быстрыми алгоритмами факторизации являются:
метод Ленстры – метод эллиптических кривых со сложностью $L_n\left[1/2, 1\right]$,
метод Померанца – метод квадратичного решета со сложностью $L_n\left[1/2, 1\right]$,
метод Полларда – общий метод решета числового поля со сложностью $L_n\left[1/3, c\right]$, $c = (64/9)^{1/3}$, метод Шенкса – метод квадратичных форм со сложностью $O(n^{1/4})$.

Алгоритмы, время работы которых определяется функциями n, $\log n$, n^2, и $n \log n$, имеющими невысокую скорость роста, также можно считать быстро действующими.

Комбинаторный метод согласно приведенной выше оценке его сложности является экспоненциальным. Его можно отнести к группе алгоритмов, работающих за квазилинейное время $T(n) = O(n \log^k n)$. Одним из близких к нему по сложности можно считать алгоритм сортировки слиянием, работающий за время $T(n) = O(n \log^2 n)$. Как известно, алгоритмы квазилинейного времени работают быстрее любого полинома от n со степенью строго большей единицы.

Однако сравнение комбинаторного метода с существующими будет не корректным, если не иметь в ввиду, что он факторизует не число x_m, а интервал $x \leq x_m$ или любой другой, как угодно малый.

В классической теории алгоритмов рассматриваются проблемы разрешимости различных задач. Вычислительная сложность полученных при этом алгоритмов не исследуется. Она является предметом исследования в теории сложности вычислений. Вычислительная сложность является характеристикой не только(и не столько) природы алгоритма. Её оценка не

всегда является однозначной, ибо существенно зависит от реально существующих вычислительных машин и возможностей программирования. В связи с этим её роль в оценке научной значимости алгоритма постепенно снижается по мере снижения вычислительной беспомощности. Речь идёт о внедрении параллельных и распределённых вычислений и суперкомпьютеров с производительностью, измеряемой в пентафлопсах.

Определяющим фактором при оценке научной значимости алгоритма является не вычислительная сложность, а его новизна, позволяющая объяснить (если не открыть) какие-либо свойства натурального ряда. Ниже приведены преимущества комбинаторного метода, позволяющие оценить степень его научной новизны.

Существующие методы факторизации чисел по своей сути являются методами последовательных испытаний. Комбинаторный метод с помощью простого и прозрачного алгоритма приводит непосредственно к цели.

Алгоритм факторизации комбинаторного метода в определённом смысле слова является универсальным, так как время его выполнения зависит только от размера факторизуемого числа и не зависит от особенностей структуры и свойств числа .

Весь объём вычислений выполняется с привлечением только простых чисел из заданной последовательности. Все вычислительные операции по построению графов однозначны и порождают однозначные следствия. В алгоритме метода применяется только один тест – сравнение ограничивающих делителей между собой.

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.

Проблема программирования процесса построения графов состоит в том и только в том, чтобы с помощью простых формул отыскать оценки ограничивающих делителей в кронах всех уровней графа и по ним выбрать эти делители из заданной последовательности простых чисел.

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

Одним из наиболее значимых следствий комбинаторной факторизации является возможность разложить интервал чисел на подмножества по числу делителей в них. Это позволяет исследовать любое из подмножеств обособленно , ограничиваясь построением только одного графа.

Другим значимым следствием комбинаторной факторизации является возможность выделить подмножества чисел интервала, кратных какому-либо простому делителю. Именно это следствие даёт возможность выделить факторизацию чётных чисел в отдельную проблему.

При составлении таблиц факторизаций с оптимальным выбором шага соотношение числа факторизаций и числа потребных операций получается предельно 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. Последовательность результатов, полученных на множестве смежных и достаточно малых промежутков натурального ряда, выражает собой закон распределения простых чисел.

Комбинаторный метод не конкурирует с существующими методами в решении других проблем, в том числе экзотических типа взлома ключей, имеющих сомнительное отношение к теории чисел. Однако не исключено,

что его алгоритм будет востребован при дальнейшей разработке существующих методов.

Комбинаторный метод решает целочисленную математическую проблему, не прибегая к средствам аналитической теории чисел, что заслуживает особого внимания. В ряде случаев элементарными методами достигаются результаты, пока недоступные аналитическим средствам. Элементарные методы имеют очевидное методическое значение и часто дают простой и естественный взгляд на полученные результаты и на причины их вызывающие.

Литература

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

2. Бондаренко П.С. Теория вероятностей и математическая статистика: учебное пособие/ П.С. Бондаренко, Г.В. Горелова, И.А. Кацко; под ред. И.А. Кацко, А.И. Трубилина. Москва: КНОРУС, 2017. – 390 с. – (Бакалавриат).

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

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

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

6. 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. Bondarenko P.S. Teoryia veroyatnostey i matematicheskaya statistika: uchebnoe posobie/ P.S.,Bondarenko, G.V.Gorelova, I.A. Katchko, pod redakciej I.A. Katchko, A.I. Troubilina. Moskva: KNORUS, 2017. – 390 c. – (Bakalavriat).

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

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

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

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