УДК 511; 519.6

А.Е.Ваулин

СВЕДЕНИЕ ЗАДАЧИ ФАКТОРИЗАЦИИ НАТУРАЛЬНОГО ЧИСЛА К ЗАДАЧЕ РАЗБИЕНИЯ ЧИСЛА НА ЧАСТИ. ЧАСТЬ 2

Ваулин А.Е. **Сведение задачи факторизации натурального числа к задаче разбиения числа на части. Часть 2.**
Аннотация. В настоящей работе рассматриваются и описываются вопросы разработки алгоритмов факторизации составных натуральных чисел. 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). Такой подход обеспечивает преобразование задачи разложения числа на множители в задачу поиска специального разбиения новой характеристики числа, названной ф-инвариантом, что следует признать менее сложной задачей.
Ключевые слова: натуральный ряд, нечетное число, ф-инвариант числа, разбиения числа, контур натурального ряда чисел.

Vaulin A.E. **Conversion of Integer Factorization to a Problem of Decomposition of a Number. Part 2.**
Abstract. The development of factorization mechanisms of composite integer numbers is examined in this work. The author proposes a different approach, based on the study of the internal structure of the positive integers and the use of the properties of numbers which do not depend on their digits (the criterion for divisibility). That kind of approach provides a conversion from integer factorization task to a retrieval task of the special partition of the new characteristic of a number, so-called f-invariant, which turns out to be less complex problem. – Bibl. 22 items.
Keywords: natural number, odd number, f-invariant of a numbers, partitions of a number, the contour of the natural numbers.

1. Введение. Разработка новых методов решения задачи факторизации больших чисел (ЗФБЧ) за приемлемые для практических нужд временные интервалы становится необходимостью настоящего времени. Известные характеристики лучших компьютеров настоящего времени не обеспечивают требуемых параметров решения ЗФБЧ. Самые мощные компьютеры мира (Tianhe-2, его производительность 33,86 петафлопс) в Китае; на втором месте – американский Titan (17,59 петафлопс); суперкомпьютер России «Ломоносов» из МГУ (0.9 петафлопс) – на 42 месте, фактически не изменяют ситуацию к лучшему.

Сложность вычислений в ЗФБЧ, как правило, связывают с зависимостью количества операций, необходимых для вычисления рассматриваемой функции, от разрядности аргумента функции. По нарастанию различают полиномиальную, субэкспоненциальную и экспоненциальную сложности.

Зависимость свойств чисел от разрядности, на которых базируются современные алгоритмы факторизации, не позволяет создать при их использовании быстродействующие алгоритмы [4–16]. Проблема факторизации числа имеет непосредственное отношение к теории чисел, так как среди арифметических операций этой теории отсутствует операция факторизации натурального числа [11-16], которая удовлетворяла бы запросам науки и общественной практики.

Метод дискретного логарифмирования Копперсмита сегодня является лучшим по скорости, но его применимость ограничена, для группы точек эллиптической кривой он не применим.

В предлагаемой работе вводятся новые модель натурального ряда чисел (НРЧ) и характеристика нечетного числа ф-инвариант. Эта числовая характеристика, определяется для нечетного натурального числа $\boldsymbol{N}$, имеющего произвольную разрядность и представляется разбиениями специального вида. Разбиения соответствуют разным интервалам для числа $\boldsymbol{N}$ и отображаются в контурную структуру модели НРЧ. Соответствующие числу $\boldsymbol{N}$ интервалы имеют полные квадраты на своих границах. Это свойство числа не зависит от его разрядности.

Формула, описывающая интервал длиной $\boldsymbol{N}$, расстоянием между граничными точками интервала (между квадратами), обеспечивает время реализации решения ЗФБЧ $\boldsymbol{N}$ весьма слабо зависящим от разрядности факторизуемого числа.

В этой (II) части работы показывается путь преобразования ЗФБЧ в задачу о разбиениях числа на основе новой его характеристики ф-инварианта с обоснованием преимуществ такого сведения.

2. Ф-инвариант числа. Инвариантом объекта (числа) называется количественная характеристика, которая остается без изменений при преобразованиях (изменениях), выполняемых с объектом. Так, например, аффинная и проективная геометрии отличаются инвариантами: в аффинной – это простое отношение, а в проективной – двойное отношение.

Ф-инвариантом числа $\boldsymbol{N}$ называется меньшее число, обозначаемое $\boldsymbol{k_п(N)/2}$ и равное половине номера предельного контура числа $\boldsymbol{N}$. Ф-инвариант существует для чисел произвольной разрядности. Получаемые различные представления (разными интервалами в НРЧ) числа $\boldsymbol{N}$ сохраняют значение ф-инварианта.

Пример 1. Рассмотрим введенные понятия на числовом примере. Пусть задано нечетное составное число $\boldsymbol{N = 3{\cdot}5{\cdot}7 = 105}$. Это наименьшее из нечетных чисел с тремя различными простыми нетривиальными делителями. Число $\boldsymbol{105}$ является составным правым нечетным числом, так как $\boldsymbol{N_п = 105 \equiv 1(\mathrm{mod}4)}$. Определим для $\boldsymbol{N_п = 105}$ номер предельного контура через его длину $\boldsymbol{k_п = L_п(N)\ /8 = (103 + 105)/8 = 26.}$

Так как число $N_п = 105$ в составе контура лишь правая «половина» (полуконтур), то ему соответствует лишь половина номера, то есть $k_п\ (N=105)/2 = 26/2 = 13$. Это значение $k_п\ (N)/2 = 13$ для N называется (является) ф-инвариантом.

Для числа $N_п = 105$ альтернативными предельному полуконтуру интервалами, определяемыми их границами, являются еще три интервала, характеристики которых приведены ниже в таблице 1.

Можно показать, что, если число N является нечетным левым и составным, то рассмотренные зависимости имеют место и в этом случае. Изменится только положение крайнего полуконтура в соответствующих интервалах, он станет равным половине меньшего, а большего контура в сумме. На сумму номеров контуров это изменение положения полуконтура влияния не окажет: она останется равной половине номера предельного контура.

Анализ данных таблицы показывает, что все альтернативные интервалы образованы совокупностями контуров и полуконтура такими, что их номера следуют непрерывно один за другим. В сумме эти номера задают специальные разбиения числа **13** равного половине номера предельного контура $k_п\ (105)/2 = 13$.

Таблица 1. Характеристики альтернативных интервалов (моделей) числа $N_п = 105$

Альтернативные интервалы их границы и длина для заданного числа $N_п = 105$	Суммы номеров контуров и длин полуконтуров, образующие интервалы, и их длины для числа $N_п = 105$
$Г_{п1} = 11^2, Г_{л1} = 4^2,$ $Г_{п1} – Г_{л1} = 121 – 16 = 105$	$2/2 + 3 + 4 + 5 = 13;$ спецразбиение $9+11+13+15+17+19+21=105$
$Г_{п2} = 13^2, Г_{л2} = 8^2,$ $Г_{п2} – Г_{л2} = 169 – 64 = 105$	$4/2 + 5 + 6 = 13;$ спецразбиение $17+19+21+23+25 = 105$
$Г_{п3} = 19^2, Г_{л3} = 16^2,$ $Г_{п3} – Г_{л3} = 361 – 256 = 105$	$8/2 + 9 = 13;$ спецразбиение $33+35+37 = 105$

Обратим внимание на то, что в суммах номеров контуров и полуконтура, вычисляемых для альтернативных интервалов, все слагаемые являются следующими подряд натуральными числами. Исключение составляет одно из крайних слагаемых, но и в этом случае контур, из номера которого берется в сумму лишь половина, имеет номер, примыкающий к основной последовательности номеров.

Это наблюдение дает основание для рассмотрения в качестве подмодели факторизуемого числа N суммы элементов разбиений специального вида для числа, равного половине номера предельного контура этого факторизуемого числа. А также рассматривается в качестве части алгоритма решения задачи факторизации числа N алгоритм генерации разбиений специального вида для ф-инварианта (половины номера предельного контура числа ***N***). Следующий пример служит для прояснения сказанного.

Пример 2. В средней колонке таблицы 2 в части I работы [3] приводится точечная диаграмма Феррера [13] для разбиений чисел. Блокам разбиения соответствуют строки диаграммы с возрастающим на единицу числом точек при движении вверх. Каждая строка точек интерпретируется как номер контура в интервальной модели натурального числа ***N***. Части всех разбиений (в строках) образованы монотонно возрастающими на единицу натуральными числами (точками строк). Разбиваемые числа (комбинаторные сочетания из ***k*** по два) C_k^2 описываются непрерывными совокупностями строк, начиная с нижней строки. Крайние блоки специальных разбиений – номера полуконтуров обозначены ***p*** и ***n***, ***p > n***.

Таблица 2. Сочетания для числового примера $C_k^2 = C_6^2$

Сочетания по 2 из 6 цифровых элементов $P = \{1,2,3,4,5,6\}$, $\|P\| = 6$		
1. 1 2	6. 2 3	11. 3 5
2. 1 3	7. 2 4	12. 3 6
3. 1 4	8. 2 5	13. 4 5
4. 1 5	9. 2 6	14. 4 6
5. 1 6	10. 3 4	15. 5 6

Например, строки (см. таблицу 2, [3]) с первой снизу по пятую строку включительно содержат количества точек: $1+2+3+4+(p=5)=15$, что соответствует числу комбинаторных сочетаний C_k^2, где значение ***k*** на единицу больше последнего элемента в сумме, т.е. $k = p + 1 = 5 + 1 = 6$ и $C_6^2 = 15$. В этом легко убедиться, построив все такие сочетания и подсчитав суммы (см. таблицу 2, [3]).

Таким образом, интерес в задаче факторизации числа ***N*** представляют не все возможные разбиения половины номера $k_п(105)/2 = 26/2 = 13$ предельного контура для $N = 105$, а только разбиения специального типа. Примеры таких специальных разбиений приведены в табл.***1.*** Они ниже в табл. ***3*** выделены заливкой. В этой таблице приводится список всех лексикографически упорядоченных разбиений числа ***13*** на все части для числового примера с $N_n = 105.$ Список сформирован в таблице 3 программой-генератором разбиений чисел.

Среди множества всех лексикографически упорядоченных разбиений числа $k_n/2 = 13$ (таблица 3, см. пример 4) диаграмме Феррера (см. таблицу 2, [3]) удовлетворяют лишь четыре специальных разбиения, а именно, разбиения с лексикографическими номерами:
№53 → 2/2 + 3 + 4 + 5; №70 → 4/2+ 5+ 6; №94 →8/2 + 9 и ***№101→13.***

Эти разбиения выделены заливкой в таблице 3. Последнее ***101***-е разбиение образовано одной частью (одной строкой), равной самому числу ***13***. Особенность этих разбиений состоит в том, что меньший блок разбиения в каждом из них равен лишь половине числа, которое начинает список блоков каждого разбиения. В ***53***-м разбиении это число ***2***, за которым следуют ***3, 4*** и ***5***, но от двойки в сумму берется лишь половина, т.е. единица. В ***70***-м разбиении меньший номер контура – это число ***4***, за которым следуют ***5*** и ***6***, но от четверки в сумму берется лишь половина, т.е. двойка. В ***94***-м разбиении это число ***8***, за которым следует единственное число ***9***, но от восьмерки в сумму берется лишь половина, т.е. четверка. Последнее разбиение №***101*** соответствует половине номера ***26/2*** предельного контура для правого числа $\boldsymbol{N = 105}$, т.е. $\boldsymbol{k_n/2 = 26/2 = 13}$.

Таблица 3. Полный список упорядоченных разбиений числа $\boldsymbol{k_п(105)/2 = 13}$ на все части

Лексикографически упорядоченные разбиения числа 13 на все части с указанием их номеров				
1. 1 1 1 1 1 1 1 1 1 1 1 1 1	21. 3 3 3 3 1	41. 5 2 1 1 1 1 1 1	61. 6 2 2 2 1	81. 7 5 1
2. 2 1 1 1 1 1 1 1 1 1 1 1	22. 4 1 1 1 1 1 1 1 1 1	42. 5 2 2 1 1 1 1	62. 6 3 1 1 1 1	82. 7 6
3. 2 2 1 1 1 1 1 1 1 1 1	23. 4 2 1 1 1 1 1 1 1	43. 5 2 2 2 1 1	63. 6 3 2 1 1	83. 8 1 1 1 1
4. 2 2 2 1 1 1 1 1 1 1	24. 4 2 2 1 1 1 1 1	44. 5 2 2 2 2	64. 6 3 2 2	84. 8 2 1 1 1
5. 2 2 2 2 1 1 1 1 1	25. 4 2 2 2 1 1 1	45. 5 3 1 1 1 1 1	65. 6 3 3 1	85. 8 2 2 1
6. 2 2 2 2 2 1 1 1	26. 4 2 2 2 2 1	46. 5 3 2 1 1 1	66. 6 4 1 1 1	86. 8 3 1 1
7. 2 2 2 2 2 2 1	27. 4 3 1 1 1 1 1 1	47. 5 3 2 2 1	67. 6 4 2 1	87. 8 3 2
8. 3 1 1 1 1 1 1 1 1 1 1	28. 4 3 2 1 1 1 1	48. 5 3 3 1 1	68. 6 4 3	88. 8 4 1
9. 3 2 1 1 1 1 1 1 1 1	29. 4 3 2 2 1 1	49. 5 3 3 2	69. 6 5 1 1	89. 8 5
10. 3 2 2 1 1 1 1 1 1	30. 4 3 2 2 2	50. 5 4 1 1 1 1	*70. 6 5 2*	90. 9 1 1 1 1
11. 3 2 2 2 1 1 1 1	31. 4 3 3 1 1 1	51. 5 4 2 1 1	71. 6 6 1	91. 9 2 1 1
12. 3 2 2 2 2 1 1	32. 4 3 3 2 1	52. 5 4 2 2	72. 7 1 1 1 1 1 1	92. 9 2 2
13. 3 2 2 2 2 2	33. 4 3 3 3	*53. 5 4 3 1*	73. 7 2 1 1 1 1	93. 9 3 1
14. 3 3 1 1 1 1 1 1 1	34. 4 4 1 1 1 1 1	54. 5 4 4	74. 7 2 2 1 1	*94. 9 4*
15. 3 3 2 1 1 1 1 1	35. 4 4 2 1 1 1	55. 5 5 1 1 1	75. 7 2 2 2	95. 10 1 1 1
16. 3 3 2 2 1 1 1	36. 4 4 2 2 1	56. 5 5 2 1	76. 7 3 1 1 1	96. 10 2 1
17. 3 3 2 2 2 1	37. 4 4 3 1 1	57. 5 5 3	77. 7 3 2 1	97. 10 3
18. 3 3 3 1 1 1 1	38. 4 4 3 2	58. 6 1 1 1 1 1 1 1	78. 7 3 3	98. 11 1 1
19. 3 3 3 2 1 1	39. 4 4 4 1	59. 6 2 1 1 1 1 1	79. 7 4 1 1	99. 11 2
20. 3 3 3 2 2	40. 5 1 1 1 1 1 1 1 1	60. 6 2 2 1 1 1	80. 7 4 2	100. 12 1
				101. 13

Задача представления ф-инварианта, необходимого для факторизации, таким образом, может быть сведена к разработке алгоритма и построению генератора разбиений такого специального вида. Аналитическое исследование возможностей получения таких разбиений может быть выстроено и иначе. Легко получается сумма элементов (точек) строк от первой до некоторой заданной с номером $k - 1$ – это расчет числа сочетаний по формуле $C_k^2 = k(k - 1)/2$. Например, при $k = 7$ имеем $C_k^2 = k(k - 1)/2 = 7{\cdot}6/2 = 21$. К сожалению, приведенная формула не учитывает «половинки» номеров крайних контуров, что при расчетах вызывает неудобства.

Выход из положения состоит в том, чтобы каким-то образом такие половинки учесть. Оказывается это вполне реализуемая задача. Так, например, имеем сумму ряда чисел в общем виде, где последнее слагаемое (верхняя строка диаграммы Феррера (см. табл. ***2,*** [3])) делится пополам, тогда $1 + 2 + 3 +\ldots+ n - 1 + n/2 = n^2/2$. В случае конкретных чисел $1 + 2 + 3 + 4/2 = 4^2/2 = 8$, как видим, сумма такого ряда вычисляется также достаточно просто.

Обозначим символом $\Delta(N)$ разность суммы C_k^2 номеров строк диаграммы Феррера (см. табл. ***2,*** [3]) до верхней выделенной строки с номером $k - 1 = 6$ и суммы $n^2/2$ номеров строк, учитывающей половину точек верхней строки с заданным номером $n = 4$ этой диаграммы, где, если $n < k$, как $\Delta(N) = C_k^2 - n^2/2$, а если $k < n$, то наоборот $\Delta(N) = n^2/2 - C_k^2$.

Очевидно, для решения задачи факторизации в обоих случаях разность должна быть равна ф-инварианту, т.е. половине номера $k_n(N)/2$ предельного контура числа N.

Другими словами, путем выбора значений k и n при вычислении $\Delta(N) = |C_k^2 - n^2/2| = k_п(N)/2$ необходимо обеспечить выполнение записанного равенства при заданном N. При этом состав и номера строк диаграммы, привлекаемых для вычислений сохраняются. Понятно, что определив одну из величин k или n, другая определяется как функция от первой. Например, при заданном значении k значение n определяется (берется арифметическое значение корня) как $n = \sqrt{2C_k^2 - k_n(N)}$.

Пример 3. (*Формирование специального разбиения: число* ***N = 105*** *– это правый полуконтур в предельном контуре*).

Факторизовать правое число $N = 105$ с использованием специальных разбиений.

Для $N = 105$ ранее был определен ф-инвариант (номер предельного полуконтура) $k_n(105)/2 = 26/2 = 13$. Необходимо выбрать в точечной диаграмме (см. табл. ***2,*** [3]) трапецию, определяемую ее основаниями, с суммарным значением точек равным $k_n(105)/2 = 13$. Уже пятая строка ($k = 5$) диаграммы таблицы ***2*** соответствует ***15*** точкам, следовательно, значение k может быть только большим, чем ***5***. Вычисления для $k = 7$ дают значение $C_k^2 = 21$. Необходимо для выполнения равенства $\Delta(105) = |C_k^2 - n^2/2| = k_n(105)/2 = 13$ определить значение переменной n (номер нижнего основания трапеции). Очевидно, n должно быть таким, чтобы выполнялось равенство $C_k^2 - 13 = n^2/2$.

Тогда $21 - 13 = 8 = n^2/2$ и $n = \sqrt{2 \cdot 8} = 4$. Действительно, при $k = 7, p = k - 1 = 6$ и $n = 4$ разность $\Delta(105) = 13$ и факторизация числа $N = 105$ может быть успешно выполнена. В примере найдены значения крайних блоков (номеров контуров в НРЧ): $p = 6$ и $n = 4$, специального разбиения, формирующего представляющий число N интервал.

Ранее суммированием элементов было показано и получено значение $4/2 + 5 + 6 = 13$, которое интерпретируется с одной стороны как сумма блоков специального разбиения числа 13, а с другой – как сумма номеров контуров НРЧ, образующих интервал для факторизуемого числа N. Преобразование номеров контуров (аддитивная форма числа) в их длину и суммирование этих длин дает следующий результат:

$$6 \cdot 8 + 5 \cdot 8 + (4 \cdot 8 + 2)/2 = 48 + 40 + 17 = 105 = N.$$

В последнем слагаемом левой части вычисляется длина крайнего (правого) полуконтура контура с номером $k = 4$. Суммарный интервал из длин контуров равняется как раз факторизуемому числу. Представляющий N интервал найден правильно. Но этого недостаточно, чтобы выполнить факторизацию N. Необходимо перейти к мультипликативной форме представления числа для чего определяются значения границ найденного интервала $Г_п(105); Г_п(105)$ или значения крайних точек представляющего число $N = 105$ интервала. Разумеется, они должны быть квадратами натуральных чисел. Определим эти границы.

Меньшая, левая граница совпадает с центральной границей меньшего контура, имеющего номер 4, т.е.:

$$Г_л(105) = Г_ц(4) = (2 \cdot 4)^2 = 8^2 = 64.$$

Большая, правая граница совпадает с правой границей большего контура с номером $k = 6$, т.е. $Г_п(105) = Г_п(6) = (2 \cdot 6+1)^2 = 13^2 =169$.

После этих вычислений, используя основное соотношение мультипликативной модели составного натурального числа:

$$N = x_1^2 - x_o^2 = (x_1 - x_o)(x_1 + x_o),$$

находятся факторы числа, а именно,

$$N = Г_п - Г_л = 13^2 - 8^2 = (13 - 8)(13 + 8) = 5 \cdot 21 = 105.$$

Пример 4. (*Формирование специального разбиения – число* N=1 1 1 *это левый полуконтур в предельном контуре*).

Факторизовать левое число ***N*** с использованием специальных разбиений. Рассмотрим натуральное левое нечетное число ***N* = *1 1 1*,** $N_л = 1\ 1\ 1 \equiv 3(\mathrm{mod}4)$ **.** Предельный контур заданного числа имеет текущий номер $k_n(1\ 1\ 1) = (N+1)/4 = 28$, и полуконтуру соответствует число $k_n(1\ 1\ 1)/2 = 28/2 = 14$.

В полном списке разбиений числа ***14*** (табл.4) единственное специальное разбиение с номером №***123 → 9 +10/2 = 14*** соответствует нумерационной модели этого натурального составного числа ***N* = *1 1 1***. Суммарная длина представляющего интервала равна:

$$8\cdot 9 + (8\cdot 10 - 2)/2 = 72 + 39 = 1\ 1\ 1.$$

Таблица 4. Полный список упорядоченных разбиений числа $k_п(1\ 1\ 1)/2 = 14$ на все части

Лексикографически упорядоченные разбиения числа 14 на все части с указанием их номеров				
1.1 1 1 1 1 1 1 1 1 1 1 1 1 1	28.4 2 2 2 2 1 1 1 1	55.5 3 2 2 1 1	82.6 4 2 1 1	109.8 2 2 2
2.2 1 1 1 1 1 1 1 1 1 1 1 1	29.4 2 2 2 2 1 1	56.5 3 2 2 2	83.6 4 2 2	110.8 3 1 1 1
3.2 2 1 1 1 1 1 1 1 1 1 1	30.4 2 2 2 2 2	57.5 3 3 1 1 1	84.6 4 3 1	111.8 3 2 1
4.2 2 2 1 1 1 1 1 1 1 1	31.4 3 1 1 1 1 1 1 1	58.5 3 3 2 1	85.6 4 4	112.8 3 3
5.2 2 2 2 1 1 1 1 1 1	32.4 3 2 1 1 1 1 1	59.5 3 3 3	86.6 5 1 1 1	113.8 4 1 1
6.2 2 2 2 2 1 1 1 1	33.4 3 2 2 1 1 1	60.5 4 1 1 1 1 1	87.6 5 2 1	114.8 4 2
7.2 2 2 2 2 2 1 1	34.4 3 2 2 2 1	61.5 4 2 1 1 1	88.6 5 3	115.8 5 1
8.2 2 2 2 2 2 2	35.4 3 3 1 1 1 1	62.5 4 2 2 1	89.6 6 1 1	116.8 6
9.3 1 1 1 1 1 1 1 1 1 1 1	36.4 3 3 2 1 1	63.5 4 3 1 1	90.6 6 2	117.9 1 1 1 1 1
10.3 2 1 1 1 1 1 1 1 1 1	37.4 3 3 2 2	64.5 4 3 2	91.7 1 1 1 1 1 1 1	118.9 2 1 1 1
11.3 2 2 1 1 1 1 1 1 1	38.4 3 3 3 1	65.5 4 4 1	92.7 2 1 1 1 1 1	119.9 2 2 1
12.3 2 2 2 1 1 1 1 1	39.4 4 1 1 1 1 1 1	66.5 5 1 1 1 1	93.7 2 2 1 1 1	120.9 3 1 1
13.3 2 2 2 2 1 1 1	40.4 4 2 1 1 1 1	67.5 5 2 1 1	94.7 2 2 2 1	121.9 3 2
14.3 2 2 2 2 2 1	41.4 4 2 2 1 1	68.5 5 2 2	95.7 3 1 1 1 1	122.9 4 1
15.3 3 1 1 1 1 1 1 1 1	42.4 4 2 2 2	69.5 5 3 1	96.7 3 2 1 1	*123.9 5*
16.3 3 2 1 1 1 1 1 1	43.4 4 3 1 1 1	70.5 5 4	97.7 3 2 2	124.10 1 1 1 1
17.3 3 2 2 1 1 1 1	44.4 4 3 2 1	71.6 1 1 1 1 1 1 1 1	98.7 3 3 1	125.10 2 1 1
18.3 3 2 2 2 1 1	45.4 4 3 3	72.6 2 1 1 1 1 1 1	99.7 4 1 1 1	126.10 2 2
19.3 3 2 2 2 2	46.4 4 4 1 1	73.6 2 2 1 1 1 1	100.7 4 2 1	127.10 3 1
20.3 3 3 1 1 1 1 1	47.4 4 4 2	74.6 2 2 2 1 1	101.7 4 3	128.10 4
21.3 3 3 2 1 1 1	48.5 1 1 1 1 1 1 1 1 1	75.6 2 2 2 2	102.7 5 1 1	129.11 1 1 1
22.3 3 3 2 2 1	49.5 2 1 1 1 1 1 1 1	76.6 3 1 1 1 1 1	103.7 5 2	130.11 2 1
23.3 3 3 3 1 1	50.5 2 2 1 1 1 1 1	77.6 3 2 1 1 1	104.7 6 1	131.11 3
24.3 3 3 3 2	51.5 2 2 2 1 1 1	78.6 3 2 2 1	105.7 7	132.12 1 1
25.4 1 1 1 1 1 1 1 1 1 1	52.5 2 2 2 2 1	79.6 3 3 1 1	106.8 1 1 1 1 1 1	133.12 2
26.4 2 1 1 1 1 1 1 1 1	53.5 3 1 1 1 1 1 1	80.6 3 3 2	107.8 2 1 1 1 1	134.13 1
27.4 2 2 1 1 1 1 1 1	54.5 3 2 1 1 1 1	81.6 4 1 1 1 1	108.8 2 2 1 1	135.14

Границами представляющего интервала служат левая граница девятого (***k = 9***) контура и центральная граница – правого (***k = 10***):

$$Г_л(1\,1\,1) = Г_л(9) = (2\cdot 9-1)^2 = 17^2 = 289;\ \text{и}\ Г_п(1\,1\,1) = Г_ц(10) = (2\cdot 10)^2 = 20^2 = 400.$$

Использование этих границ обеспечивает решение задачи факторизации числа ***N = 1 1 1*** на основе основного соотношения модели:

$$N = Г_п - Г_л = 20^2 - 17^2 = (20 - 17)(20 + 17) = 3\cdot 37 = 1\,1\,1.$$

Рассмотрим теперь вопрос о связи характеристик интервальной и нумерационной моделей числа ***N*** более подробно**.**

3. Взаимосвязь характеристик интервальной и нумерационной моделей. *Пример 5. (Взаимосвязь характеристик интервальной и нумерационной моделей нечетного натурального числа* ***N****)*

Пусть $N = 231 = 1\,1\cdot 21 = 33\cdot 7 = 77\cdot 3 = 231\cdot 1$, $N = 231 \equiv 3(\mathrm{mod}4)$, число ***N*** левое. Интервальная модель числа ***N*** сформирована как последовательность примыкающих друг к другу полуконтуров. Полуконтур в интервальной модели самый большой из всех в сумме и размещен справа, а больший квадрат (правая граница интервала) четный. Длина предельного контура $L_п = 231 + 233 = 464$, его номер $k_п(231) = L/8 = 464/8 = 58$, границы предельного полуконтура: правая граница $Г_п = Г_ц = (2k_п)^2 = 1\,16^2$, левая граница $Г_л = (2k_п - 1)^2 = 1\,15^2$.

Запишем интервальную модель ***N*** разностью границ интервала

$$N = Г_п - Г_л = x_{1i}^2 - x_{oi}^2 = (2\cdot 58)^2 - (58\cdot 2 - 1)^2 = 1\,16^2 - 1\,15^2 = 231\cdot 1.$$

Такое представление приводит к тривиальному разложению на множители числа ***N***. Нетривиальные нумерационные модели числа ***231*** с ф-инвариантом $k_п(231)/2 = 58/2 = 29$ представлены тремя, $i = 1(1)3$, суммами номеров (тремя наборами слагаемых) последовательных номеров контуров с учетом лишь половины номера от большего контура Здесь таблицу со списком всех разбиений не приводим (она слишком велика), а укажем ниже только специальные разбиения из нее:

$$k_п(N)/2 = 29 = (3 + 4 + 5 + 6 + 7 + 8\,/2) = (7 + 8 + 9 + 10/2) = (19 + 20/2).$$

Через суммы номеров контуров (нумерационные модели) число $N = 231 = 4k - 1 = 58\cdot 4 - 1$ имеет три представления, где число ***29*** представляется разными суммами номеров, приведенными выше:

$$N = 231 = 29\cdot 8 - 1 = (3 + 4 + 5 + 6 + 7 + 8/2)8 - 1 =$$
$$= (7 + 8 + 9 + 10/2)8 - 1 = (19 + 20/2)8 - 1.$$

Эти три суммы в скобках представляют собой разбиения в полном лексикографическом списке разбиений числа ***29*** и имеют в этом списке лексикографические номера: ***№1403→8/2 7 6 5 4 3=7 6 5 4 4 3; №2533 →10/2 9 8 7 = 9 8 7 5; №4468 →20/2 19 = 19 10.***

Можно увидеть, что в разбиении с номером ***№1403*** как бы не выполнено условие специальности разбиения, так как оно имеет два одинаковых подряд следующих блока (***4 4***). На самом деле одна из четверок это половина номера большего контура (***8/2 = 4***), следующего за седьмым контуром. В следующем разбиении блок ***5*** следует не за шестым, а за седьмым блоком. Это означает, что пятерка – это половина номера десятого контура, следующего в НРЧ за девятым контуром. Аналогично и в последнем разбиении ***10 = 20/2*** – это половина номера двадцатого контура, следующего за девятнадцатым. Дело в том, что совсем не тривиальная программа-генератор лексикографически упорядоченных разбиений числа представляет блоки разбиения именно в таком порядке. Особой необходимости переделывать программу не возникает, и здесь ограничиваемся просто краткими пояснениями.

Ниже выписаны представления числа $N = 231$ границами интервалов (интервальная модель) и результаты факторизации числа:

$$N = Г_п - Г_л = x_{1i}^2 - x_{oi}^2,\ i = 1(1)4,$$

$$Г_п\ (2 \cdot 8) - Г_л\ (3 \cdot 2 - 1) = x_{1i}^2 - x_{oi}^2 = 256 - 25 = 231 = (16 + 5)(16 - 5) = 21 \cdot 1\ 1;$$

$$Г_п\ (2 \cdot 10) - Г_л\ (7 \cdot 2 - 1) = x_{1i}^2 - x_{oi}^2 = 400 - 169 = 231 = (20 + 13)(20 - 13) = 33 \cdot 7;$$

$$Г_п\ (2 \cdot 20) - Г_л\ (19 \cdot 2) = x_{1i}^2 - x_{oi}^2 = 600 - 1369 = 231 = (40 + 7)(40\ 37) = 77 \cdot 3;$$

$$Г_п(2 \cdot 58) - Г_л(58 \cdot 2 - 1) = x_{1i}^2 - x_{oi}^2 = 1\ 16^2 - 1\ 15^2 = (1\ 16 + 1\ 15)(1\ 16 - 1\ 15) = 231 \cdot 1.$$

Наличие различных представлений ф-инварианта $k_n(N)/2$ несколькими суммами свидетельствует о том, что N составное число и в его интервальной модели контурный состав формируется в разных областях НРЧ.

Так для $N = 231$ в НРЧ существуют четыре интервала. Ближний к началу НРЧ интервал включает контуры с номерами от контура ***3*** до контура ***8***, от большего из которых в интервал включатся только левый полуконтур. Существует второй интервал, включающий контуры с номерами от контура ***7*** до контура ***10***, и еще один интервал от контура ***19*** до ***20*** и, наконец, предельный контур с номером ***58*** , левый полуконтур которого и есть число равное $N = 231.$ Причем, от большего контура в каждом случае берется лишь его левый полуконтур.

Рассмотренный пример иллюстрирует все возможные решения задачи факторизации числа $N = 231$ на два сомножителя (фактора). По основной теореме арифметики в разложениях N необходимо указывать все простые делители для числа $N.$ Это выполняется несложно, применяя алгоритм к найденным факторам до тех пор, пока все факторы не станут простыми числами. Здесь приведено решение задачи, но не показано, как оно получено. Ранее указывались отдельные возможные способы нахождения решений. Этот вопрос достаточно объемный и сложный и не рассматривается в работе детально.

Пример 6. (Взаимосвязь характеристик интервальной и нумерационной моделей числа кратного трем).

Для левого числа $N(x_1, x_o) = 183$ и правого числа $N(x_1, x_o) = 189$ выполнить факторизацию, определить значение предельного контура чисел $k_п\ (N_л) = k_п\ (183) = (183 + 185)/8 = 46$, и $k_п(N_п) = k_п(189) = (187 + 189)/8 = 47$. Далее составляется уравнение в общем виде для номера предельного полуконтура в нумерационной модели $k_п\ (183)/2 = (k + 1)/2 + k$, откуда $k_п = 3k + 1$ и $k = (k_п - 1)/3 = 45/3 = 15$. Большая граница интервала для $N = 183$ правая четная $Г_ц(16) =(2 \cdot 16)^2 = 32^2 =1024$ и меньшая левая граница $Г_л(15) = (2 \cdot 15-1)^2 =29^2 = 841$. Факторизация числа $N = 183 = 32^2 - 29^2 = (32 + 29)(32 - 29) = 61 \cdot 3$.

Связь правых чисел вида $N_п(x_1, x_o) = 3t$ (t - произвольное ННЧ) с суммой номеров контуров интервальной модели следующая: половина номера контура плюс номер следующего контура интервала равны половине номера предельного контура $k_п\ (N_п)/2$ исследуемого числа.

Для правого числа $N(x_1, x_o) = 189$ значение предельного полуконтура $k_п\ (189)/2 = (k - 1)/2 + k$, откуда:

$$k_п = 47 = 3k - 1 \text{ и } k = (k_п + 1)/3 = 48/3 = 16.$$

Меньшая граница интервала для $N = 189$ левая четная лежит в 15 контуре $Г_ц(15) =(2 \cdot 15)^2 = 30^2 = 900$ и $Г_п(16) = (2 \cdot 16 +1)^2 =33^2 = 1089$.

Факторизация числа:

$$N = Г_п(16) - Г_ц(15) = 1089 - 900 = (33 + 30)(33 - 30) = 63 \cdot 3$$

Аналогичные расчеты могут быть выполнены для чисел левых и правых кратных ***5, 7, 9*** и т.д.

4. Специальные разбиения натурального числа кратного трем. Натуральные нечетные числа $N(x_1, x_o) = 3t$ (t – произвольное нечетное) кратные трем всегда формируются тремя смежными полуконтурами, два из которых – целый контур. Пусть номер целого контура обозначен как k. Для таких чисел нумерационная модель очень простая. Для левых нечетных натуральных чисел:

$$k_п(N_л)/2 = k + (k + 1)/2 \rightarrow k_п(N_л) = 3k + 1. \text{ Отсюда } k = (k_п(N_л) - 1)/3.$$

Для правых нечетных натуральных чисел:

$$k_п(N_п)/2 = (k - 1)/2 + k \rightarrow k_п(N_п) = 3k - 1. \text{ Отсюда } k = (k_п(N_п) + 1)/3.$$

Пример 7. (*Факторизация чисел кратных числу три*). Задано составное кратное трем нечетное число $N = 129 = 3\cdot 43$. Это число правое, так как $129 \equiv 1(\mathrm{mod}4)$.

Предельный контур для этого числа имеет длину $127+ 129 =256$. Номер $k_n(129)$ предельного контура числа равен $k_n(129) = 256/8 = 32$. Ф-инвариант для числа 129 равен $k_n(129)/2 = 32/2 = 16$. Подставляем в формулу для k найденные значения $k = (32 + 1)/3 = 1\ 1$. Это номер большего контура из двух полуконтуров $43 + 45 = 88 = 1\cdot 18$. Для формирования интервала включаем в сумму правый (больший) полуконтур из предшествующего контура с номером $k_{np} = 10 = 1\ 1 - 1$, длина которого $M = 4k_{np} + 1 = 41$.

И окончательно, длина интервала позиций для числа $N = 129$ есть сумма трех полуконтуров $129 = 41+ 43+ 45$. Теперь можно найти значения границ этого интервала и факторизовать N.

– меньшая граница интервала $Г_л(129) = Г_ц(k =10)$ – это левая граница для контура с номером 10, $Г_ч(10) = (2\cdot 10)^2 = 400 = 20^2$;

– большая граница интервала $Г_n(129) = Г_n(1\ 1)$ – это правая граница для правого контура с номером $1\ 1$, $Г_ц(1\ 1) = (2\cdot 1\ 1 + 1)^2 = 529 = 23^2$;

Интервал числа $N = 129$ представляем разностью границ

$$Г_n(129) – Г_л(129) = Г_n(1\ 1) – Г_ц(10) = 23^2 – 20^2 = (23 – 20)(23 + 20)$$

и получаем разложение N на множители $3\cdot 43 = 129$.

Пример 8. (*Разбиение правого числа, где половина номера предельного контура (не целое число) в сумму берется от меньшего контура).* Для правого числа $N(x_1, x_o) = 621$ выполнить факторизацию.

Будем формировать нумерационную модель числа. Определяем номер $k_п(N_п)$ по значению длины предельного контура числа 621, $k_п(N_п) = k_n(621) = (621–1)/4 = (619 + 621)/8 = 155$. Затем определяем его половину $k_n(621)/2 = 77,5$ и находим разность $C^2_{k+1} – k_n /2$, ближнюю к началу НРЧ. В столбце C^2_{k+1} (см. табл. 2 [3]) находим при $k=12$ значение 78, превышающее $k_n(621)/2 = 77,5$. Тогда искомая разность $C^2_{k+1} – k_n /2 =78 – 77,5 = 0,5$. Проверяем, совпадает ли найденная разность со значением $k^2 /2$ при некотором значении k. Совпадение имеет место со значением $0,5$ в нижней строке таблицы. Отсюда определяется номер меньшего контура $k_n^2 /2 = 0,5 \rightarrow k = 1$, формируемого интервала. Интервал, представляющий число $N = 621$, начинается средней точкой квадрата (четной) первого контура и доходит до 12-го контура включительно. Известно, что через границы длина интервала для числа N представляется выражением $N = Г_n – Г_л = x_{1i}^2 – x_{oi}^2$. Зная номера контуров на границах интервала, находим его граничные точки. Границами интервала будут:

для правого полуконтура первого контура левая граница $\Gamma_л = (2k)(2{\cdot}1)^2 = 4$, и правая граница контура при $k = 12$ есть $\Gamma_п = (2k+1)^2 = (2{\cdot}12+1)^2 = 625$.

Тогда $N = \Gamma_п - \Gamma_л = x_{1i}^2 - x_{oi}^2 = 625 - 4 = 621.$ С другой стороны, при наличии границ легко выполняется факторизация числа:

$$N = x_{1i}^2 - x_{oi}^2 = (25 + 2)(25 - 2) = 27{\cdot}23.$$

Рассмотренная в примере схема решения задачи факторизации обеспечивает нахождение и других альтернативных пар границ. Поиск разности $C_{k+1}^2 - k_п/2$, совпадающей с $k^2/2$ приводит к получению такого совпадения при большем $k = 19$.

Имеем равенство $C_{k+1}^2 - k_п/2 = 190 - 77{,}5 = 112{,}5$ из которого находим меньшее $k = \sqrt{2 \cdot 112{,}5} = \sqrt{225} = 15$. Теперь можно приступить к поиску границ интервала и факторизации.

Границами интервала будут:
левая граница при $k = 15$, $\Gamma_л = (2k)^2 = (2{\cdot}15)^2 = 900$, и
правая граница при $k = 19$ есть $\Gamma_п = (2k + 1)^2 = (2{\cdot}19 + 1)^2 = 39^2 = 1521$,
$N = \Gamma_п - \Gamma_л = x_{1i}^2 - x_{oi}^2 = 1521 - 900 = 621$ и $N = x_{1i}^2 - x_{oi}^2 = (39+30)(39-30) = 69{\cdot}9.$

Пример 9. (*Разбиение левого числа, где половина номера предельного контура (не целое число) в сумму берется от большего контура).* Пусть задано число $N = 235$, число $N = 235 \equiv 3(\mathbf{mod} 4)$ левое. Для числа 235 длина предельного контура $L_п = 235 + 237 = 472$, его номер $k_п = L/8 = 472/8 = 59$, $k_п/2 = 29.5$, границы предельного контура: правая $\Gamma_п = (2k_п)^2 = 118^2$, левая $\Gamma_л = (2k_п - 1)^2 = 117^2$ им соответствует тривиальное разложение числа $N = 235{\cdot}1$.

Из нумерационной модели следует, что $k_п/2 = 29.5.$ Для $N=235$ (см. пример ранее) $k_п(235)/2 = 29.5.$

Ближайшее значение в столбце $n^2/2 = 40.5$ лежит в строке $n = 9.$ Ему соответствует разность $n^2/2 - k_п/2 = 40.5 - 29.5 = 11,$ которая отсутствует в столбце «сумма». Следующий допустимый уровень $n = 11$ и $n^2/2 = 60.5,$ ему соответствует разность $n^2/2 - k_п/2 = 60.5 - 29.5 = 31,$ которая также отсутствует в столбце «сумма». Следующий допустимый уровень $n = 13$ и $n^2/2 = 84.5,$ ему соответствует разность $n^2/2 - k_п/2 = 84.5 - 29.5 = 55,$ которая присутствует в столбце «сумма» в строке с номером 10.

Отсюда следует вывод о том, что все строки диаграммы Ферера, начиная с номера 10 и ниже, не включаются в сумму $k_п/2$. Следовательно, $k_п/2 = 29.5 = 11 + 12 + 13/2.$

Выполним факторизацию заданного числа. Найдены номера контуров, образующие нумерационную модель числа: $k = 11, 12$ и 13. От $k =$

13 в формулу входит лишь левая половина этого контура. Вычислим длины контуров $L(11 = 8\cdot 11 = 88; L(12) = 8\cdot 12 = 96; L(13) = 8\cdot 13 = 104;$ левая половина (полуконтур) ***13***-го контура $m(13)=104/2-1=51$. Интервальная модель $88 + 96 + 51 = 235$.

Определим границы интервальной модели:

$$Г_п(13) = (2\cdot 13)^2 = 26^2 = 676; \; Г_л(11) = (2\cdot 11-1)^2 = 21^2 = 441.$$

Теперь число $N = 235$ можно факторизовать:

$$N(x_1, x_o) = 235 = (x_1 + x_o)(x_1 - x_o) = (26 + 21)(26 - 21) = 47\cdot 5 = 235.$$

Пример 10. (*Разбиение правого числа, где половина номера предельного контура (не целое число) в сумму берется от меньшего контура).* Пусть $N = 357$. Это правое число $N = 357 \equiv 1(\mathbf{mod}4)$. Длина предельного контура $L_n = 357 + 355 = 712$, его номер $k_п = L/8 = 712/8 = 89$, $k_п /2 = 44.5$, границы предельного контура: левая $Г_л = (2\,k_п - 1)^2 = 177^2$, средняя $Г_ц = (2\,k_п) = 178^2$, правая $Г_п = (2\,k_п + 1)^2 = 179^2$ им соответствует тривиальное разложение числа $N = 357\cdot 1$.

а) $x_1 = 19; x_o = 2; N = Г_п\,(2\cdot 58) - Г_л\,(58\cdot 2- 1) = x_{1i}^2 - x_{oi}^2 = 19^2 - 2^2 = 361- 4 = (19 + 2)\cdot(19 - 2) = 21\cdot 17 = 357, k_п /2 = ½ + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 44.5$

б) $x_1 = 61; x_o = 58; N = Г_п(2\cdot 58) - Г_л(58\cdot 2-1) = x_{1i}^2 - x_{oi}^2 = 61^2 - 58^2 = 3721- 3364 = (61+58)\cdot(61-58) = 119\cdot 3 = 357; k_п /2 = 29/2 + 30 = 44.5.$

Длина произвольных контура и интервала натурального ряда чисел между нечетными квадратами кратна числу ***8***. Вычет нечетного квадрата по **mod** ***8*** равен ***1***. Разность квадратов нечетных простых чисел ≥ 5 кратна ***24*** ($7^2 - 5^2 = 24$). Это можно показать следующим образом. Рассмотрим квадраты двух нечетных простых чисел, а затем найдем их разность. Из трех смежных чисел $2n - 1, 2n, 2n + 1$ одно всегда кратно трем. В нашем случае – это число n, так как крайние числа простые по условию.

$$Нч_1^2 = (2n - 1)^2 = 4n^2 - 4n + 1 = 1 + 4n(n - 1) = 1 + 8\,C_n^2,$$
$$Нч_2^2 = (2n + 1)^2 = 4n^2 + 4n + 1 = 1 + 4n(n + 1) = 1 + 8\,C_{k+1}^2\,,$$
$$Нч_2^2 - Нч_1^2 = 8(C_{k+1}^2 - C_n^2) = 4n(n + 1 - n + 1) = 8n = 8\cdot 3t = 24t.$$

Если число ***N*** кратно 3, оно в интервальной модели образовано тремя полуконтурами, стоящими рядом. Другими словами, если число правое, то полуконтур от меньшего контура. Для $N = 357 = 119\cdot 3, k_п/2 = 44.5$. Значение номера полуконтура определяется формулой ($k_п/2 - 1$)/3 = $(44/5 - 1)/3 = 14.5$. Следовательно, номер меньшего контура $14.5\cdot 2 = 29$, а номер следующего ***30***. Действительно, $29/2 + 30 = 44.5 =$

$k_п/2$. Если число N кратно 5 (образовано пятью полуконтурами), то номер $(k_п/2 - 6)/5$.

Пример 11. (*Восстановление числа $N_п$, кратного трем по номеру меньшего контура*). Задан номер левого контура в интервальной модели числа $N_п$ кратного трем с номером $k = 40$. Тогда ф-инвариант:

$$k_n(N_n)/2 = 40/2 + 41 = 61,$$

а длина интервала, представляющего число в интервальной модели:

$$L = 20\cdot 8 + 1 + 41\cdot 8 = 161 + 328 = 161 + 163 + 165 = 489.$$

Это правое нечетное число, так как $489 \equiv 1(\mathrm{mod}4)$. Границы интервала в интервальной модели обрабатываемого числа: правая большая $Г_n(41) = (2\cdot 41 + 1)^2 = 83^2 = 6889$; левая меньшая – четное число

$$Г_л(40) = (2\cdot 40)^2 = 80^2 = 6400.$$

Представление числа разностью границ интервала
$N_n(x_1, x_o) = Г_n - Г_л = 83^2 - 80^2 = 6889 - 6400 = 489$ и его факторизация имеет вид: $N_n(x_1, x_o) = N_n(83, 80) = (83 + 80)(83 - 80) = 163\cdot 3 = 489$.

Число 163 – простое и других разложений не существует.

Пример 12. Пусть задано число $N(x_1, x_o) = 663 = 3t$, кратное трем. Это левое число, так как $663 \equiv 3(\mathrm{mod}4)$. Границы интервала модели числа правая большая четная и левая меньшая нечетная. Сам интервал образован контуром с номером k и левым полуконтуром $(k + 1)$-го контура. Рассмотрим нумерационную модель числа. Половина номера предельного полуконтура заданного числа $k_n(N_л)/2 = k_n(663)/2 = (663 + 665)/16 = 83 = k + (k + 1)/2 = (3k + 1)/2$, откуда $k = (166 - 1)/3 = 55$.

Выполним переход к интервальной модели числа. Длина интервала $L(k + (k + 1)/2) = 8\cdot 55 + 8\cdot 56/2 - 1 = 440 + 223 = 663$.

Значения границ интервальной модели:

$$Г_n(56) = (2\cdot 56)^2 = 1\,12^2 = 12544;\ Г_л(55) = (2\cdot 55 - 1)^2 = 109^2 = 1\,1881.$$

Теперь число N можно факторизовать $N(x_1, x_o) = 663 =$
$= (x_1 + x_o)(x_1 - x_o) = (1\,12 + 109)(1\,12 - 109) = 221\cdot 3 = 3\cdot 13\cdot 17 = 663$.

Пример 13. (*Разбиение инварианта левого $N_л$ числа, где половина номера (целое число) контура, включаемого в сумму, берется от большего контура).*

Пусть $N = 207$, число левое $N = 207 \equiv 3(\mathrm{mod}4)$. Длина предельного контура $L_n = 207 + 209 = 416$, его номер $k_n = L/8 = 416/8 = 52$, $k_n/2 = 26$. Границы предельного полуконтура: правая $Г_n = (2k_n)^2 = 104^2$, левая $Г_л = (2k_n - 1)^2 = 103^2$. Этим границам соответствует тривиальное мультипликативное разложение числа $N = 207 = 207\cdot 1$.

Из нумерационной модели следует, что имеются три разбиения $k_n(N_л)/2 = k_n(207)/2 = 17 + 18/2 = 26 = 4 + 5 + 6 + 7 + 8/2 = 4 + 5 + 6 + 7 + 4$.

Эти разбиения в полном списке ***2436*** разбиений числа ***26*** имеют лексикографические номера

№***927*** $\rightarrow$ ***76544*** (разбиение содержит две одинаковые части (четверки)), №***2369*** $\rightarrow$ ***17+ 9***. Для $N = 231$ (см. пример ***1*** ранее) $k_n(231)/2 = 29$ или $3 + 4 + 5 + 6 + 7 + 8/2 = 29$ в разбиении также присутствуют две четверки. Результат факторизации $207 = 23 \cdot 9 = 69 \cdot 3$.

5. Заключение. На основе нового подхода к описанию натурального ряда чисел, в котором главная роль отводится положению квадратов натуральных чисел и интервалов между ними, формируется конструктивная модель НРЧ. Нечетные числа распределены в *два класса*: левые и правые. Модель используется для синтеза операции обращения произведения чисел, т.е. решения задачи *факторизации* больших чисел. Многочисленные числовые примеры иллюстрируют сведение ЗФБЧ к задаче формирования специальных разбиений числа.

В модели НРЧ используются понятия *контура* – расстояния между квадратами последовательных нечетных чисел, *полуконтура* – расстояния между квадратами смежных чисел, положение которых естественным образом упорядочено в пределах НРЧ. Этот порядок в модели реализуется естественной (от первого контура между 3^2 и 1 с увеличением на единицу для последующих) *нумерацией* контуров и полуконтуров. Положение контуров в НРЧ постоянное. С каждым контуром связывается пара полуконтуров, им также соответствуют номера. Вводятся понятия *длины* L контуров (полуконтуров) и, что особенно важно, их *границы,* роль которых играют квадраты чисел.

Любое нечетное число $N = pq$, $p < q$, в модели НРЧ представляется непрерывной последовательностью нечетного количества (равного p) полуконтуров (фрагментом арифметической прогрессии со средним членом равным q), которая названа *интервалом*. Интервалы могут перемещаться вдоль НРЧ, но их границы всегда квадраты чисел разной четности.

Такое свойство обусловливает возможность представления длины интервалов (равна значению $L = N$) разностью их правой и левой границ $N = Г_п - Г_л = x_{1i}^2 - x_{oi}^2$ из чего следует мультипликативная форма записи для числа $N = (x_{1i} - x_{oi})(x_{1i} + x_{oi})$, соответствующая его факторизации.

Наличие нескольких альтернативных интервалов для представления нечетного числа N обусловлено множеством его простых делителей. Для определения положения альтернативных интервалов в НРЧ вводится понятие *ф-инварианта* нечетного числа, значение которого сохраняется независимо от рассматриваемого альтернативного интервала. Эта числовая характеристика ***N*** допускает ее представление комбинаторными *разбиениями специального вида*, в которых роль частей разбиения играют номера контуров, формирующих интервалы для ***N*.**

Все сформулированные положения обеспечивают универсальность подхода и допускают алгоритмизацию. Создаваемые алгоритмы базируются на свойствах, практически не зависящих от разрядности чисел, на использовании границ интервалов для ***N***, являющихся квадратами, что позволяет предположить высокое быстродействие при практической реализации.

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., Назаров М.С.* Сведение задачи факторизации натурального числа к задаче разбиения числа на части. Часть 1 // Труды СПИИРАН. 2015. Вып. 39. С. 157-176.
4. *Ваулин А.Е.* и др. Фундаментальные структуры натурального ряда чисел // Сб.тр. 7-го Международного симпозиума. М.: РУСАКИ. 2006. С. 384–387.
5. *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.
6. *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.
7. *Дэвенпорт Г.* Высшая арифметика // М.: Наука. 1966. 176 с.
8. *Евклид*. Начала. М–Л. 1948–1950. Т. 1–3.
9. RSA. URL: https://ru.wikipedia.org/wiki/RSA.
10. *Ноден П., Китте К.* Алгебраическая алгоритмика (с упражнениями и решениями) // М. Мир. 1999. 720 с.
11. *Пойя Д.* Математика и правдоподобные рассуждения // М.: ИЛ. 1957. 464 с.
12. *Ферма П.* Исследования по теории чисел и диофантову анализу // М.: Наука. 1992. 320 с.
13. *Эндрюс Г.* Теория разбиений // М.: Наука. 1982. 256 с.
14. *Дирихле П.Г.Л.* Лекции по теории чисел //М.: Книжный дом «ЛИБРОКОМ». 2014. 368с.
15. *Манин Ю.И., Панчишкин А.А.* Введение в современную теорию чисел // М.: МЦНМО. 2013. 552с.
16. *Шафаревич И.Р.* Основы алгебраической геометрии //М.:МЦНМО. 2007.589с.

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., Nazarov M.S. [Reduction of the integer factorization problem to the partition number on the part. Part 1]. *Trudy SPIIRAN – SPIIRAS Proceedings*. 2015. vol. 39. pp. 157-176.
4. 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.).
5. 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.).
6. 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.).
7. Davenport G. *Vysshaja arifmetika* [Higher Arithmetic]. M.: Nauka. 1966. 176 p.
8. Euclid. *Euclid's Elements*. M-L. 1948–1950. vol. 1–3. (In Russ.).
9. RSA. Available at: https://ru.wikipedia.org/wiki/RSA. (In Russ.).
10. Noden P., Kitte K. *Algebraicheskaja algoritmika (s uprazhnenijami i reshenijami)* [Algebraic algorithmics (with exercising and decisions)]. Moscow: Mir, 1999. 720 p. (In Russ.).
11. Pojja D. *Matematika i pravdopodobnye rassuzhdenija* [Mathematics and plausible reasoning]. M.: IL, 1957. 464 p. (In Russ.).
12. Ferma P. *Issledovanija po teorii chisel i diofantovu analizu* [Studies in number theory and diophantine analease]. M.: Nauka. 1992. 320 p. (In Russ.).
13. Andrews G. *Teorija razbienij* [The Theory of partitions]. M.: Nauka. 1982. 256 p. (In Russ.).
14. Dirichlet P.G.L. *Lekcii po teorii chisel* [Lectures on the theory of numbers]. M.: Knizhnyj dom «LIBROKOM». 2014. 368 p. (In Russ.).
15. Manin Y.I., Panchishkin A.A. *Vvedenie v sovremennuju teoriju chisel* [Introduction to the modern theory of numbers]. M.: MCNMO. 2013. 552 p. (In Russ.).
16. Shafarevich I.R. *Osnovy algebraicheskoj geometrii* [Foundations of algebraic geometrii]. M.:MCNMO. 2007.589 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: криптоаналитиз, теория автоматов. Число научных публикаций — 200. mikl21@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. mikl21@mail.ru; 13, Zhdanovskaya street, St. Petersburg, 197198, Russia; office phone: +7(812)347-9687.

РЕФЕРАТ

Ваулин А.Е. **Сведение задачи факторизации натурального числа к задаче разбиения числа на части. Часть 2.**

Новый подход к проблеме факторизации составных целых чисел рассматривается работе. Предполагается, что новый метод и алгоритм будет быстродействующим и эффективным при его реализации. Метод базируется на использовании свойств чисел, слабо зависящих от их разрядности, что как ожидается, обеспечит ему высокую степень универсальности.

Большую роль при разработке метода играет изучении внутреннего строения натурального ряда чисел и создание его модели, включающей ряд новых понятий. Применения таких понятий как контур, полуконтур, интервал, границы объектов модели и некоторых других понятий обеспечивают разработку моделей отдельных нечетных чисел. Введение понятия ф-инварианта нечетных чисел, для которых рассматриваются два класса: левые и правые, открывает возможность выполнить переход от традиционного подхода к решению задачи факторизации к сведению поиска разбиений числа специального вида. При этом ожидается, что проблема будет менее сложной.

SUMMARY

Vaulin A.E. **Conversion of Integer Factorization to a Problem of Decomposition of a Number. Part 2.**

A new approach to the problem of factoring integers is considered in this work. It is assumed that the new method and the algorithm are fast and efficient in its implementation. The method is based on the properties of numbers, slightly dependent on their digits, which is expected to provide it with a high degree of versatility.

Important role in the development of a method plays a study of the internal structure of the positive integers and the creation of their model, which includes a number of new concepts. Application of concepts such as contour, half contour, the interval boundaries of model objects and some other concepts ensure the development of individual models of odd numbers.

The introduction of the concept of f-invariant of odd numbers, for which two classes are considered: the left and right, opens the possibility to perform the transition from the traditional approach to solving the factorization problem to a retrieval task of partitions of a number of a special kind. It is expected that the problem would be less complicated.