УДК 511; 519.6

А.Е. Ваулин, М.С. Назаров

СВЕДЕНИЕ ЗАДАЧИ ФАКТОРИЗАЦИИ НАТУРАЛЬНОГО ЧИСЛА К ЗАДАЧЕ РАЗБИЕНИЯ ЧИСЛА НА ЧАСТИ. ЧАСТЬ 1

Ваулин А.Е., Назаров М.С. **Сведение задачи факторизации натурального числа к задаче разбиения числа на части. Часть 1.**

Аннотация. В настоящей работе рассматриваются вопросы разработки алгоритмов факторизации составных натуральных чисел. Анализ возможностей существующих алгоритмов показывает, что в перспективе ближайших десятилетий существенного прогресса в повышении их быстродействия ожидать не приходится. Дело, по-видимому, в ограниченности одностороннего математического подхода, базирующегося на использовании математических решет. Автором предлагается иной подход, основанный на изучении внутренней структуры натурального ряда чисел и использовании свойств чисел, не зависящих от их разрядности (по типу признаков делимости).

Ключевые слова: натуральный ряд, нечетное число, ф-инвариант числа, разбиения числа, контур натурального ряда чисел.

Vaulin A.E., Nazarov M.C. **Conversion of Integer Factorization to a Problem of Decomposition of a Number. Part 1.**

Abstract. The development of factorization mechanisms of composite integer numbers is considered in this work. The existent methods will not become more rapid and efficient in the nearest decade, due to narrow and inadequate mathematical approach to solution of this problem, which is based on so-called sieve of Eratosthenes. The mechanism suggested by author of this work, uses a completely new method based on examination of internal structure of natural sequence and application of digit place independent features (the criterion for divisibility).

Keywords: natural number, odd number, f-invariant of a numbers, partitions of a number, time-beating, natural numbers circuit.

1. Введение. В работе анализируются возможности факторизации больших натуральных чисел, и показывается необходимость разработки новых методов решения этой задачи за приемлемые для практических нужд временные интервалы. В общей постановке проблема факторизации является проблемой теории чисел, так как среди арифметических операций этой теории отсутствует операция факторизации натурального числа [8–12], которая удовлетворяла бы запросам науки и общественной практики.

Обращается внимание на исключительно важную роль нечетных натуральных чисел на их свойства и особенности. Показывается, что алгоритмы факторизации сегодняшнего уровня развития теории самым тесным образом связаны со свойствами чисел, зависящими от разрядности факторизуемых чисел. Такая зависимость не позволяет создать быстродействующие алгоритмы факторизации [2–7]. В работе предлагается опираться на свойства чисел свободные от такой зависи-

мости, и разработать алгоритмы свободные от нее. О существовании таких свойств свидетельствуют известные признаки делимости.

В работе намечается путь ослабления и даже полного устранения связи, определяющей длительность выполнения факторизации с разрядностью числа. С этой целью используются новые установленные свойства нечетных натуральных чисел (ННЧ), не зависящие от их разрядности. Длительность вычислений при этом требуется существенно меньшая и слабо зависит от разрядности числа.

Приводятся описания двух моделей ННЧ: *интервальной* и *нумерационной*, а также показывается, как используются понятия модели натурального ряда чисел.

На основе нумерационной модели и теоремы о предельном контуре [4] разработан алгоритм факторизации произвольных ННЧ, использующий формирование разбиения (представление суммой номеров контуров) половины номера $k_п(N)/2$ предельного контура числа N. Поскольку значение $k_п(N)/2$ – ограниченное число, и возможности его представления суммой подряд следующих чисел конечны, то отсюда следует конечность алгоритма и его сходимость. Числовые примеры иллюстрируют основные понятия моделей, их взаимосвязи и демонстрируют работоспособность предлагаемых методов.

Приводится возможный алгоритм факторизации числа, использующий связь кубов чисел и сумм ННЧ, легко вычисляемых в рамках модели натурального ряда чисел (НРЧ).

Формула, описывающая интервал длиной N, расстоянием между граничными точками интервала (между квадратами), реализует разложение числа N на множители, т.е. реализует его факторизацию.

Изложение материала сопровождается многочисленными ссылками на публикации и числовыми примерами, призванными сделать его более ясным и доступным.

2. Проблема факторизации больших чисел. В теории чисел (высшей арифметике) настоящего времени отсутствует простая и доступная операция (факторизация) обратная умножению чисел – разложение составного числа на множители. Отдельные числа большой, но ограниченной разрядности с большими трудностями удается разложить квалифицированным специалистам, но в принципе задача сегодня из разряда нерешаемых.

Задача факторизации известна с древнейших времен, как задача разложения натурального числа на простые множители, но до настоящего времени она не получила практически полезного результативного разрешения. Самыми известными результатами на сегодняшний день в области создания метода решения задачи факторизации боль-

ших чисел (ЗФБЧ) следует признать методы и алгоритмы различных математических решет. Теория решет берет свое начало от решета Эратосфена (до н.э.), позднее придуманы решета Бруна, Сельберга, Линника, а последнее достижение – это решето с числовым полем, предложенное в 1990 году Х.В. Ленстра, А.К. Ленстра, Манассе и Поллардом.

В лучших традициях 17 века, когда отдельные математики (Ферма, Мерсенн и др.) формулировали математические задачи и в личной переписке предлагали их для решения коллегам за рубежом и в своей стране, поступила фирма RSA.

Фирма в 1991 году представила на своем сайте в интернете список из 42 чисел [10], которые предложила факторизовать любому желающему, испытать свои силы и возможности на этом поприще. Достижения человечества в решении задачи факторизации хорошо иллюстрируются данными таблицы 1.

Таблица 1. Достижения в области факторизации больших чисел, список которых объявлен фирмой RSA в 1991году

Число	Количество десятичных цифр	Стоимость	Дата факторизации
RSA – 100	100		Апрель 1991
RSA – 110	110		Апрель 1992
RSA – 120	120		Июнь 1993
RSA – 129	129	$100	Апрель1994
RSA – 130	130		Апрель 10, 1996
RSA – 140	140		Февраль 2, 1999
RSA – 150	150		Апрель 16, 2004
RSA – 155	155		Август 22, 1999
RSA – 160	160		Апрель 1, 2003
RSA – 200	200		Май 9, 2005
RSA – 576	174	$10 000	Декабрь 3, 2003
RSA – 640	193	$20 000	Ноябрь 4, 2005
RSA – 704	212	$30 000	–
RSA – 768	232	$50 000	Январь 2010
RSA – 896	270	$75 000	–
RSA – 1024	309	$100 000	–
RSA – 1536	463	$150 000	–
RSA – 2048	617	$200 000	–

Для подкрепления интереса к поиску решений заданий из списка фирма назначила премии за правильно найденное решение для отдельных чисел. Таблица 1 содержит 18 чисел из этого списка RSA. Часть чисел этого списка уже факторизована, но с момента опубликования прошло уже более 20 лет.

Видим, что за 20 с небольшим лет лучшими математиками преодолен рубеж факторизации для конкретного числа только из 232 десятичных цифр. Другое число такой же разрядности потребует для факторизации не намного меньшее время. Заметим также, что каждое из чисел списка формировалось как произведение всего лишь двух простых чисел практически одинаковой разрядности. Эта дополнительная информация, возможно, способствует поиску решения.

По-видимому, алгоритмы, используемые математиками для факторизации, существенным образом зависят от разрядности факторизуемого числа. Такой вывод следует из рассмотрения таблицы. За меньшее время (исчисляемое в годах) были разложены числа меньшей разрядности. Использование мультипликативной модели числа приводит к огромному перебору вариантов, хотя такой перебор, конечно же, не является тотальным. Размер области поиска решения с течением времени (в годах) очень медленно сокращается.

В предлагаемой работе рассматривается другой, оригинальный подход к решению задачи факторизации, который опирается на модели натурального ряда чисел в целом и отдельного натурального числа.

Исключительно важную роль в рассматриваемом подходе играют некоторые теоремы, натуральные нечетные числа и, в частности, последовательности нечетных чисел, для которых вводятся классы.

Теорема (*Основная теорема арифметики*):

Каждое целое число, неравное нулю, представляется произведением степеней простых чисел единственным образом с точностью до порядка сомножителей и их знаков

$$\boldsymbol{n} = \prod_{i} \boldsymbol{p}_i^{\boldsymbol{\alpha}_i} = \boldsymbol{p}_1^{\boldsymbol{\alpha}_1} \boldsymbol{p}_2^{\boldsymbol{\alpha}_2} \ldots \boldsymbol{p}_k^{\boldsymbol{\alpha}_k} \ .$$

Эта формула представляет каноническое разложение числа $\boldsymbol{n}$ на сомножители.

В основной теореме арифметики выделяют два утверждения, требующие доказательства. Во-первых, утверждение о существовании представления всякого целого числа произведением степеней простых чисел, и во-вторых, утверждение о единственности такого представления. Доказательства обоих утверждений приводятся практически во всех руководствах и учебниках по теории чисел. Результат этой теоремы достигается для произвольного числа процедурой факторизации.

Теорема (Факторизация натуральных чисел): Произвольное составное натуральное число $\boldsymbol{N}$ может быть представлено произведением чисел (факторизовано) путём последовательного выполнения над ним следующих преобразований:

1. Если N – составное чётное натуральное число, то оно представляется в виде $N = 2^{t_2} \cdot p_2$,

где $p_2 \equiv 1 (\mathrm{mod}\ 2)$ – нечётное число, $t_2 = 1(1)\ldots$, и $2 \nmid p_2$;

2. Если $N = p_2$ – нечётное число, оканчивающееся цифрой **5**, то оно представляется в виде $N = 5^{t_5} \cdot p_5$, где p_5 – нечётное число, $t_5 = 1(1)\ldots$; и $5 \nmid p_5$;

3. Если $N = p_5$ - нечётное число, оканчивающееся одной из цифр **1, 3, 7, 9**, а его свёртка $s(N)$ (сумма цифр) кратна числу **3**, то оно представляется в виде $N = 3^{t_3} \cdot p_3$,

где p_3 – нечётное число, $t_3 = 1(1)\ldots$; и $3 \nmid p_3$;

4. Если $N = p_3$ - нечётное число, оканчивающееся одной из цифр **1, 3, 7, 9**, то оно имеет вид $N = p_k + 30 \cdot t$, где t – натуральное число, а $p_k \in \{7, 11, 13, 17, 19, 23, 29, 31\}$, и факторизацию можно выполнить, например, с использованием теоремы о предельном контуре.

Поскольку делители составного нечетного натурального числа (СННЧ) – это натуральные числа, то, по-видимому, можно предположить, что сами делители некоторого натурального числа $N = d_м\ d_м = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$ и их кратные значения некоторым образом распределены в натуральном ряде чисел. Эти числа (делители и кратные им) содержат информацию о делителях N. Очевидно, что кратных значений может быть бесконечно много, но практически в работе будут использоваться только меньшие N значения. Будем далее рассматривать задачу факторизации СННЧ N.

Возможны несколько вариантов информированности исследователя задачи относительно делителей N.

Один вариант – все (возможно, кроме одного) делители N известны. Делением N на все делители определяется и неизвестный последний делитель.

Другой вариант – неизвестны несколько делителей N. Остающиеся неизвестными делители могут быть определены делением исходного N на все известные делители. Если таким путем не все делители определяются, то задача сводится к факторизации составных меньших N чисел, определенных при предварительных делениях числа N на известные делители.

3. Аддитивная и мультипликативная формы представления чисел. Общий замысел нового подхода к задаче факторизации чисел состоит в следующем. В соответствии с теоремой факторизации этой процедуре подвергаются составные нечетные натуральные числа.

Аддитивная форма таких чисел – это сумма нечетного числа слагаемых, которые представляют собой непрерывный фрагмент последовательности нечетных чисел в НРЧ. Эта сумма, начиная с первого нечетного числа в ней, формируется далее нечетными числами, возрастающими всегда на две единицы. Для числа N могут существовать несколько различных сумм в разных областях (местах) НРЧ.

Пример 1. Пусть $N = 105$, тогда $N = 9+11+13+15+17+19+21 = 17+19+21+23+25 = 33 + 35 + 37 = 105$ представляется тремя различными нетривиальными суммами, а четвертая – тривиальная образована одним слагаемым N.

Далее, известно, что в НРЧ между квадратами последовательных чисел разности равны последовательным нечетным числам, которые могут описываться границами интервалов левой $\Gamma_л(N)$, и правой $\Gamma_п(N)$, соответствующих этим нечетным числам. Границы при этом всегда являются полными квадратами $N = \Gamma_п(N) - \Gamma_л(N)$.

Пример 2. Для сумм, представляющих $N = 105$, имеем (в кавычках записываются слагаемые сумм равные разностям указанных квадратов смежных чисел, имеющих разную четность):

4^2 «9» 5^2 «11» 6^2 «13» 7^2 «15» 8^2 «17» 9^2 «19» 10^2 «21» 11^2 или 8^2«17»9^2«19»10^2«21»11^2«23»12^2«25»13^2 или 16^2«33»17^2«35»18^2«37»19^2.

Мультипликативная форма чисел – это представление произведением разности квадратов границ интервала, соответствующего N и сформированного отрезком последовательности нечетных чисел. Если рассматривать суммы для $N = 105$, как интервалы (расстояния) между внешними границами крайних слагаемых в каждой из трех сумм примера *1*, то получим представление числа $N = 105$ мультипликативной формой.

Пример 3. Выпишем мультипликативное представление квадратами: $11^2 - 4^2 = 13^2 - 8^2 = 19^2 - 16^2 = 105$ или в скобочном виде $105 =(11 - 4)\cdot(11 + 4) =7\cdot15 = (13 - 8)\cdot(13 + 8) = 5\cdot21= (19 - 16)\cdot(19 +16) = 3\cdot35$.

Представление N в такой форме как раз и обеспечивает разложение составного нечетного числа N на два нечетных сомножителя, из которых либо один, либо оба могут оказаться составными, либо, что случается более редко – оба простые числа.

Каждый полученный составной нечетный фактор можно подвергнуть далее такой же процедуре представления в аддитивной и мультипликативной форме.

Так необходимо действовать до получения в качестве всех факторов числа N только простых чисел.

Представляется, что рассмотренная алгоритмическая схема обработки составного нечетного числа N весьма слабо зависит от раз-

рядности N и сам процесс факторизации для больших, очень больших и малых чисел будет занимать практически одинаковое время, исчисляемое секундами или их долями при компьютерной обработке.

Таков общий замысел предлагаемого нового подхода к решению проблемы факторизации чисел. Реализация описанного процесса на практике встречает определенные трудности, преодоление которых возможно несколькими путями. Один из таких путей и рассматривается далее в работе. Необходимо осознать, что существующие на сегодняшний день практика и подходы к решению задачи факторизации больших чисел – это по существу путь «проб и ошибок», который ориентирован на использование свойств чисел, жестко зависящих от их разрядности. Чем больше разрядность числа, тем большее время требуется для его факторизации.

Существенное сокращение времени ожидается в алгоритмах факторизации, использующих свойства чисел, не зависящие от их разрядности. Такие свойства существуют и даже практически используются, например, признаки делимости чисел. Число N делится на три, если на три делится сумма (свертка) его цифр, доведенная до одной цифры. Факторизация таких чисел, описываемых сотнями и тысячами цифр, занимает секунды.

Пример 4. Пусть $N = 123456789$. Тогда сумма цифр фрагмента НРЧ $1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 45 \rightarrow 4 + 5 = 9 = 3 \cdot 3$.

Если число N имеет в записи сотни или даже тысячи цифр, то их сумма находится очень быстро и время ее вычисления слабо зависит от разрядности числа. Отсюда следует, что необходимо найти и использовать свойства чисел, не зависящие от их разрядности. Одно из таких свойств (ф-инвариант) числа используется для разработки алгоритма факторизации и позволяет преобразовать задачу факторизации в другую задачу – формирования разбиений специального вида для заданного числа N. Процедура такого преобразования (сведения) и рассматривается в предлагаемой работе.

Рассмотрим рисунок 1. На числовой оси x выделены четыре точки 2^2, 15^2, 110^2 и 111^2, в которых размещены квадраты натуральных чисел. Интервал между левой (первой) парой точек $15^2 - 2^2 = 221$ совпадает с интервалом между второй парой точек $111^2 - 110^2 = 221$. Если необходимо найти значения делителей меньшего $d_м$ и большего $d_б$ числа $N = 221$, то можно воспользоваться формулой сокращенных вычислений, а именно:

$$N = x_1^2 - x_o^2 = (x_1 - x_o)(x_1 + x_o) = d_м \cdot d_б,$$

где, в частности, для правой пары неизвестные переменные x_o и x_1 могут определяться выражениями:

$$x_o = (N - 1)/2 = 110,\ x_1 = (N + 1)/2 = 111,$$

и являются смежными натуральными числами, между квадратами которых лежит исследуемое число ***221.***

Подставляя вычисленные значения в формулу $N = (x_1 - x_o)(x_1 + x_o) = (111 - 110)(111 + 110) = 1 \cdot 221$, получаем делители меньший $d_м = 1$ и больший $d_б = 221$. Это тривиальное разложение, но, оказывается, существует еще пара квадратов, которая приводит к другому разложению числа $N = 221$ на множители, а именно:

$$N = (x_1 - x_o)(x_1 + x_o) = d_м \cdot d_б = (15 - 2)(15 + 2) = 13 \cdot 17,$$

которое является окончательным решением, так как оба делителя – простые числа.

Как видим, разрядность чисел нигде и никак себя не проявила. Проблема заключается в получении пар альтернативных чисел-квадратов разной четности, между которыми лежит факторизуемое число ***N***.

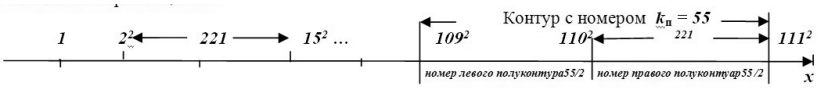

Рис. 1. Положение в НРЧ интервалов длиной $N = 221$ с квадратами в качестве границ

Тривиальный случай разложения здесь рассмотрен не зря. Именно он создает отправной посыл для разработки нового направления в решении проблемы факторизации больших чисел. Положение числа со значением $N = 221$ на числовой оси можно представлять отрезками НРЧ длиной из ***221*** позиции, среди которых только два отрезка будут с граничными позициями, содержащими полные квадраты. В результате изучения проблемы обнаружена такая характеристика нечетного числа (НЧ) и соответствующего ему интервала, которая является инвариантом интервала с границами-квадратами и длиной равной числу ***N*** независимо от того, где этот интервал на числовой оси размещается.

Известно, что любое натуральное нечетное число лежит между квадратами чисел. Тривиальное разложение на множители всегда позволяет указать пару квадратов для смежных чисел разной четности и числовую характеристику отрезка для числа, остающуюся неизменной при допустимых смещениях отрезка вдоль числовой оси. Допустимыми являются положения интервала длиной ***N*** , концы которого размещаются в точках квадратах натурального ряда чисел. Таких допустимых положений для интервала, соответствующего числу ***N***, тем больше, чем больше у ***N*** делителей. Сама эта характеристика представляет собой комбина-

торное разбиение со специальными свойствами некоторого другого (не ***N***) постоянного числа, зависящего от факторизуемого ***N***. В разбиении числа-константы, представляемого суммой меньших чисел, все слагаемые различаются на ***1*** кроме крайнего в сумме, от которого в сумму включается лишь половина слагаемого. Для рассматриваемого примера существует единственное допустимое смещение тривиального интервала длиной ***N = 221***, которое и изображено на рисунке 1. Оба этих интервала характеризуются одним разбиваемым числом-константой (ф-инвариантом), равным половине числа ***55.*** Ниже приводится представление константы в форме специального разбиения:

$$55/2 = 27.5 = ½ + 2 + 3 + 4 + 5 + 6 + 7.$$

4. Два специальных разбиения натурального числа *N*. Будем рассматривать задачу о разбиении натурального числа. Разбиением натурального числа ***N*** называется конечная невозрастающая последовательность натуральных чисел $k_0, k_1, k_2, k_3, \ldots, k_t$, меньших ***N***, для которой $N = \sum_i^t k_i$, числа k_i называются блоками (частями) разбиения. Разбиения чисел бывают на нечетные и отдельно на четные части, а также упорядоченными и неупорядоченными [12]. Существуют разбиения чисел разбиения чисел на одинаковые и различные части и т.п.

Для наших целей будем использовать графическое представление *специальных разбиений* чисел на разные части. Специфика разбиений связана с ограничением на отличие ($\Delta = 1$) одной части разбиения от другой и в том, что крайняя часть (меньшая или большая) в сумме равна половине слагаемого, удовлетворяющего ограничению:

$$k_t - k_{(t-1)} = \ldots = k_3 - k_2 = k_2 - k_1 = k_1 - k_0 = 1,$$

для чего воспользуемся точечным графом Феррера**.**

Далее будем использовать зависимости для целочисленных рядов [1]:

– сумма ***n*** натуральных чисел:

$$1 + 2 + 3 + \ldots + n - 1 + n = n(n+1)/2 = C_{n+1}^2,$$

– сумма ***n*** натуральных чисел, где последнее слагаемое равно ***n/2***, (вариант специального разбиения):

$$1 + 2 + 3 + \ldots + n - 1 + n/2 = n^2/2;$$

– сумма ***n*** нечетных натуральных чисел:

$$1 + 3 + 5 + \ldots + (2n - 3) + (2n - 1) = n^2.$$

В задаче разбиения числа, связываемой с задачей факторизации, имеют дело с *двумя специальными случаями* разбиений не самого числа N, а его ф-инварианта, числа $k_п(N)/2$, т.е. половины номера предельного контура для N. Кроме того, будем различать разбиения числа $k_п(N)/2$, соответствующие целым и дробным числам, а также соответствующие *левым* ($N_л$) и *правым* ($N_п$) *натуральным нечетным числам*.

Графическое представление (см. таблица 2) множества разбиений чисел $k_п(N)/2$ имеет вид трапеции как составной части треугольной точечной диаграммы Феррера, образованной из ее подряд следующих строк. Такая трапеция вкладывается в треугольную диаграмму. Одно из оснований трапеции (верхнее или нижнее) всегда включает в сумму разбиения только половину своих точек.

Основная специализация рассматриваемых здесь двух типов разбиений заключается в том, что отличие частей разбиения числа одной от другой составляет лишь единицу ($\Delta = 1$), и только крайние части (строки основания трапеции графического представления) разбиения числа могут отличаться от соседних на величину большую, чем единица. Крайняя строка (верхняя для $N_л$, нижняя для $N_п$) всегда разбивается пополам. Если разбиваемая пополам строка содержит четное число точек, то все части разбиения числа N – целые числа, если число точек в такой строке нечетное, то крайняя часть разбиения – дробное число.

Отметим также некоторые другие особенности этих специальных разбиений. Эти особенности легко и наглядно воспринимаются при рассмотрении числовых примеров, которые и составляют основное содержание работы.

Все различные слагаемые в сумме разбиений ф-инварианта для числа N, кроме одного крайнего слагаемого, всегда отличаются на единицу, т.е. это числа k_i, следующие в натуральном ряде одно за другим:

$$k_п(N)/2 = \sum_{i=p}^{t} k_i \pm k/2,$$

где p – индекс номера начального (меньшего) контура;

t – индекс номера конечного (большего) контура;

$\pm$ – знак в сумме определяется видом (левое $k > k_t$, правое $k < k_p$) числа N;

k – номер крайнего контура (без индекса), от которого в сумме участвует только половина номера.

Тот факт, что сумма в специальном разбиении числа $k_п(N)/2$ формируется натуральными числами, возрастающими на 1, имеет ре-

шающее значение для нумерационной модели натурального числа. Все разбиения такого типа (все суммы $k_n(N)/2$) оказываются представленными в треугольной точечной диаграмме Феррера (графического представления разбиения числа) и могут быть получены из нее.

Во-первых, для N_n (правого нечетного числа) представление половины номера предельного контура (числа $k_n(N_л)/2$) разбиением всегда сформировано различными слагаемыми (частями), причем от от меньшего контура в сумму включается только половина его номера.

Во-вторых, для $N_л$ (левого нечетного числа) представление половины номера предельного контура (числа $k_n(N_л)/2$) разбиением всегда сформировано различными частями, если $k_n(N_л)/2$ – дробное число.

В-третьих, для $N_л$, если $k_n(N_л)/2$ – целое, то два слагаемых в сумме могут совпадать, причем, одно слагаемое из такой пары – это половина номера большего контура в сумме.

В-четвертых, все слагаемые во всех суммах – это интервалы позиций НРЧ, в которых крайние позиции заняты квадратами целых чисел. Поясним эти понятия числовыми примерами.

В средней части таблицы помещено графическое разбиение числа ***231*** на разные части (строки с точками), отличающиеся одна от другой на единицу. Для нечетных натуральных чисел N в пределах первой тысячи на основе этой диаграммы может быть проведена факторизация их на два фактора. Первые четыре колонки таблицы содержат характеристики интервальной модели (характеристики контуров). Колонка справа от точечной диаграммы – номера контуров. Две последние колонки – характеристики нумерационной модели. Уровнем названа n-я снизу строка таблицы. Значения характеристики в строках приведены с нарастанием от нижней строки вверх. В последнем столбце суммы точек из предшествующих строк суммируются с половиной количества точек текущей строки. В предпоследнем столбце суммы точек полных строк.

Для левых $N_л$ чисел такие суммы $k_n/2$, соответствующие интервалам длины $N_л$ **,** всегда содержат определенное число точек и строк из треугольника и в верхней части лишь половину количества точек строки. Очевидно, если зафиксировать строку из суммы, которой соответствует значение равное $k_n/2$ или ближайшее большее, но также содержащее половину верхней строки, то для решения о номере нижней строки в сумме остается определить только номер нижнего (меньшего) контура или соответствующей строки, формирующей сумму $k_n/2$**.** Это значение определяется разностью между суммой точек для уровня фиксированной верхней строки и значением $k_n/2$**.** Если такая разность

присутствует в рассматриваемой колонке, то строка ей соответствующая, и строки ниже нее не учитываются в сумме.

Приведем таблицу 2 с такой диаграммой, сопроводив ее дополнительными сведениями об интервальной и нумерационной моделях числа N.

Таблица 2**.** Характеристики интервальной и нумерационной моделей числа N

Интервальная модель N				Диаграмма Феррера	Нумерационная модель N		
Правая граница контура	Средняя точка контура	Левая граница контура	Длина контура с №k	Графическое разбиение половины номера предельного контура $k_п$	Номер контура k	Сумма точек C^2_{n+1} уровня	Значение $k^2/2$ для уровня
1849	1764	1681	168	°°°°°°°°°°°°°°°°°°°°	21	231=21·11	220.5
1681	1600	1521	160	°°°°°°°°°|°°°°°°°°°	20	210=21·10	200
1521	1444	1369	152	°°°°°°°°°°°°°°°°°	19	190=19·10	180.5
1369	1296	1225	144	°°°°°°°°°|°°°°°°°°°	18	171=19·9	162
1225	1156	1089	136	°°°°°°°°°°°°°°°°	17	153=17·9	144.5
1089	1024	961	128	°°°°°°°°|°°°°°°°°	16	136=17·8	128
961	900	841	120	°°°°°°°°°°°°°°	15	120=15·8	112.5
841	784	729	112	°°°°°°°|°°°°°°°	14	105=15·7	98
729	676	625	104	°°°°°°°°°°°°	13	91=13·7	84.5
625	576	529	96	°°°°°°|°°°°°°	12	78=13·6	72
529	484	441	88	°°°°°°°°°°	11	66=11·6	60.5
441	400	361	80	°°°°°|°°°°°	10	55=11·5	50
361	324	289	72	°°°°°°°°°	9	45=9·5	40.5
289	256	225	64	°°°°|°°°°	8	36=9·4	32
225	196	169	56	°°°°°°°	7	28=7·4	24.5
169	144	121	48	°°°|°°°	6	21=7·3	18
121	100	81	40	°°°°°	5	15=5·3	12.5
81	64	49	32	°°|°°	4	10=5·2	8
49	36	25	24	°°°	3	6=3·2	4.5
25	16	9	16	°°	2	3=3·1	2
9	4	1	8	°	1	1=1·1	0.5

Поиск разности $C^2_{k+1} - k_п/2$ начинаем от значения $C^2_{k+1} > k_п/2$, а вычисленную разность сравниваем с $k^2/2$, до тех пор, пока они не совпадут. При несовпадении увеличиваем значение k.

Пример 5. (*Возникновение равных слагаемых в специальном разбиении*). Задано СННЧ $N = 119$, это число левое, так как сравнимо $119 \equiv 3 (\mathbf{mod} 4)$ с тройкой**.** Предельный контур для этого числа имеет длину $L(119) = 119 + 121 = 240$. Номер предельного контура равен $k_п(119) = 240/8 = 30.$ Значение ф-инварианта для числа 119 равно $k_п(119)/2 = 30/2 = 15.$ Специальное разбиение этого ф-инварианта имеет вид $15 = 3 + 4 + 5 + 6/2 = 3 + 4 + 5 + 3.$ В итоговой сумме все

слагаемые (кроме последнего) отличаются от соседних на $\Delta = 1$, и получились два одинаковых слагаемых, равных тройке. Чтобы убедиться, что разбиение ф-инварианта приводит к факторизации числа $N = 119$, восстановим N по разбиению, все слагаемые которого (кроме последнего) – это номера контуров. Последнее слагаемое 3 – номер полуконтура 6-го контура.

Умножаем слагаемые на $8: 3\cdot 8 + 4\cdot 8 + 5\cdot 8 + 6\cdot 8 = 24 + 32 + 40 + 48$. Последнее (большее равное 48) слагаемое должно давать в сумму только свой левый (меньший) полуконтур $23+25 = 48$, т.е. число 23. Итак, устанавливаем длину интервала для $N = 119$ (проверяем: $24+32+40+23 = 119$).

Остается вспомнить, что границами контуров и полуконтуров в НРЧ всегда являются квадраты целых чисел и получить их крайние значения у крайних слагаемых интервала:

– меньшая граница интервала $\Gamma_л(119) = \Gamma_л(3)$ – это левая граница для контура с номером 3,

$$\Gamma_л(3) = (2\cdot 3 - 1)^2 = 25 = 5^2,$$

– большая граница интервала $\Gamma_п(119) = \Gamma_ц(6)$ – это правая граница для левого полуконтура с номером

$$6/2 = 3, \Gamma_ц(6) = (2\cdot 6)^2 = 144 = 12^2.$$

Последний штрих: число $N = 119$ представляем расстоянием между границами интервала, т.е.

$\Gamma_п(119) - \Gamma_л(119) = \Gamma_ц(6) - \Gamma_л(3) = 12^2 - 5^2 = (12 - 5)(12 + 5) = 7\cdot 17 = 119$

и получаем разложение N на множители.

5. Две модели натурального числа. Представим числовую ось, размеченную точками $x, x+1, x+2 \ldots,$ пронумерованными числами натурального ряда, начиная от единицы. Вдоль этой оси перемещается движок с окошком (по типу логарифмической линейки), вмещающим N точек от точки с меньшим значением x_o, до точки с большим значением x_1 (натуральных чисел, нумерующих точки). Решение задачи факторизации можно представить следующим механизмом.

Перемещаем движок вдоль числовой оси так, чтобы крайние точки окна (x_1, x_o) в движке совпали с целыми квадратами разметки на оси. Такая ситуация достижима всегда для любых нечетных натуральных N, даже, если N простое число. Для ННЧ квадраты будут иметь разную четность, которая определяется для x_1 и x_o однозначно.

Для простого N задача решается исключительно просто, хотя в отличие от составных N, для простого числа существует лишь единственный вариант требуемого положения движка. Дело в том, что числа,

квадраты которых должны совпасть с крайними точками окна, всегда для нечетного простого числа соседние: одно четное, другое – нечетное $x_o = (N - 1)/2$, $x_1 = (N+ 1)/2$.

Действительно, квадраты этих чисел удовлетворяют задаче разложения на множители для любых N:

$$N = x_1^2 - x_o^2 = (x_1 - x_o)(x_1 + x_o) = 1 \cdot N.$$

Формальное решение задачи факторизации числа N получено, но, как следовало ожидать, оно тривиальное.

Для составных чисел N имеется два и/или более варианта положения движка на числовой оси, удовлетворяющих условиям задачи. Каждый вариант соответствует различным разложениям числа N на множители. Алгоритм решения задачи факторизации числа может обеспечивать получение одного нетривиального решения, после чего он, может быть применен, многократно повторяясь, но уже к найденным делителям (факторам), до полного разложения числа N на простые множители.

Таким образом, основная проблема заключается в нахождении нужного положения движка с «окном».

В основе сведения одной из названных в заголовке задачи к другой лежит принцип представления отдельного натурального числа моделью интервала числовой оси и представления моделью всего натурального ряда чисел нумерованными контурами. Из основной теоремы факторизации следует, что факторизации необходимо подвергать только отдельные трудно факторизуемые нечетные числа, поэтому далее кратко рассматриваются модели именно для таких чисел. Приведем некоторые понятия модели НРЧ.

Контуром (интервалом числа) в НРЧ называется непрерывное множество позиций, занимаемых последовательными натуральными числами, из которых меньшее является квадратом нечетного числа, а большее предшествует следующему по величине нечетному квадрату. Среди чисел контура обязательно присутствует один квадрат четного числа, лежащий между квадратами нечетных смежных чисел, формирующими границы контура. Длина (число позиций) любого контура кратна числу восемь. Таким образом, нечетные квадраты делят НРЧ на контуры, которые образованы всегда только двумя смежными ННЧ, разделяемыми четным квадратом.

Все контуры в НРЧ получают порядковые номера k, равные длине контура $L(k)/8$ поделенной на восемь.

Полуконтуром НРЧ называется часть контура (левая или правая), лежащая между квадратами чисел разной четности. Длины левого

и правого полуконтуров в одном контуре различаются на две единицы. Полуконтуры не снабжаются специальными номерами, но поскольку они нечетные числа, то для каждого из них легко определяется его порядковый номер в НРЧ. Пусть нечетное число $N = 2n - 1$, где $n = 0(1)\ldots$ – порядковый номер числа, тогда для любого натурального нечетного числа N его порядковый номер $n = (N + 1)/2$. Полуконтуру в модели НРЧ приписывается половина номера $k_п(N)/2$ его предельного контура, но не n.

Пример 6. Пусть ННЧ $N = 35$. Тогда $n = (35 + 1)/2 = 18$.

Интервалом числа НРЧ, соответствующим отдельному нечетному числу N, называется непрерывная последовательность контуров (полуконтуров), меньшей, чем N длины, суммарная длина которых равна N. Это означает, что любой интервал для полуконтура всегда начинается и заканчивается позициями квадратов чисел разной четности. Для отдельного составного числа в НРЧ, могут существовать несколько интервалов в разных частях НРЧ. Для простого числа такой интервал всегда один и он образован единственным полуконтуром *предельного контура* этого простого числа.

Интервальная модель натурального числа N представляет собой непрерывную последовательность контуров натурального ряда чисел, суммарная длина которых равна основной *характеристике* интервальной модели числа – значению факторизуемого числа N. В такой модели границами интервалов каждого нечетного числа N являются числовые квадраты разной четности. Это обстоятельство создает ряд неудобств, так как один из крайних контуров модели представлен в суммарной длине интервала лишь своей половиной (с границей – четным квадратом), т.е. полуконтуром.

При этом возникает два варианта положения такого полуконтура. Если факторизуемое нечетное число $N \equiv 3 (\mathrm{mod}\, 4)$, то граница интервала – четный квадрат является большим из двух (правая граница интервала для N), если число $N \equiv 1 (\mathrm{mod}\, 4)$, то четный квадрат меньший из двух (левая граница интервала для N).

Таким образом, вопрос о четности границ (правой, левой) для любого нечетного числа N решается однозначно, что, в свою очередь, определяет структуру интервальной модели числа N.

Структура интервала формируется конечным множеством непосредственно примыкающих друг к другу контуров и одного крайнего, примыкающего к ним полуконтура. Длина интервала определяется как сумма длин всех контуров и длины одного полуконтура. Эта модель далее преобразуется в другую модель путем замены длин контуров в сумме их номерами, а для крайнего полуконтура половиной номера

его предельного контура. После такой замены интервальная модель преобразуется в нумерационную модель, т.е. в сумму последовательных четных и нечетных натуральных чисел (номеров контуров). Неудобство создается и необходимостью учета для одного из крайних контуров лишь его полуконтура или половины номера контура.

Нумерационная модель натурального числа. Описанное ранее преобразование от интервальной модели к нумерационной модели числа упрощает ее, сводит к сумме последовательных натуральных чисел от некоторого значения $\boldsymbol{k}$ до значения $\boldsymbol{\ell}$. Замечательной особенностью этой модели является равенство этой суммы половине номера предельного контура $\boldsymbol{k_п(N)/2}$ нечетного числа $\boldsymbol{N}$. Независимо от положения в НРЧ исходного интервала числа $\boldsymbol{N}$ это равенство следует из теоремы о предельном контуре.

Значение $\boldsymbol{k_п(N)/2}$ находится элементарными простыми вычислениями для любого нечетного числа $\boldsymbol{N}$ и является основной *характеристикой* нумерационной модели числа. Для составных нечетных чисел $\boldsymbol{N}$ одно значение $\boldsymbol{k_п(N)/2}$ и суммы номеров контуров, образующих интервал для $\boldsymbol{N}$, может быть представлено разным количеством и разными по составу слагаемыми и, как следствие, разными разложениями числа $\boldsymbol{N}$ на два фактора.

Для нечетного числа $\boldsymbol{N}$ в НРЧ существует единственное представление, если число простое, и два или более представляющих интервалов, если число составное. Эти интервалы для составных чисел образуются контентом целых контуров и половиной одного крайнего из них. Интервал для $\boldsymbol{N}$ всегда образован нечетным числом полуконтуров, и это число является меньшим делителем $\boldsymbol{d_м}$ факторизуемого числа $\boldsymbol{N}$. Расположены контенты таких интервалов в разных частях НРЧ, на разном удалении от начала ряда. Особенностью интервалов является то, что граничными точками (числами) интервалов являются квадраты чисел разной четности. Среди таких интервалов всегда есть один, границами которого служат квадраты двух соседних чисел. Этот интервал называется *предельным полуконтуром*. Квадраты-границы альтернативных интервалов для числа $\boldsymbol{N}$ как бы раздвигаются по отношению к предельному. Количество полуконтуров, образующих интервал, тем больше, чем ближе интервал к началу НРЧ, так как контуры имеют меньшую длину. Заметим, что длина среднего полуконтура (при их нечетном количестве) равна $\boldsymbol{d_б}$ большему делителю числа $\boldsymbol{N}$.

Длина предельного интервала, как и всех других альтернативных, равна значению числа $\boldsymbol{N}$, но сам интервал при этом представляет собой лишь половину контура, который также называется *предельным контуром*.

Номер предельного контура важнейшая характеристика нечетного числа N. Он обозначается символом $k_{\text{п}}$ и вычисляется по формуле:

$$k_{\text{п}} = L_n(N)/8,\ L_n(N) = f(N) = N_л + N_n.$$

Здесь $N_л$ и N_n это полуконтуры предельного контура, а число N может быть любым из них. Четным квадратом в предельном (и в любом другом) контуре (общая граница полуконтуров) является квадрат его удвоенного номера $(2k_n)^2$. Тогда границы контура и значения его полуконтуров определяются через его номер k_n, как:

$$\Gamma_n(N) = (2k_n + 1)^2,\ \Gamma_л(N) = (2k_n - 1)^2 \text{ и } N_i = 4k_{\text{п}} \pm 1.$$

Знак в последнем выражении выбирается в зависимости от класса (левый, правый) нечетного числа N. Длина предельного контура определяется как разность его границ:

$$L_n(N) = \Gamma_n(N) - \Gamma_л(N) = 8k_{\text{п}}.$$

Границы всех других (альтернативных) интервалов образуют квадраты несмежных натуральных чисел, но также разной четности и в том же порядке.

6. Заключение. Рассмотренные в работе вопросы позволяют сделать некоторые выводы об описываемых задачах и о проблеме факторизации в целом. На факторизацию как на проблему явно не указывали великие математики, а некоторые из них лишь косвенно ее затрагивали Диофант, Ферма, Гаусс, Эйлер, Гильберт, не включая в перечень нерешенных задач. Возможно, именно это и притормаживало развитие теории в этом направлении, пока острой потребности в арифметической операции обращения умножения не возникало.

Развитие теории криптологии (двухключевые системы) всколыхнуло математическую мысль, но ни компьютерная вооруженность, ни распределенные сетевые вычисления к быстрому успеху не привели. Отсутствие фундаментальных теоретических результатов о таком объекте как НРЧ не позволяет найти выход из возникшего математического тупика. Даже финансовая стимуляция исследований не привела к ускорению процесса решения ЗФБЧ.

В работе предложена общая схема обработки составного натурального числа, базирующаяся на основной теореме арифметики и теореме факторизации, приводящая к разложению числа на множители и исключающая перебор вариантов. Рассмотренный подход к решению ЗФБЧ основывается на использовании закономерностей структурного

построения НРЧ и свойства натуральных чисел, не зависящего от их разрядности.

Литература

1. *Бронштейн И.Н., Семендяев К.А.* Справочник по математике для инженеров и учащихся ВТУЗов // М.: ГИТТЛ. 1954. 608 с.
2. *Василенко О.Н.* Теоретико-числовые алгоритмы в криптографии // М.: МЦНМО. 2003. 328 с.
3. *Ваулин А.Е.* и др. Фундаментальные структуры натурального ряда чисел // Сб.тр. 7-го Международного симпозиума. М.: РУСАКИ. 2006. С. 384–387.
4. *Ваулин А.Е.* Новый метод факторизации больших чисел в задачах анализа и синтеза двухключевых криптографических алгоритмов. Ч.1. // Информация и космос. 2005. №3. С. 74–78.
5. *Ваулин А.Е.* Новый метод факторизации больших чисел в задачах анализа и синтеза двухключевых криптографических алгоритмов. Ч.2. // Информация и космос. 2005. №4. С. 104 –112с.
6. *Дэвенпорт Г.* Высшая арифметика // М.: Наука. 1966. 176 с.
7. *Евклид*. Начала. М–Л. 1948–1950. Т. 1–3.
8. RSA. URL: https://ru.wikipedia.org/wiki/RSA.
9. *Ноден П., Китте К.* Алгебраическая алгоритмика (с упражнениями и решениями) // М.:Мир. 1999. 720 с.
10. *Пойя Д.* Математика и правдоподобные рассуждения // М.: ИЛ. 1957. 464 с.
11. *Ферма П.* Исследования по теории чисел и диофантову анализу // М.: Наука. 1992. 320 с.
12. *Эндрюс Г.* Теория разбиений // М.: Наука. 1982. 256 с.

References

1. Bronshtejn I.N., Semendyaev K.A. *Spravochnik po matematike dlja inzhenerov i uchashhihsja VTUZov* [Handbook of mathematics for engineers and students VTUZov]. M.: GITTL. 1954. 608 p. (In Russ.).
2. Vasilenko O.N. *Teoretiko-chislovye algoritmy v kriptografii* [Number-theoretic algorithms in the cryptography]. M.: MTsNMO. 2003. 328 p. (In Russ.).
3. Vaulin A.E. et al. [The fundamental structure of the naturally row numbers]. *Sb.tr. 7-go Mezhdunarodnogo simpoziuma*. [Proceedings of the 7th International Symposium]. M.: RUSAL KI. 2006. pp. 384–387. (In Russ.).
4. Vaulin A.E. [A new method of factoring large numbers in the analysis and synthesis of two-key cryptographic algorithms. Part 1]. *Informacija i kosmos – Information and Space.* 2005. no. 3. pp. 74– 78. (In Russ.).
5. Vaulin A.E. [A new method of factoring large numbers in the analysis and synthesis of two-key cryptographic algoritmov. Part 2]. *Informacija i kosmos – Information and Space.*. 2005. no. 4. pp. 104–112. (In Russ.).
6. Davenport G. *Vysshaja arifmetika* [Higher Arithmetic]. M.: Nauka. 1966. 176 p.
7. Euclid. *Euclid's Elements*. M-L. 1948–1950. vol. 1–3. (In Russ.).
8. RSA. Available at: https://ru.wikipedia.org/wiki/RSA. (In Russ.).
9. Noden P., Kitte K. *Algebraicheskaja algoritmika (s uprazhnenijami i reshenijami)* [Algebraic algorithmics (with exercisingtions and decisions)]. Moscow: Mir, 1999. 720 p. (In Russ.).
10. Pojja D. *Matematika i pravdopodobnye rassuzhdenija* [Mathematics and plausible reasoning]. M.: IL, 1957. 464 p. (In Russ.).
11. Ferma P. *Issledovanija po teorii chisel i diofantovu analizu* [Studies in number theory and diophantine analease]. M.: Nauka. 1992. 320 p. (In Russ.).

12. Andrews G. *Teorija razbienij* [The Theory of partitions]. M.: Nauka. 1982. 256 p. (In Russ.).

Ваулин Арис Ефимович — к-т техн. наук, доцент, доцент кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: криптоанализ, теория автоматов. Число научных публикаций — 200. yourmail_@mail.ru; ул. Ждановская д.13, Санкт-Петербург, 197082; р.т.: +7(812)347-9687.

Vaulin Aris Efimovich — Ph.D., associate professor, associate professor of system for collecting and processing information department, Mozhaisky military space Academy. Research interests: information security in automated systems for special purposes, cryptanalyst. The number of publications — 200. yourmail_@mail.ru; 13, Zhdanovskaya street, St. Petersburg, 197198, Russia; office phone: +7(812)347-9687.

Назаров Михаил Сергеевич — адъюнкт кафедры систем сбора и обработки информации, Военно-космическая академия имени А.Ф. Можайского. Область научных интересов: схемотехника, микроэлектроника. Число научных публикаций — 10. mikl21@mail.ru; ул. Ждановская д.13, Санкт-Петербург, 197082; р.т.: +7(812)347-9687.

Nazarov Mikhail Sergeevich — adjunct of systems for collecting and processing information department, Mozhaisky Military Space Academy. Research interests: circuitry, microelectronics. The number of publications — 10. mikl21@mail.ru; 13, Zhdanovskaya street, St. Petersburg, 197082, Russia; office phone: +7(812)347-9687.

РЕФЕРАТ

Ваулин А.Е., *Назаров М.С.* **Сведение задачи факторизации натурального числа к задаче разбиения числа на части. Часть 1.**

Развитие механизмов факторизации составных целых чисел рассматривается работе. От современных методов не следует ожидать, что алгоритм будет быстродействующим и эффективным в ближайшее десятилетие, в связи с ограниченным подходом к учету свойств чисел математический подход к решению этой проблемы, который базируется на методах типа решета Эратосфена, не является перспективным.

Механизм, предлагаемый автором этой работы, использует совершенно новый подход, основанный на изучении внутреннего строения натурального ряда и применения ряда свойств, слабо зависящих от разрядности числа. Примером такого свойства является признак делимости числа на 3. Такой подход обеспечивает переход от факторизации целых чисел к поиску специального свойства названного ф-инвариантом числа. При этом ожидается, что проблема будет менее сложной.

SUMMARY

Vaulin A.E., Nazarov M.C. **Conversion of Integer Factorization to a Problem of Decomposition of a Number. Part 1**.

The development of factorization mechanisms of composite integer numbers is being examined in this work. The current methods should not be expected to become more rapid and efficient in the nearest decade, due to narrow and inadequate mathematical approach to solution of this problem, which is based on so-called sieve of Eratosthenes.

The mechanism suggested by author of this work, uses a completely new method, based on examination of internal structure of natural sequence and application of digit place independent features (the criterion for divisibility). That kind of approach provides a conversion from integer factorization to a retrieval of the special figure separation, so-called F-invariant, which turns out to be less complex problem.