

СИММЕТРИЧНОЕ ПРЕДСТАВЛЕНИЕ КОЛЬЦЕВОЙ ФАКТОРИЗАЦИИ ПРИ ПОИСКЕ ПРОСТЫХ ЧИСЕЛ

В.А. Минаев, М.П. Сычев, А. Вайш, Д.В. Никеров, С.А. Никонов

В статье сформулирована и доказана теорема о симметричном представлении кольцевой факторизации, позволяющем ускорить поиск простых чисел

Ключевые слова: информационная безопасность, простые числа, кольцевая факторизация, симметричное представление

Введение

При решении задачи нахождения полного множества простых чисел на определенном отрезке натурального ряда во многих современных алгоритмах используется предварительный отбор составных чисел. При этом для предварительного отбора составных чисел, как правило, применяется метод кольцевой факторизации [1]. Существо метода заключается в следующем: перемножаются несколько первых простых чисел, идущих подряд (математическая операция, известная как примориал), например, $3\# = 2 \times 3 = 6$, $5\# = 2 \times 3 \times 5 = 30$, $7\# = 2 \times 3 \times 5 \times 7 = 210$ и т.д. Затем строится таблица с числом столбцов, равным полученному примориалу, ячейки которой нумеруются по порядку так, как показано в таблицах 1 [2]. При этом для обобщения добавлена кольцевая факторизация для $2\# = 2$. В построенных таблицах отметим столбцы, которые начинаются: с единицы; с простых чисел, не участвовавших в получении примориала; а также со всевозможных произведений этих простых чисел, меньших примориала.

Владимир Александрович Минаев — МГТУ им. Н.Э. Баумана, д-р техн. наук, профессор, e-mail: m1va@yandex.ru

Михаил Павлович Сычев — МГТУ им. Н.Э. Баумана, д-р техн. наук, профессор, e-mail: mpsichov@sm.bmstu.ru

Abhishek Vaish — Indian Institute of Information Technology, Allahabad, MS, PhD
e-mail: abhishek.infosec@gmail.com

Дмитрий Викторович Никеров — Российский новый университет, аспирант, e-mail: dnik@bk.ru

Семен Андреевич Никонов — Российский новый университет, аспирант, e-mail: simon никонов@phystech.edu

Согласно методу кольцевой факторизации, в неотмеченных столбцах находятся только составные числа, за исключением всех участвовавших в получении примориала простых.

В дальнейшем будем опускать из рассмотрения неотмеченные столбцы, при этом учитывая все участвовавшие в получении примориала простые числа. Очевидно, что в отмеченных столбцах находятся простые числа, а также единица и оставшиеся после предварительного отбора составные числа. Определим понятие *порядка кольцевой факторизации*.

Определение 1.1 *Порядок кольцевой факторизации* — количество сомножителей примориала, используемого при построении соответствующей таблицы предварительного отбора составных чисел.

Метод кольцевой факторизации позволяет отсеять значительную часть составных чисел [1], а именно: для $3\#$ отсеивается 66,66...% всех составных чисел, для $7\#$ — больше 77%, а для $251\#$ — около 90%. На следующем этапе для исключения оставшихся составных чисел применяют различные алгоритмы: решето Эратосфена, решето Аткина и другие, а также современные алгоритмы, основанные на индексном представлении составных чисел в натуральном ряду [3-6].

Для удобства дальнейшего изложения примем следующие обозначения:

N_0 — множество всех натуральных чисел и $\{0\}$;

N — множество всех натуральных чисел;

Табличное отображение кольцевой факторизации для 2#, 3# и 5#

(a) 2#

1	2
3	4
5	6
...	...

(b) 3# = 2 × 3

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
...

(b) 5# = 2 × 3 × 5

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90
...	

$\{q\}$ — множество всех простых и составных чисел;

$\{c\}$ — множество всех составных чисел;

$\{p\}$ — множество всех простых чисел.

Для нумерации простых чисел подряд по возрастанию будем использовать левый верхний индекс: ${}^1 p = 2$, ${}^2 p = 3$, ${}^3 p = 5$, ${}^4 p = 7$ и т.д. Отметим также, что 1 является единственным натуральным числом, не являющимся ни простым, ни составным, т.е. $\{q\} = \mathbb{N} \setminus \{1\}$.

Переход к симметричному виду кольцевой факторизации

Пусть ${}^n p$ — n -е простое число. При исключении из отрезка натурального ряда $[1; {}^n p\#]$ чисел, равных и кратных ${}^1 p$, ${}^2 p$, ..., ${}^n p$, в нем останутся числа из первой строки таблицы кольцевой факторизации n -го порядка. При этом первая строка таблицы кольцевой факторизации первого порядка имеет $2 - 1 = 1$ число, первая строка таблицы кольцевой факторизации второго порядка имеет $(2 - 1) \times (3 - 1) = 2$ числа, первая строка таблицы кольцевой факторизации третьего порядка имеет $(2 - 1) \times (3 - 1) \times (5 - 1) = 8$ чисел и т.д. Определим функцию запаздывающего примориала (*retarded primorial*).

Определение 2. Функция запаздывающего примориала от аргумента $n \in \mathbb{N}$:

$${}^n p\#_{-1} = \prod_{i=1}^n \{{}^i p - 1\} \quad (1)$$

Отметим, что исследование асимптотики функции запаздывающего примориала представляет собой отдельную задачу.

При исключении из отрезка натурального ряда $[1; {}^n p\#]$ чисел, равных и кратных ${}^1 p$, ${}^2 p$, ..., ${}^n p$, в нем, согласно (1), останется ${}^n p\#_{-1}$ чисел из первой строки таблицы кольцевой факторизации n -го порядка.

Определим параметр s как следующую функцию от аргумента $n \in \mathbb{N}$:

$$\begin{aligned} n &= 1 : s = 0 \\ n &\geq 2 : s = {}^n p\#_{-1} / 2 - 1 \end{aligned} \quad (2)$$

Сформулируем и докажем теорему о симметричном представлении кольцевой факторизации второго и более старших порядков.

Теорема. Таблица кольцевой факторизации n -го порядка ($n \geq 2$) имеет ${}^n p\#_{-1}$ столбцов, числа в которых представимы в виде $\{{}^n p\# \cdot k \pm_0^n q\}$, $\{{}^n p\# \cdot k \pm_1^n q\}$, ..., $\{{}^n p\# \cdot k \pm_s^n q\}$, ..., $\{{}^n p\# \cdot k \pm_{s+1}^n q\}$, где k — номер строки таблицы кольцевой факторизации, $k \in \mathbb{N}$; ${}_0^n q = 1$; ${}_1^n q$, ..., ${}_r^n q$, ..., ${}_s^n q$ — не участвовавшие в получении ${}^n p\#$ простые числа и их произведения, меньшие ${}^n p\# / 2$ и записанные по возрастанию; s (2) — количество простых чисел и их произведений на интервале $({}^n p; {}^n p\# / 2)$; $r \in \{0; 1; \dots; s\}$.

Доказательство. Таблица кольцевой факторизации n -го порядка имеет " $p\#_{-1}$ " (1) столбцов, т.к. первая строка этой таблицы имеет столько же чисел.

Число " $p\#$ " по определению кратно числам ${}^1 p$, ${}^2 p$, ..., ${}^n p$, откуда на отрезке натурального ряда $[1; {}^n p\#]$ следует симметричность расположения чисел, равных и кратных ${}^1 p$, ${}^2 p$, ..., ${}^n p$, относительно " $p\#/2$ " ($\forall n \in \mathbb{N} \quad {}^n p\#\vdash 2$). Следовательно, числа первой строки таблицы кольцевой факторизации n -го порядка также имеют симметричное расположение относительно " $p\#/2$ ".

Поскольку при $n \geq 2$ количество чисел первой строки таблицы кольцевой факторизации n -го порядка будет четным, эти числа представимы в виде $\{{}^n p\# \pm {}_0^n q\}$, $\{{}^n p\# \pm {}_1^n q\}, \dots, \{{}^n p\# \pm {}_r^n q\}, \dots, \{{}^n p\# \pm {}_s^n q\}$, где ${}_0^n q = 1$; ${}_1^n q, \dots, {}_r^n q, \dots, {}_s^n q$ — не участвовавшие в получении " $p\#$ " простые числа и их произведения, меньшие " $p\#/2$ " и записанные по возрастанию; s (2) — количество простых чисел и их произведений на интервале $({}^n p; {}^n p\#/2)$; $r \in \{0; 1; \dots; s\}$.

Каждая следующая строка таблицы увеличивает значения чисел в столбцах на " $p\#$ ", следовательно, числа в k -той строке таблицы кольцевой факторизации n -го порядка представимы в виде $\{{}^n p\# \cdot k \pm {}_0^n q\}$, $\{{}^n p\# \cdot k \pm {}_1^n q\}, \dots, \{{}^n p\# \cdot k \pm {}_r^n q\}, \dots, \{{}^n p\# \cdot k \pm {}_s^n q\}$. \square

Определим индексы $i, j, k \in \mathbb{N}$. Введем обозначения:

$\{q_n p\#.k\}$ — множество всех простых и составных чисел, не равных и не кратных ${}^1 p$, ${}^2 p$, ..., ${}^n p$;

$\{c_n p\#.j\}$ — множество всех составных чисел, не кратных ${}^1 p$, ${}^2 p$, ..., ${}^n p$;

$\{p_n p\#.i\}$ — множество всех простых чисел, кроме ${}^1 p$, ${}^2 p$, ..., ${}^n p$.

В соответствии с теоремой о симметричном представлении кольцевой факторизации второго и более старших порядков, $\{q_n p\#.k\}$ можно разбить на " $p\#_{-1}$ " подмножества. Представим данные подмножества в виде матрицы $2 \times (s+1)$ (2):

$$\begin{Bmatrix} {}^{-0}_0 q \\ q \end{Bmatrix} \begin{Bmatrix} {}^{-1}_1 q \\ q \end{Bmatrix} \dots \begin{Bmatrix} {}^{-r}_r q \\ q \end{Bmatrix} \dots \begin{Bmatrix} {}^{-s}_s q \\ q \end{Bmatrix} \quad (3)$$

где $r \in \{0; 1; \dots; s\}$; $\forall n \geq 2$ k принимает все значения натурального ряда для каждого элемента матрицы подмножеств (3) $\{q_n p\#.k\}$, элементы которой представимы следующим образом:

$$\begin{aligned} q^{\pm {}_r^n q}_{n p\#.k} &= {}^n p\# \cdot k \pm {}_r^n q \\ c^{\pm {}_a^n q}_{n p\#.j} &= {}^n p\# \cdot j \pm {}_a^n q \\ p^{\pm {}_b^n q}_{n p\#.i} &= {}^n p\# \cdot i \pm {}_b^n q \end{aligned} \quad (4)$$

при этом $a, b \in \{0; 1; \dots; s\}$; знаки в левой и правой частях в каждом из соотношений (4) расставлены соответственно; $\forall n \geq 2$ при $a = b$ для одинаковых знаков второго и третьего соотношений (4) i и j совместно принимают все значения натурального ряда таким образом, что i принимает те значения, которые не принимает j , а j принимает те значения, которые не принимает i . Таким образом, $\{c_n p\#.j\}$ также можно разбить на

" $p\#_{-1}$ " подмножеств в виде матрицы $2 \times (s+1)$:

$$\begin{Bmatrix} {}^{-0}_0 q \\ c \end{Bmatrix} \begin{Bmatrix} {}^{-1}_1 q \\ c \end{Bmatrix} \dots \begin{Bmatrix} {}^{-a}_a q \\ c \end{Bmatrix} \dots \begin{Bmatrix} {}^{-s}_s q \\ c \end{Bmatrix} \quad (5)$$

$$\begin{Bmatrix} {}^{+0}_0 q \\ c \end{Bmatrix} \begin{Bmatrix} {}^{+1}_1 q \\ c \end{Bmatrix} \dots \begin{Bmatrix} {}^{+a}_a q \\ c \end{Bmatrix} \dots \begin{Bmatrix} {}^{+s}_s q \\ c \end{Bmatrix}$$

и $\{p_n p\#.i\}$ также можно разбить на " $p\#_{-1}$ " подмножеств в виде матрицы $2 \times (s+1)$:

$$\left\{ p_{^n p \# i}^{-n} q \right\} \left\{ p_{^n p \# i}^{-1} q \right\} \dots \left\{ p_{^n p \# i}^{-b} q \right\} \dots \left\{ p_{^n p \# i}^{-s} q \right\} \\ \left\{ p_{^n p \# i}^{+n} q \right\} \left\{ p_{^n p \# i}^{+1} q \right\} \dots \left\{ p_{^n p \# i}^{+b} q \right\} \dots \left\{ p_{^n p \# i}^{+s} q \right\} \quad (6)$$

Поскольку принадлежащие множеству $\{c_{^n p \# j}\}$ составные числа не делятся на $^1 p$, $^2 p$, ..., $^n p$, каждое принадлежащее множеству $\{c_{^n p \# j}\}$ составное число $c_{^n p \# j}^{\pm n} q$ может быть представлено в виде:

$$\forall n \in \mathbb{N}, \forall a \in \{0; 1; \dots; s\} \\ \exists i, k \in \mathbb{N}, b, r \in \{0; 1; \dots; s\}; \quad (7)$$

$$c_{^n p \# j}^{\pm n} q = p_{^n p \# i}^{\pm n} q \cdot q_{^n p \# k}^{\pm n} q$$

где $p_{^n p \# i}^{\pm n} q$ — простой делитель $c_{^n p \# j}^{\pm n} q$, при этом $p_{^n p \# i}^{\pm n} q \leq q_{^n p \# k}^{\pm n} q$.

Таким образом, с помощью доказанной теоремы мы вплотную подошли к описанию мультипликативного представления составных чисел множества $\{c_{^n p \# j}\}$ для более эффективного их отбора.

Заключение

В настоящей работе авторами обосновано симметричное представление кольцевой факторизации и приведено

доказательство соответствующей теоремы. Как показали расчеты, такое представление позволяет ускорить поиск простых чисел, что весьма важно при решении задач шифрования/дешифрования информации.

Литература

1. Wheel factorization – [Электронный ресурс]. URL: https://en.wikipedia.org/wiki/Wheel_factorization (Дата обращения: 25.05.2015).
2. Wheel factorization – [Электронный ресурс]. URL: <https://primes.utm.edu/glossary/xpage/WheelFactorization.html> (Дата обращения: 25.05.2015).
3. Минаев, В.А. Простые числа: новый взгляд на закономерности формирования. — М.: Логос, 2011. – 80 с.
4. Минаев, В.А., Васильев, Н.П., Лукьянов, В.В., Никонов, С.А., Никеров, Д.В. Высокопроизводительный алгоритм генерации простых чисел в произвольном диапазоне // Материалы XIV международной научной конференции «Цивилизация знаний: проблемы и смыслы образования». 2013. – М.: Изд-во РосНОУ. С. 494-498.
5. Минаев, В.А., Никонов, С.А., Никеров, Д.В. Симметричные формы индексных алгоритмов вычисления простых чисел. // Спецтехника и связь – М.: РосНОУ, – 2014. – №5. – С. 40-48.

6. Минаев, В.А., Никеров, Д.В., Никонов, С.А. Аддитивный индексный алгоритм вычисления простых чисел // Спецтехника и связь – М.: РосНОУ, – 2015. – №1. – С. 46-50.

ФГБОУ ВПО «Московский государственный технический университет имени Н.Э. Баумана»

Bauman Moscow state technical university

SYMMETRIC REPRESENTATION OF WHEEL FACTORIZATION IN SEARCH OF PRIMES

V.A. Minaev, M.P. Sychev, A. Vaish, D.V. Nikerov, S.A. Nikonorov

The article deals with definition and proof of the theorem on symmetric representation of wheel factorization, allowing accelerate search of primes

Key words: information security, primes, wheel factorization, symmetric representation