УДК 511.333;511.337

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЙ МОДИФИЦИРОВАННОГО СИММЕТРИЧНОГО ИНДЕКСНОГО АЛГОРИТМА ПОИСКА ПРОСТЫХ ЧИСЕЛ

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

В статье рассматривается результаты различных исследований модифицированного симметричного индексного алгоритма поиска простых чисел, результаты сведены в схему, отражающую улучшение в процентном соотношении

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

При решении задачи нахождения полного множества простых чисел на определенном отрезке натурального ряда во многих современных алгоритмах используется предварительный отбор составных чисел. Как правило, 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 приморилу, 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 приморилла; а также со всевозможных произведений этих простых чисел, меньших приморилла.

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

Авторы развили упомянутый метод и опубликовали ряд работ, в которых выполнены:

1) теоретическое обоснование и практическая реализация математической модели поиска простых чисел в произвольном диапазоне с помощью несимметричного индексного алгоритма произвольного порядка [1, 2];

2) теоретическое обоснование и практическая реализация математической модели поиска простых чисел в произвольном диапазоне с помощью симметричного индексного алгоритма произвольного порядка [3];

3) численные расчеты при практической реализации метода индексного алгоритма произвольного порядка с применением параллельных вычислений [4];

4) численные расчеты при сравнении времени отклика метода индексного алгоритма произвольного порядка и решета Аткина [5];

5) теоретическое обоснование и практическая реализация математической модели поиска простых чисел в произвольном диапазоне с помощью симметричного индексного алгоритма с использованием предварительного вероятностного тестирования [6];

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 — МГТУ им. Н.Э. Баумана, аспирант,
e-mail: simon.nikonov@phystech.edu

6) обобщение модели формирования простых чисел на основе симметричного представления кольцевой факторизации [7].

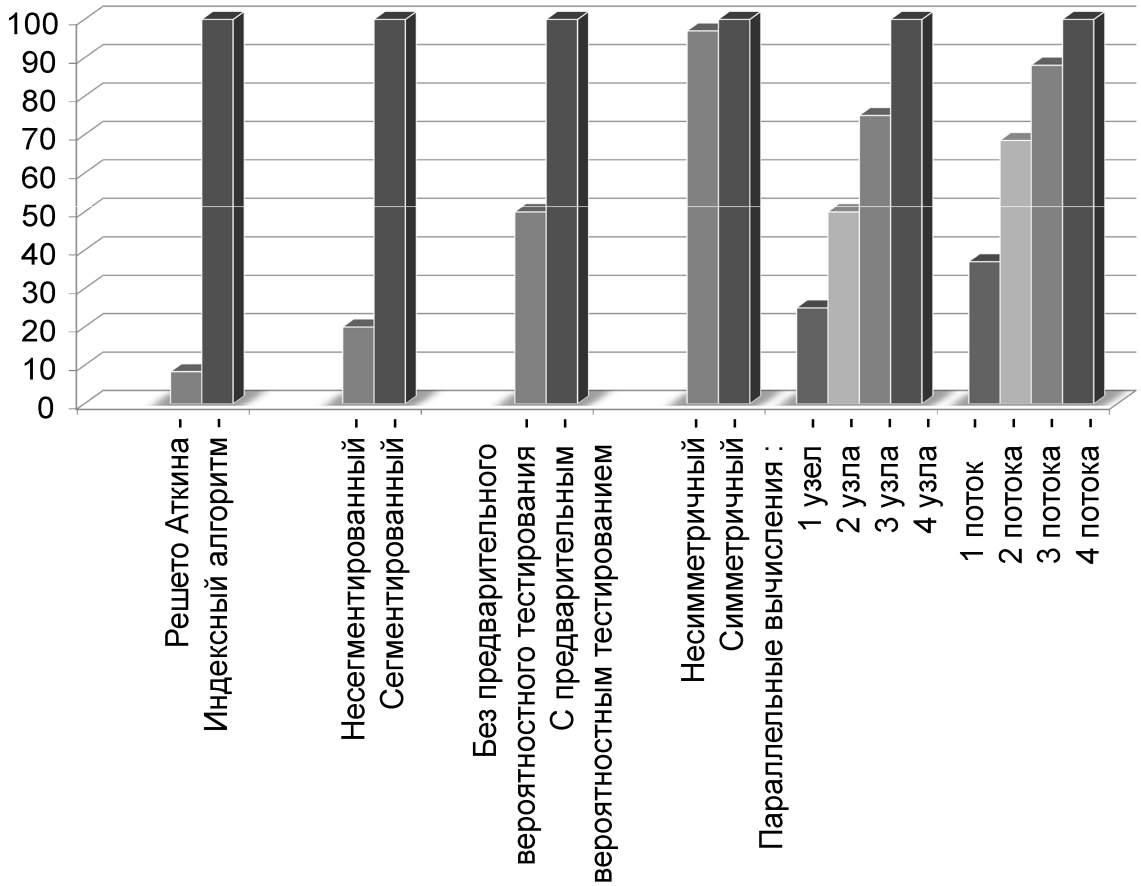

Рис. 1. Обобщенные результаты исследований комплекса программ, отражающие улучшение в процентном соотношении

Также разработан комплекс программ поиска простых чисел, который способен, исходя из условий поставленной задачи, исполнять соответствующие алгоритмы, обеспечивающие:

1) вероятностный тест на простоту Миллера-Рабина (из пакета *GMP*);

2) детерминированный тест на простоту Агравала-Каяла–Саксены;

3) симметричный индексный поиск простых чисел 64-битной разрядности;

4) симметричный индексный поиск простых чисел на длинной арифметике [8].

Использование индексных алгоритмов поиска простых чисел показало их преимущества, в ряде случаев - существенные, для решения прикладных задач. В частности сравнительное исследование быстродействия индексного алгоритма поиска простых чисел по отношению к алгоритму с наименьшей асимптотической сложностью – решету Аткина – показало, что для исследованной части натурального ряда индексный алгоритм работает значимо быстрее (в 12 раз), чем решето Аткина [5] (см. рис. 1).

Сравнение друг с другом несимметричных и симметричных индексных алгоритмов, реализованных в «длинной арифметике», показало, что симметричный алгоритм работает на 2-3% быстрее несимметричного.

Исследование влияния применения сегментирования отрезка поиска к индексным алгоритмам свидетельствует о том, что блочный индексный алгоритм работает в 5 раз быстрее обычного. При этом размер сегмента лучше всего выбирать равным половине от размера кэша второго уровня процессора, на котором исполняется алгоритм.

Табл. 1

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

(а) $2\#$

1	2
3	4
5	6
…	…

(б) $3\# = 2 \times 3$

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

(в) $5\# = 2 \times 3 \times 5$

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
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Произведенная оценка быстродействия индексного алгоритма поиска простых чисел с использованием технологий параллельных вычислений в зависимости от мощности используемой вычислительной системы показала, что на увеличение количества узлов алгоритм реагирует линейным увеличением производительности, на увеличение количества потоков в узле алгоритм реагирует нелинейно, но, тем не менее, значительно [4] (см. рис. 1).

Использование модифицированного индексного алгоритма поиска простых чисел с помощью предварительного тестирования на простоту для исследованной части натурального ряда, позволяет ускорить решение поставленной задачи в 2 раза, по сравнению с обычным индексным алгоритмом [6] (см. рис. 1).

Рассматривая полученные результаты, историю развития алгоритмов поиска простых чисел, изобразим с помощью схемы, приведенной на рис. 2.

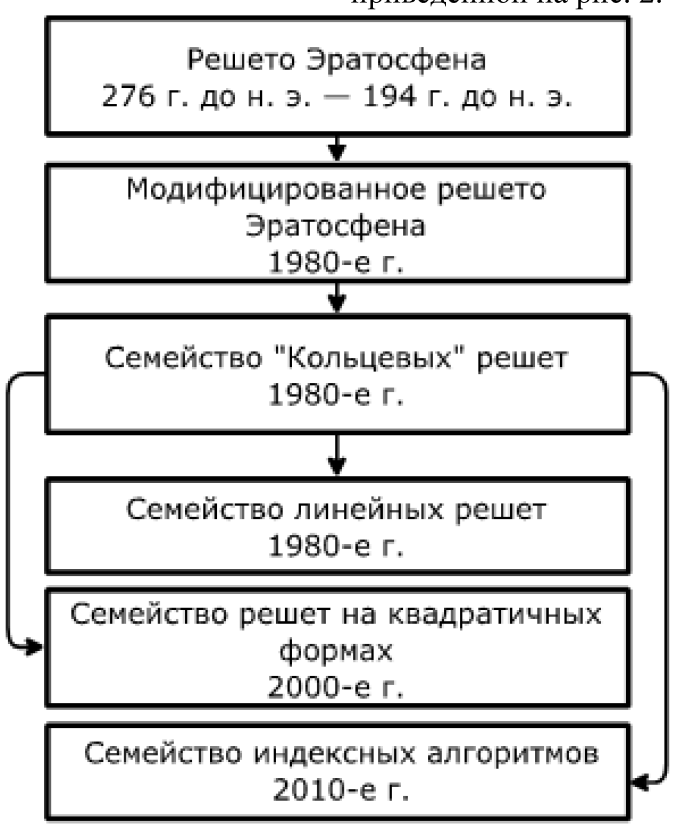

Рис. 2. Современное представление развития алгоритмов поиска простых чисел

Общим итогом исследований авторов выступает теоретическое и модельное обоснование индексного алгоритма поиска простых чисел, в том числе - его симметричной формы. Такой подход позволил увеличить производительность алгоритмов вычисления простых чисел, а, следовательно, как следствие, дал основание к разработке новых алгоритмов факторизации составных чисел.

Авторы надеются, что развитый ими математический аппарат приведет в ближайшей перспективе к новым открытиям в теории чисел и прикладных областях, связанных с применением простых чисел.

Литература

1. Минаев В.А. Высокопроизводительный алгоритм генерации простых чисел в произвольном диапазоне / Минаев В.А., Васильев Н.П., Лукьянов В.В., Никонов С.А., Никеров Д.В. // Сборник трудов Четырнадцатой Международной научной конференции «Цивилизация знаний: проблемы и смыслы образования». РосНОУ, 26-27 апреля 2013 г., Часть I, 2013 г. С.494-498.

2. Минаев В.А. Высокопроизводительный алгоритм генерации простых чисел в произвольном диапазоне с применением кольцевой факторизации/ Минаев В.А., Васильев Н.П., Лукьянов В.В., Никонов С.А., Никеров Д.В. // Спецтехника и связь, № 5, 2013 г. С.49-57.

3. Минаев В.А. Симметричные формы индексных алгоритмов вычисления простых чисел. / Минаев В.А., Никонов С.А., Никеров Д.В. // Спецтехника и связь, № 5, 2014 г. С.40-48.

4. Минаев В.А. Реализация индексных алгоритмов поиска простых чисел с помощью параллельных вычислений. / Минаев В.А., Сычев М.П., Никонов С.А., Никеров Д.В. // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение», № 6 (105), 2015 г. С.82-90.

5. Минаев В.А. Сравнение быстродействия модифицированного индексного алгоритма с решетом Аткина при поиске простых чисел. / Минаев В.А., Никонов С.А., Никеров Д.В. // Спецтехника и связь, № 2, 2015 г. С.38-41.

6. Минаев В.А. Вероятностный тест при поиске простых чисел с помощью модифицированного индексного алгоритма. / Минаев В.А., Сычев М.П., Никонов С.А., Никеров Д.В. // Спецтехника и связь, № 5, 2015 г. С.45-47.

7. Минаев В.А. Модель формирования простых чисел на основе симметричного представления кольцевой факторизации при отборе составных чисел. / Минаев В.А., Вайц Е.В., Никонов С.А., Никеров Д.В. // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение», № 1, 2016 г. С.89-97.

8. Никонов С.А. Свидетельство № 2015660307 от 28 сентября 2015 г. о регистрации программы «Программа поиска простых чисел по симметричному индексному алгоритму».

ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
Bauman Moscow State Technical University

RESEARCHING RESULTS OF MODIFIED SYMMETRIC INDEX ALGORITHM FOR PRIMES CALCULATING

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

The article deals with research results of modified index symmetric primes search algorithm, the results are summarized in the diagram, reflecting a percentage improvement

Key words: information security, Primes, wheel factorization