В.А. Минаев[1]

АЛГОРИТМ НАХОЖДЕНИЯ ВСЕХ ПРОСТЫХ ЧИСЕЛ

В статье уточняется классификация чисел натурального ряда, доказывается теорема о полном множестве простых чисел и дается описание линейного алгоритма нахождения всех простых чисел.

Ключевые слова: *теорема, алгоритм, простые числа.*

V.A. Minaev

ALGORITHM FOR FINDING ALL PRIME NUMBERS

In article classification of natural numbers is specified, the theorem on the complete set of primes is proved, the description of linear algorithm of all prime numbers finding is given.

Keywords: *theorem, algorithm, prime numbers.*

В работе производится уточнение классификации чисел натурального ряда, доказательство теоремы о полном множестве простых чисел и детальное описание алгоритма нахождения всех простых чисел.

Согласно основной теореме арифметики [1], впервые точно сформулированной и доказанной в книге К.Ф. Гаусса в 1801 году, каждое натуральное число $n > 1$ единственным образом представимо в виде:

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}, \qquad (1)$$

где $p_1 < p_2 < ... < p_k$ – простые числа, а α_1, ... , α_k – некоторые натуральные числа. Представление числа n в виде (1) называется его каноническим разложением.

Несмотря на особую роль соотношения (1) в теории чисел, его практическое применение, например для решения задач информационной безопасности, подчас затруднительно из-за вычислительной сложности оперирования с мультипликативным представлением натуральных чисел.

Вместе с тем, аддитивное представление любого составного числа через простые числа дает, с одной стороны, возможность существенного ускорения вычислительных процедур (в частности, при решении задач факторизации чисел), а с другой – позволяет эффективно подойти к решению многих математических проблем, включая проблему формального и однозначного описания полного множества простых чисел.

Аддитивное представление составных чисел вида $\{6k \pm 1\}$, $k = 1, 2, 3, ...$ впервые использовано в 2005 году при реализации программы «Линейный генератор простых чисел подряд», на которое получено свидетельство о регистрации [3]. В 2008 году опубликована работа, в которой приводится математическое описание формирования множеств как составных, так и простых чисел [4].

Уточнение классификации чисел натурального ряда

Для доказательства теоремы о полном множестве простых чисел уточним классификацию чисел натурального ряда.

С учетом того, что в современной математике натуральные числа определены неоднозначно (на самом деле, например 2 – одновременно простое и четное, 9 – одновременно нечетное и составное, 5 – одновременно нечетное и простое), для удобства дальнейшего изложения уточним их классификацию.

Для этого весь ряд натуральных чисел разобьем на следующие последовательные циклы подмножеств:

$$\{n_{k,l}\} = 6k + l, \qquad (2)$$

где k = 0, 1, 2, 3, …; l = 1, 2, 3, 4, 5, 6.

Очевидно, что при $k = 0$

$$\{n_{0,l}\} = \{1,\ 2,\ 3,\ 4,\ 5,\ 6\},$$

далее при $k = 1$

$$\{n_{1,l}\} = \{7,\ 8,\ 9,\ 10,\ 11,\ 12\},$$

при $k = 2$

$$\{n_{2,l}\} = \{13,\ 14,\ 15,\ 16,\ 17,\ 18\} \text{ и т.д.}$$

Таким образом, бесконечное множество чисел натурального ряда N состоит из сложения подмножеств $\{n_{k,l}\}$, где k = 0, 1, 2, 3,…; l = 1, 2, 3, 4, 5, 6.

$$\{N\} = \bigcup_{l=1}^{l=6} \bigcup_{k=0}^{\infty} \{n_{k,l}\}. \qquad (3)$$

Среди l простыми числами являются 2, 3 и 5, а 4 и 6 – составными. В каждом из подмножеств $\{n_{k,l}\}$ находятся и простые числа, и составные.

[1] Доктор технических наук, профессор, проректор НОУ ВПО «Российский новый университет».

Определим l, при котором число в подмножестве $\{n_{k,l}\}$ может быть простым.

Очевидно, что при любом k и l, равном 2, 4, 6, формируется *подмножество четных (двукратных) чисел* натурального ряда:

$$\{C_2\} = \{2,\ 4,\ 6,\ 8,\ ...\},$$

члены которого образуются по формуле:

$$c_2^m = 2 + 2m, \qquad (4)$$

где m = 0, 1, 2, 3, 4 … .

Напомним, что четных чисел в натуральном ряду – половина (50%), и их определение в данной работе – классическое.

Таким образом, первый член арифметической прогрессии (4) и ее разность равны первому простому числу 2.

Далее, для любого k при l, равном 3, формируется *подмножество троекратных чисел* натурального ряда:

$$\{C_3\} = \{3,\ 9,\ 15,\ ...\},$$

члены которого образуются с помощью соотношения:

$$c_3^m = 3 + 6m, \qquad (5)$$

где m = 0, 1, 2, 3, 4 … .

То есть троекратные числа образуются арифметической прогрессией с первым членом, равным простому числу 3, и разностью, равной шести. Таких чисел в составе натурального ряда – одна шестая – 16,666…%.

Очевидно, что троекратные числа входят в подмножество нечетных чисел в их классическом определении ($2n$ + 1), n = 0, 1, 2, 3, 4. При этом четные числа, кратные шести, согласно нашему определению (5), не являются троекратными, а относятся к четным.

Итак, по определению – подмножества четных и троекратных чисел не содержат простых чисел, кроме 2 и 3 – первых членов арифметических прогрессий (4) и (5).

Осталось рассмотреть варианты l = 1,5.

С учетом того, что $6k + 5 = 6(k + 1) - 1$, очевидно, что подмножества:

$$\{^{-}S\} = \{6(k+1) - 1\},\ \ k = 0,\ 1,\ 2,\ 3,\ 4,\ ...$$
$$\{^{+}S\} = \{6k + 1\},\ \ k = 1,\ 2,\ 3,\ 4,\ ... \qquad (6)$$

содержат все простые числа, кроме 2 и 3.

В работах [4, 5, 8] числа 2 и 3 названы *фундаментальными простыми числами*. И для такого определения есть все основания. Именно эти два числа напрямую в (4) и (5) либо с использованием их произведения в (6) с добавлением, либо вычитанием единицы формируют все до одного числа натурального ряда, начиная с 2.

Соотношения (6), содержа все простые числа, кроме 2 и 3, также включают и составные числа вида $\{6n \pm 1\}$, n = 1, 2, 3, … .

Для многих математиков, занимавшихся теорией чисел, задача – отделить друг от друга с помощью каких-либо формул, формальных процедур простые числа от составных, находящихся в множествах:

$$\{^{-}S\} = \{6n - 1\} \qquad (7)$$
$$\{^{+}S\} = \{6n + 1\},\ n = 1,\ 2,\ 3,\ 4,\ \ldots,$$

выступала на протяжении веков в качестве приоритетной задачи.

В таблице 1 для наглядности приведена бесконечная матрица последовательных циклов подмножеств $\{n_{k,l}\} = 6k + l;\quad k = 0,\ 1,\ 2,\ 3,\ ...;$ $l = 1,\ 2,\ 3,\ 4,\ 5,\ 6$. В столбцах 1 и 5 жирным цветом выделены простые числа, большие или равные 5. В столбцах 2 и 3 в нулевой строке выделены фундаментальные простые числа 2 и 3.

Анализ таблицы 1 показывает, что в первом столбце, начиная со второй строки, располагаются простые и составные числа с избыточной единицей для деления нацело на шесть. Назовем их, в соответствии с работой [5], где впервые дано их определение, *плюс простые числа* (ППЧ) и *плюс составные числа* (ПСЧ).

Таблица 1

Последовательные циклы подмножеств $\{n_{k,l}\} = 6k + l$

k / l	1	2	3	4	5	6
0	1	**2**	**3**	4	**5**	6
1	**7**	8	9	10	**11**	12
2	**13**	14	15	16	**17**	18
3	**19**	20	21	22	**23**	24
4	25	26	27	28	**29**	30
5	**31**	32	33	34	35	36
6	**37**	38	39	40	**41**	42
7	**43**	44	45	46	**47**	48
…	…	…	…	…	…	…
n	$6n$ + 1	$6n$ + 2	$6n$ + 4	$6n$ + 5	$6n$ + 5	$6n$ + 6
…	…	…	…	…	…	…

В пятом столбце, начиная с первой строки, расположены простые и составные числа с недостающей единицей для деления нацело на шесть. Их, соответственно, определим как *минус простые числа* (МПЧ) и *минус составные числа* (МСЧ) [5].

Нетрудно видеть, что последовательность чисел в первом столбце, начиная с 7, описывается арифметической прогрессией:

$$7, 7 + 6, 7 + 2 \cdot 6, ..., 7 + (n-1) \cdot 6;\ n = 1,\ 2,\ 3,\ \ldots, \qquad (8)$$

где первый член прогрессии равен 7, а ее разность – 6.

Поскольку первый член и разность прогрессии – натуральные взаимно простые числа, то она содержит, согласно теореме Дирихле о простых числах в арифметической прогрессии [6], бесконечное количество простых.

Аналогично последовательность чисел в пятом столбце, начиная с первой строки, описывается арифметической прогрессией:

$$5,5+6,5+2\cdot 6,...,5+(n-1)\cdot 6; n = 1, 2, 3, \dots, \quad (9)$$

где первый член прогрессии равен 7, а ее разность – 6. Очевидно, что и эта прогрессия в соответствии с теоремой Дирихле содержит бесконечное количество простых, так как первый член – 5 и разность прогрессии 6 – натуральные взаимно простые числа.

Таким образом, арифметические прогрессии (8) и (9) формируют все до одного простые числа, кроме фундаментальных простых – 2 и 3.

Исходя из приведенных рассуждений, множество простых чисел есть объединение:

• двухэлементного множества $\{2;\ 3\}$;

• вычитания из множества $\{^{+}S\}=\{6k+1\}$; $k=1,\ 2,\ 3,\ ...$ подмножества ПСЧ;

• вычитания из множества $\{^{-}S\}=\{6k-1\}$; $k=1,\ 2,\ 3,\ ...$ подмножества МСЧ.

Итогом выступает необходимая для дальнейших рассуждений классификация чисел натурального ряда на семь групп: четные числа; трехкратные числа; фундаментальные простые числа; минус простые числа; плюс простые числа; минус составные числа; плюс составные числа. Единица при этом выступает своеобразным «геномом» натурального ряда чисел.

Для нахождения полного множества простых чисел вида $\{6k\pm 1\}$, $k=1,\ 2,\ 3,\ ...$ формально опишем механизм образования ПСЧ и МСЧ.

Чтобы более наглядно представить этот механизм, а затем доказать *теорему о полном множестве простых чисел вида* $\{6k\pm 1\}$, $k=1,\ 2,\ 3,\ ...$ и реализовать алгоритм нахождения полного множества простых чисел (за исключением фундаментальных), расположим числа во множествах $\{^{-}S\}$ и $\{^{+}S\}$ друг против друга последовательно, начиная с 5 и 7 (таблица 2, жирным цветом выделены простые числа).

В таблице 2 введены следующие обозначения:

p_i^{-}, $i=1,\ 2,\ 3,\ ...$ – простое число из множества $\{6k-1\}$; $k=1,\ 2,\ 3,\ ...$ с недостающей единицей для деления нацело на 6 (МПЧ);

p_i^{+}, $i=1,\ 2,\ 3,\ ...$ – простое число из множества $\{6k+1\}$; $k=1,\ 2,\ 3,\ ...$ с избыточной единицей для деления нацело на 6 (ППЧ).

Таблица 2

Последовательности чисел из множеств $\{^{-}S\}$ и $\{^{+}S\}$

Индекс числа, i	$p_i^{-}; c_i^{-}$	$p_i^{+}; c_i^{+}$
1	**5**	**7**
2	**11**	**13**
3	**17**	**19**
4	**23**	25
5	**29**	**31**
6	35	**37**
7	**41**	**43**
8	**47**	49
9	**53**	55
10	**59**	**61**
11	65	**67**
…	…	…
n	$6n-1$	$6n+1$
…	…	…

Соответственно, c_i^{-} – составное число из множества $\{6k-1\}$; $k=1,\ 2,\ 3,\ ...$ с недостающей единицей для деления нацело на 6 (МСЧ), а c_i^{+} – составное число из множества $\{6k+1\}$; $k=1,\ 2,\ 3,\ ...$ с избыточной единицей для деления нацело на 6 (ПСЧ).

Покажем, что все МСЧ и ПСЧ (таблица 2) образуются с помощью арифметических прогрессий, где основную роль играют только простые числа и число 6 – как произведение фундаментальных простых чисел. А именно, первые члены арифметических прогрессий образуются в виде произведений простых чисел самих на себя или на простое, стоящее напротив в таблице 2. Разность же в таких прогрессиях равна произведению простого числа на 6.

Но, прежде всего, рассмотрим, к какому типу (МСЧ и ПСЧ), в зависимости от типа простых чисел (МПЧ и ППЧ), относится их произведение.

Первый случай:

$$p_i^{-}\cdot p_i^{-}=(6i-1)\cdot(6i-1)=36i^2-12i+1=$$
$$=6i(6i-2)+1=6k+1; \quad (10)$$
$$i = 1, 2, 3, \dots,$$

где $k=2i(3i-1)$.

То есть результат произведения – плюс составное число (ПСЧ).

Второй случай:

$$p_i^{+}\cdot p_i^{+}=(6i+1)\cdot(6i+1)=$$
$$36i^2+12i+1=6k+1; \quad (11)$$
$$i = 1, 2, 3, \dots,$$

где $k=2i(3i+1)$.

И в этом случае результат произведения – ПСЧ.

Третий случай:

$$p_i^- \cdot p_i^+ = (6i-1)\cdot(6i+1) = \\ = 36i^2 - 1 = 6k - 1; \\ i = 1, 2, 3, \dots, \tag{12}$$

где $k = 6i^2$.

В данном случае – результат произведения простых чисел – минус составное число (МСЧ).

Нетрудно показать, что при несовпадении индексов сомножителей в произведениях (10) – (12) результаты будут такими же, а также легко проверить, что произведение простого числа на составное из множеств $\{6k \pm 1\}$; k = 1, 2, 3, … , а также произведение составных из тех же множеств подчиняется указанному правилу.

Из рассмотрения представленных случаев вытекает ***правило знаков*** – *результат произведения любого количества простых чисел представляет собой ПСЧ, если в операции умножения участвует четное количество МПЧ, и МСЧ – в случае нечетного количества МПЧ.*

А теперь рассмотрим алгоритм нахождения всех простых чисел подряд.

Алгоритм нахождения всех простых чисел

Первый шаг

Минимальное составное число (ПСЧ) в таблице 2 равно 25. Оно формируется в результате умножения МПЧ 5 на само себя. Далее прибавлением к 25 6 · 5 = 30 формируется ПСЧ 55, затем к 55 прибавляется 30, получаем 85 и т.д. Таким образом, членами бесконечной арифметической прогрессии

$$25, 25 + 5\cdot 6, 25 + 5\cdot 6\cdot 2, 25 + \\ + 5\cdot 6\cdot 3, \dots, 25 + 5\cdot 6\cdot n, \dots, \tag{13}$$

где $n = 0, 1, 2, 3, \dots$, выступает множество ПСЧ, первый член которого равен 5 · 5 = 25, а разность равна 5 · 6 = 30.

Важно отметить, что для получения всего множества ПСЧ как результата последовательного умножения 5 на нижестоящие числа второго столбца – 11, 17, 23 и т.д. нет никакой необходимости производить саму операцию умножения. Это связано с тем, что из-за цикличности чисел первого столбца в таблице 2, обусловленной последовательным получением следующего числа путем сложения предыдущего с числом 6, все соответствующие ПСЧ образуются во втором столбце как члены арифметической прогрессии (13).

Итак, необходимость перемножения первого простого числа 5 на все остальные числа во втором столбце заменяется аддитивной арифметической прогрессией:

$$\left\{C_5^+\right\} = \left\{C_{p_1^-}^+\right\} = 5\cdot 5 + 5\cdot 6\cdot n; \\ n = 0, 1, 2, 3, \dots . \tag{14}$$

Второй шаг

Вычитаем из третьего столбца все ПСЧ, образованные арифметической прогрессией (14), и производим переиндексацию чисел, оставшихся в третьем столбце (таблица 3).

Третий шаг

Аналогично первому шагу находим следующее минимальное составное число. Оно равно произведению 5 · 7 = 35 и является по определению минус составным числом (МСЧ). Следующее МСЧ для простого числа 5 можно было бы найти путем умножения 5 · 13 = 65, затем следующее 5 · 19 = 95, но мы не будем этого делать, помня о свойстве аддитивной арифметической прогрессии:

$$\left\{C_5^-\right\} = \left\{C_{p_1^-}^-\right\} = 5\cdot 7 + 5\cdot 6\cdot n; \\ n = 0, 1, 2, 3, \dots . \tag{15}$$

Таблица 3

Последовательности чисел из множеств $\{^-S\}$ и $\{^+S\}$ после первой переиндексации

Индекс числа, i	p_i^-; c_i^-	p_i^+; c_i^+
1	**5**	**7**
2	**11**	**13**
3	**17**	**19**
4	**23**	**31**
5	**29**	**37**
6	35	**43**
7	**41**	49
8	**47**	**61**
9	**53**	**67**
10	**59**	**73**
11	65	**79**
…	…	…
n	$6n$ – 1	$6n$ + 1
…	…	…

Четвертый шаг

Вычитаем из второго столбца все МСЧ, образованные арифметической прогрессией (15), и производим вторую переиндексацию чисел (таблица 4).

Пятый шаг

Следующее минимальное составное число (МСЧ) 7 · 5 совпадает с 5 · 7. Однако, выступая первым членом прогрессии, формирует ее с другой разностью 7 · 6 = 42:

$$\left\{C_7^-\right\} = \left\{C_{p_1^+}^-\right\} = 7\cdot 5 + 7\cdot 6\cdot n; \\ n = 0, 1, 2, 3, \dots . \tag{16}$$

Таблица 4

Последовательности чисел из множеств $\{^{-}S\}$ и $\{^{+}S\}$ после второй переиндексации

Индекс числа, i	$p_i^-;\ c_i^-$	$p_i^+;\ c_i^+$
1	**5**	**7**
2	**11**	**13**
3	**17**	**19**
4	**23**	**31**
5	**29**	**37**
6	**41**	**43**
7	**47**	49
8	**53**	**61**
9	**59**	**67**
10	**71**	**73**
11	77	**79**
12	**83**	91
13	**89**	**97**
…	…	…
n	$6n-1$	$6n+1$
…	…	…

Учет эффекта «пересечения» различных арифметических прогрессий, формирующих составные числа из множеств $\{6n \pm 1\}$, n = 1, 2, 3, … , играет важную роль при решении задач интервальной оценки распределения простых чисел. Описание этого эффекта дано в работе [9, 10].

Шестой шаг

Вычитаем из второго столбца все МСЧ, образованные арифметической прогрессией (16), и производим третью переиндексацию чисел (таблица 5).

Таблица 5

Последовательности чисел из множеств $\{^{-}S\}$ и $\{^{+}S\}$ после третьей переиндексации

Индекс числа, i	$p_i^-;\ c_i^-$	$p_i^+;\ c_i^+$
1	**5**	**7**
2	**11**	**13**
3	**17**	**19**
4	**23**	**31**
5	**29**	**37**
6	**41**	**43**
7	**47**	49
8	**53**	**61**
9	**59**	**67**
10	**71**	**73**
11	**83**	**79**
12	**89**	91
…	…	…
n	$6n-1$	$6n+1$
…	…	…

Седьмой шаг

Наконец, для первой строки и третьего столбца простых чисел находим следующее составное число (ПСЧ), равное 7 · 7 = 49 и соответствующую арифметическую прогрессию:

$$\left\{C_7^+\right\} = \left\{C_{p_1^+}^+\right\} = 7 \cdot 7 + 7 \cdot 6 \cdot n; \quad n = 0,\ 1,\ 2,\ 3,\ \ldots . \tag{17}$$

Восьмой шаг

Вычитаем из третьего столбца ПСЧ, образованные арифметической прогрессией (17), и производим четвертую переиндексацию чисел (таблица 6).

Важно отметить, что описанное последовательное нахождение составных чисел (МСЧ и ПСЧ) начинается с минимального ПСЧ, равного 25, а затем их «размножение» с помощью арифметических прогрессий, формирующих $\left\{C_{p_i^-}^-\right\}$, $\left\{C_{p_i^+}^-\right\}$, $\left\{C_{p_i^-}^+\right\}$ и $\left\{C_{p_i^+}^+\right\}$, дает возможность нахождения *всех составных чисел подряд* вида $\{6k \pm 1\}$; $k = 1,\ 2,\ 3,\ \ldots$ без каких-либо пропусков. Также без пропусков находятся *все простые числа* вида $\{6k \pm 1\}$; k = 1, 2, 3, … .

Таблица 6

Последовательности чисел из множеств $\{^{-}S\}$ и $\{^{+}S\}$ после четвертой переиндексации

Индекс числа, i	$p_i^-;\ c_i^-$	$p_i^+;\ c_i^+$
1	**5**	**7**
2	**11**	**13**
3	**17**	**19**
4	**23**	**31**
5	**29**	**37**
6	**41**	**43**
7	**47**	**61**
8	**53**	**67**
9	**59**	**73**
10	**71**	**79**
11	**83**	**97**
12	**89**	**103**
…	…	…
n	$6n-1$	$6n+1$
…	…	…

Итак, в результате восьми шагов в таблице 6 до индекса i = 12 остались только простые числа. Повторяя последовательно восьмишаговую процедуру «фильтрации» простых чисел для других строк таблицы 6 путем удаления из множеств $\{^{-}S\}$ и $\{^{+}S\}$ составных чисел (МСЧ и ПСЧ), образуемых соответствующими арифметическими прогрессиями, можно найти *все до одного* простые числа в любом интервале от 1 до n. При этом однозначно определяется индекс любого ППЧ и МПЧ в указанном интервале.

Столь детальное описание алгоритма нахождения простых чисел сделано и для того, чтобы показать, что он в корне отличается от известных алгоритмов – решета Эратосфена и его модификаций (решета Сундарма и т.п.), а также решета Аткина и других современных алгоритмов.

В отличие от предыдущих, в данном алгоритме используются ***уравнения, описывающие механизм формирования составных чисел*** вида $\{6k \pm 1\}$, $k = 1, 2, 3, \ldots$ и дающие возможность однозначно выделить *все простые числа* из множеств $\{6k \pm 1\}$, $k = 1, 2, 3, \ldots$ [4, 8].

Покажем, что с помощью приведенного алгоритма находится полное множество простых чисел, за исключением фундаментальных простых чисел. Для этого докажем специальную теорему.

Теорема о полном множестве простых чисел вида $\{6k \pm 1\}$, $k = 1, 2, 3, \ldots$.

Полное множество простых чисел вида $\{6k + 1\}$, $k = 1, 2, 3, \ldots$ *формируется путем вычитания из множества* $\{{}^{+}S\}$ *подмножества чисел, определяемых с помощью уравнений:*

$$\begin{gathered} c^{+}_{p_i^-} = p_i^- \cdot p_i^- + p_i^- \cdot 6m \\ c^{+}_{p_i^+} = p_i^+ \cdot p_i^+ + p_i^+ \cdot 6m; \\ m = 0, 1, 2, 3, \ldots ; i = 1, 2, 3, \ldots , \end{gathered} \qquad (18)$$

а полное множество простых чисел вида $\{6k - 1\}$, $k = 1, 2, 3, \ldots$ *– путем вычитания из множества* $\{{}^{-}S\}$ *подмножества чисел, вычисляемых из соотношений:*

$$\begin{gathered} c^{-}_{p_i^-} = p_i^- \cdot p_i^+ + p_i^- \cdot 6m \\ c^{-}_{p_i^+} = p_i^+ \cdot p_i^- + p_i^+ \cdot 6m; \\ m = 0, 1, 2, 3, \ldots ; i = 1, 2, 3, \ldots . \end{gathered} \qquad (19)$$

Для доказательства рассмотрим таблицу 2, в которой числа из множеств $\{{}^{-}S\}$ и $\{{}^{+}S\}$ расположены друг против друга с периодом 6 в виде двух бесконечных столбцов, начиная с минимальных – 5 и 7. Обозначим числа в указанных множествах, соответственно, как q_i^- и q_i^+, $i = 1, 2, 3, \ldots$.

Очевидно, применительно к обозначениям в виде множеств, имеем:

$$\begin{gathered} \{q_i^-\} = \{p_i^-\} \cup \{c_i^-\}; \\ \{q_i^+\} = \{p_i^+\} \cup \{c_i^+\}. \end{gathered} \qquad (20)$$

Минимальное составное число вида $\{6k + 1\}$; $k = 1, 2, 3, \ldots$ (т.е. минимальное ПСЧ) равно произведению минимального простого числа $q_1^- = 5$ само на себя, т.е. $q_1^- \cdot q_1^- = c^{+}_{q_1^- \cdot q_1^-} = 25$. Перемножая q_1^- последовательно на все нижестоящие числа (таблица 2) во множестве $\{{}^{-}S\}$, получаем последовательно без пропусков бесконечный ряд ПСЧ в виде:

$$\left\{C^{+}_{q_1^- \cdot q_l^-}\right\} = \left\{q_1^- \cdot q_1^-; q_1^- \cdot q_2^-; q_1^- \cdot q_3^-; \ldots; q_1^- \cdot q_l^-; \ldots\right\}; \qquad (21)$$

при $l \to \infty$.

Так как множество $\{{}^{-}S\}$ включает **все** простые и составные числа вида $\{6k - 1\}$, $i = 1, 2, 3, \ldots$, очевидно, что путем последовательных умножений, отраженных в (21), в итоге получаем **все** до одного ПСЧ (см. правило знаков), куда входит в качестве сомножителя q_1^-.

Вычитая из множества $\{{}^{+}S\}$ подмножество $\left\{C^{+}_{q_1^- \cdot q_l^-}\right\}$, при $l \to \infty$, получаем бесконечное подмножество $\left\{{}^{+}S_{q_1^-}\right\}$:

$$\left\{{}^{+}S_{q_1^-}\right\} = \{{}^{+}S\} \setminus \left\{C^{+}_{q_1^- \cdot q_l^-}\right\}, \text{ при } l \to \infty, \qquad (22)$$

состоящее из всех ППЧ и ПСЧ, за исключением тех, куда в качестве сомножителя входит q_1^-.

На следующем шаге доказательства сформируем подмножество $\left\{{}^{+}S_{q_2^-}\right\}$:

$$\left\{{}^{+}S_{q_2^-}\right\} = \left\{{}^{+}S_{q_1^-}\right\} \setminus \left\{C^{+}_{q_2^- \cdot q_l^-}\right\}, \text{ при } l \to \infty, \qquad (23)$$

где

$$\left\{C^{+}_{q_2^- \cdot q_l^-}\right\} = \left\{q_2^- \cdot q_2^-; q_2^- \cdot q_3^-; \ldots; q_2^- \cdot q_l^-; \ldots\right\}; \qquad (24)$$

при $l \to \infty$.

Очевидно, что подмножество $\left\{{}^{+}S_{q_2^-}\right\}$ также состоит из бесконечного количества ППЧ и ПСЧ, куда в виде сомножителей не входят q_1^- и q_2^-.

Продолжая до бесконечности операции вычитания типа (22) и (23), получим подмножество:

$$\left\{{}^{+}S_{q_\infty^-; q_\infty^-}\right\} = \left\{{}^{+}S\right\} \setminus \left\{{}^{+}C_{q_1^- \cdot q_l^-}\right\} \setminus \left\{C^{+}_{q_2^- \cdot q_l^-}\right\} \setminus \ldots \setminus \left\{C^{+}_{q_k^- \cdot q_l^-}\right\} \ldots, \qquad (25)$$

(где $l \to \infty$, $k \to \infty$), состоящее из всех ППЧ и ПСЧ, за исключением тех, куда в виде сомножителей входят числа из подмножества $\{{}^{-}S\}$.

В общем случае:

$$\left\{{}^{+}S_{q_k^-}\right\} = \left\{{}^{+}S_{q_{k-1}^-}\right\} \setminus \left\{q_k^- \cdot q_k^-; q_k^- \cdot q_{k+1}^-; \ldots; q_k^- \cdot q_l^-; \ldots\right\}; \qquad (26)$$

$$l \to \infty.$$

Как нетрудно заметить, члены бесконечных подмножеств ПСЧ $\left\{C^{+}_{q_k^- \cdot q_l^-}\right\}$ в соотношениях (21), (24), (25) находятся из уравнений арифметических прогрессий:

$$c^{-}_{q_i^-} = q_i^- \cdot q_i^- + q_i^- \cdot 6m; \quad m = 0, 1, 2, 3. \qquad (27)$$

Таким образом, мультипликативные соотношения в (21), (24), (26) замещаются на аддитивные в (27).

Нужно также указать, что при использовании в (27) не только простых p_i^-, $i = 1, 2, 3, \ldots$, но и составных, формируемых от простых, образуются «дубли» ПСЧ, однако это никак не сказывается на итоговом соотношении (25), предполагающем исключение на каждом шаге всех состав-

ных, включая «дубли», образуемых соответствующими q_k^-, $k = 1, 2, 3, \ldots$.

Чтобы получить полное множество всех плюс простых чисел (ППЧ), необходимо далее из множества (25) – $\left\{{}^+S_{q_\infty^-}\right\}$ исключить все ПСЧ, образуемые числами из бесконечного множества $\left\{{}^+S\right\}$ вида $\{6k+1\}$; $k = 1, 2, 3, \ldots$. Минимальное составное число вида $\{6k+1\}$; $k = 1, 2, 3, \ldots$, образуемое числами из множества $\left\{{}^+S\right\}$ вида $\{6k+1\}$; $k = 1, 2, 3, \ldots$ равно минимальному простому $q_1^+ = 7$, умноженному само на себя, $q_1^+ \cdot q_1^+ = c^+_{q_1^+ \cdot q_1^+} = 49$.

Перемножая q_1^+ последовательно на все нижестоящие числа (см. таблицу 2) из множества $\left\{{}^+S\right\}$, так же как и в (21), последовательно, без пропусков получим бесконечный ряд ПСЧ в виде:

$$\left\{C^+_{q_1^+ \cdot q_l^+}\right\} = \left\{q_1^+ \cdot q_1^+; q_1^+ \cdot q_2^+; q_1^+ \cdot q_3^+; \ldots; q_1^+ \cdot q_l^+; \ldots\right\}; \quad (28)$$

при $l \to \infty$.

Поскольку множество $\left\{{}^+S\right\}$ включает по определению **все** простые и составные числа вида $\{6k+1\}$; $k = 1, 2, 3, \ldots$, получаем в (28) множество всех до одного ПСЧ, куда в виде сомножителя входит q_1^+.

Вычитая из множества $\left\{{}^+S_{q_\infty^-}\right\}$ подмножество $\left\{C^+_{q_1^+ \cdot q_l^+}\right\}$, при $l \to \infty$, получим бесконечное подмножество $\left\{{}^+S_{q_\infty^-}\right\}$, состоящее из всех ППЧ и ПСЧ, за исключением тех, куда в виде сомножителей входят все числа из $\left\{{}^-S\right\}$ и q_1^+:

$$\left\{{}^+S_{q_\infty^-; q_1^+}\right\} = \left\{{}^+S_{q_\infty^-}\right\} \setminus \left\{C^+_{q_1^+ \cdot q_l^+}\right\}, \text{ при } l \to \infty. \quad (29)$$

Продолжая далее логику доказательства, реализованную в (21) – (26) применительно к системе последовательных вычитаний из множества $\left\{{}^+S\right\}$ подмножеств $\left\{C^+_{q_k^- \cdot q_l^-}\right\}$; $k = 1, 2, 3, \ldots$; $l = 1, 2, 3, \ldots$, в конечном итоге получим:

$$\left\{{}^+S_{q_\infty^-; q_\infty^+}\right\} = \left[\left\{{}^+S\right\} \setminus \left\{{}^+S_{q_1^-}\right\} \setminus \left\{{}^+S_{q_2^-}\right\} \setminus \ldots \setminus \left\{{}^+S_{q_k^-}\right\} \ldots\right] \setminus$$
$$\left\{{}^+S_{q_1^+}\right\} \setminus \left\{{}^+S_{q_2^+}\right\} \setminus \ldots \setminus \left\{{}^+S_{q_k^+}\right\} \ldots; \quad (30)$$

при $k \to \infty$.

Поскольку из множества $\left\{{}^+S\right\}$ вычтены все до одного ПСЧ вида $\{6k+1\}$; $k = 1, 2, 3, \ldots$, то есть все числа, образованные всеми возможными произведениями, очевидно, что

$$\left\{{}^+S_{q_\infty^-; q_\infty^+}\right\} = \left\{p_i^+\right\}; \; i = 1, 2, 3, \ldots, \quad (31)$$

где в правой части $\left\{p_i^+\right\}$; $i = 1, 2, 3, \ldots$ есть полное множество плюс простых чисел (ППЧ) вида $\{6k+1\}$; $k = 1, 2, 3, \ldots$.

Нетрудно видеть, что ПСЧ, входящие в бесконечные подмножества $\left\{C^+_{q_k^+ \cdot q_l^+}\right\}$ в соотношениях (28) – (29), находятся из уравнений арифметических прогрессий:

$$c^+_{q_i^+} = q_i^+ \cdot q_i^+ + q_i^+ \cdot 6m; \; m = 0, 1, 2, 3, \ldots . \quad (32)$$

И также соответствующие «дубли» составных чисел (ПСЧ), появляющиеся из-за использования в (32) не только простых, но и составных чисел, очевидно, не влияют на конечный результат в виде (31).

По аналогии с процедурой доказательства полноты множества ППЧ $\left\{p_i^+\right\}$; $i = 1, 2, 3, \ldots$, использующей соотношения (21) – (32), для нахождения полного множества МПЧ $\left\{{}^-S_{q_\infty^-; q_\infty^+}\right\} = \left\{p_i^-\right\}$; $i = 1, 2, 3, \ldots$ сформируем минимальное составное число вида $\{6k-1\}$; $k = 1, 2, 3, \ldots$.

Очевидно, используя правило знаков, минимальное МСЧ равно произведению минимального простого числа $q_1^- = 5$ на число, стоящее напротив в таблице 2, т.е. на $q_1^+ = 7$, при этом $q_1^- \cdot q_1^+ = c^-_{q_1^- \cdot q_1^+} = 35$.

Перемножая q_1^- последовательно на все нижестоящие числа (см. таблицу 2) из множества $\left\{{}^+S\right\}$, получаем последовательно без пропусков бесконечный ряд МСЧ в виде:

$$\left\{C^-_{q_1^- \cdot q_l^+}\right\} = \left\{q_1^- \cdot q_1^+; q_1^- \cdot q_2^+; q_1^- \cdot q_3^+; \ldots; q_1^- \cdot q_l^+; \ldots\right\}; \quad (33)$$

при $l \to \infty$.

Так как множество $\left\{{}^+S\right\}$ включает *все* простые и составные числа вида $\{6k+1\}$, $k = 1, 2, 3, \ldots$, то путем последовательных умножений, отраженных в (33), получаем *все* до одного МСЧ (см. правило знаков), куда в виде сомножителя входит q_1^-.

Вычитая из множества $\left\{{}^-S\right\}$ подмножество $\left\{C^-_{q_1^- \cdot q_l^+}\right\}$, при $l \to \infty$, получаем бесконечное подмножество $\left\{{}^-S_{q_1^-}\right\}$:

$$\left\{{}^-S_{q_1^-}\right\} = \left\{{}^-S\right\} \setminus \left\{C^-_{q_1^- \cdot q_l^+}\right\}, \text{ при } l \to \infty, \quad (34)$$

состоящее из всех МПЧ и МСЧ, за исключением тех, куда в качестве сомножителя входит q_1^-.

Продолжая до бесконечности операции вычитания типа (34), получим подмножество:

$$\left\{{}^-S_{q_\infty^-}\right\} = \left\{{}^-S\right\} \setminus \left\{C^-_{q_1^- \cdot q_l^+}\right\} \setminus \left\{C^-_{q_2^- \cdot q_l^+}\right\} \setminus \ldots \setminus \left\{C^-_{q_k^- \cdot q_l^+}\right\} \ldots, \quad (35)$$

где $l \to \infty$, $k \to \infty$, состоящее из всех МПЧ и МСЧ, за исключением тех, куда в виде сомножителей входят числа из подмножества $\left\{{}^-S\right\}$.

Члены бесконечных подмножеств ПСЧ $\left\{C^-_{q_k^- \cdot q_l^+}\right\}$ в соотношениях (33) – (35) находятся из уравнений арифметических прогрессий (19):

$$c^-_{q_i^-} = q_i^- \cdot q_i^+ + q_i^- \cdot 6m; \; m = 0, 1, 2, 3, \ldots, \quad (36)$$

при этом мультипликативные соотношения замещаются на аддитивные.

Чтобы получить множество всех минус простых чисел (МПЧ), необходимо далее из множества (35) – $\left\{{}^{-}S_{q_\infty^-}\right\}$ исключить все МСЧ, образуемые числами из бесконечного множества $\left\{{}^{+}S\right\}$ вида $\{6k+1\}$; $k = 1, 2, 3, \ldots$.

Минимальное МСЧ вида $\{6k-1\}$; $k = 1, 2, 3, \ldots$, образуемое числами из множества $\left\{{}^{+}S\right\}$ вида $\{6k+1\}$; $k = 1, 2, 3, \ldots$, равно, как и в предыдущем случае, $q_1^+ \cdot q_1^- = c^-_{q_1^+ \cdot q_1^-} = 35$.

Перемножая q_1^+ последовательно на все нижестоящие числа (см. таблицу 2) из множества $\left\{{}^{-}S\right\}$, также без пропусков получим бесконечный ряд МСЧ в виде:

$$\left\{C^-_{q_1^+ \cdot q_l^-}\right\} = \left\{q_1^+ \cdot q_1^-; q_1^+ \cdot q_2^-; q_1^+ \cdot q_3^-; \ldots; q_1^+ \cdot q_l^-; \ldots\right\}; \qquad (37)$$

при $l \to \infty$.

Так как $\left\{{}^{+}S\right\}$ включает по определению *все* простые и составные числа вида $\{6k+1\}$; $k = 1, 2, 3, \ldots$, получаем в (37) множество всех до одного МСЧ, куда входит q_1^+.

Вычитая из множества $\left\{{}^{-}S_{q_\infty^-}\right\}$ подмножество $\left\{C^-_{q_1^+ \cdot q_l^-}\right\}$, при $l \to \infty$, получим бесконечное подмножество $\left\{{}^{-}S_{q_\infty^-; q_1^+}\right\}$, состоящее из всех МПЧ и МСЧ, за исключением тех, куда в виде сомножителей входят все числа из $\left\{{}^{-}S\right\}$ и q_1^+:

$$\left\{{}^{-}S_{q_\infty^-; q_\infty^+; q_1^+}\right\} = \left\{{}^{-}S_{q_\infty^-; q_\infty^+}\right\} \setminus \left\{C^-_{q_1^+ \cdot q_l^-}\right\}, \qquad (38)$$

при $l \to \infty$.

Продолжая далее последовательные вычитания из множества $\left\{{}^{-}S_{q_\infty^-; q_1^+}\right\}$ подмножества $\left\{C^-_{q_k^+ \cdot q_l^-}\right\}$, $k = 2, 3, \ldots$, $l = 2, 3, \ldots$ в конечном итоге получим:

$$\left\{{}^{-}S_{q_\infty^-; q_\infty^+}\right\} = \left[\left\{{}^{-}S\right\} \setminus \left\{{}^{-}S_{q_1^-}\right\} \setminus \left\{{}^{-}S_{q_2^-}\right\} \setminus \ldots \setminus \left\{{}^{-}S_{q_k^-}\right\} \ldots\right] \setminus$$

$$\setminus \left\{{}^{-}S_{q_1^+}\right\} \setminus \left\{{}^{-}S_{q_2^+}\right\} \setminus \ldots \setminus \left\{{}^{-}S_{q_k^+}\right\} \ldots \text{, при } k \to \infty. \qquad (39)$$

Очевидно, что

$$\left\{{}^{-}S_{q_\infty^-; q_\infty^+}\right\} = \left\{p_i^-\right\}, \; i = 1, 2, 3, \ldots . \qquad (40)$$

МСЧ, входящие в бесконечные подмножества $\left\{C^-_{q_k^+ \cdot q_l^-}\right\}$ в соотношениях (37) – (39), находятся из уравнений арифметических прогрессий:

$$c^-_{q_i^+} = q_i^+ \cdot q_i^- + q_i^+ \cdot 6m, \; m = 0, 1, 2, 3, \ldots , \qquad (41)$$

и в этом случае «дубли» МСЧ, появляющиеся из-за использования в (41) не только простых, но и составных чисел, не влияют на конечный результат в виде (40).

Таким образом, теорема о полном множестве простых чисел вида $\{6k \pm 1\}$, $k = 1, 2, 3, \ldots$ *доказана.*

Используя результаты доказательства теоремы, восьмишаговый циклический алгоритм нахождения всех простых чисел подряд, который мы описали, можно существенно упростить, используя формальное представление механизма образования составных чисел вида $\{6k \pm 1\}$, $k = 1, 2, 3, \ldots$ в виде (18) – (19).

Основными особенностями предлагаемого ниже алгоритма являются:

• простота реализации по сравнению с другими алгоритмами нахождения простых чисел;

• линейная зависимость времени расчета от числа *n* натурального ряда;

• возможность быстрого вычисления всех простых чисел подряд из множеств $\{6k \pm 1\}$, $k = 1, 2, 3, \ldots$.

Суть алгоритма заключается в реализации следующих пяти этапов.

1. Определяется натуральное число *n*, применительно к которому необходимо вычислить все простые числа, его не превосходящие.

2. Вычисляются два ряда проиндексированных натуральных чисел q_i^- и q_i^+, $i = 1, 2, 3, \ldots$ из множеств $\{6k-1\}$ и $\{6k+1\}$, $k = 1, 2, 3, \ldots$, не превосходящих *n*.

3. Находятся все решения следующих уравнений, не превышающие *n*.

$$\begin{aligned} c^+_{q_i^-} &= q_i^- \cdot q_i^- + q_i^- \cdot 6m \\ c^+_{q_i^+} &= q_i^+ \cdot q_i^+ + q_i^+ \cdot 6m \\ c^-_{q_i^-} &= q_i^- \cdot q_i^+ + q_i^- \cdot 6m \\ c^-_{q_i^+} &= q_i^+ \cdot q_i^- + q_i^- \cdot 6m, \end{aligned} \qquad (42)$$

$m = 0, 1, 2, 3, \ldots ; i = 1, 2, 3, \ldots$.

4. Из множества $\{6k-1\}$, $k = 1, 2, 3, \ldots$ вычитается объединение множеств $\left\{C^-_{q_i^-}\right\} \bigcup \left\{C^-_{q_i^+}\right\}$, $i = 1, 2, 3, \ldots$, а из множества $\{6k+1\}$, $k = 1, 2, 3, \ldots$ – объединение множеств $\left\{C^+_{q_i^-}\right\} \bigcup \left\{C^+_{q_i^+}\right\}$, $i = 1, 2, 3, \ldots$.

5. Полученные в результате операций вычитания простые числа, не превышающие *n*, располагаются в порядке возрастания, и каждому простому присваивается соответствующий индекс $j = 1, 2, 3, \ldots$.

Отметим, что использование q_i вместо p_i в соотношениях (42) значительно:

• ускоряет (и упрощает) процедуру нахождения простых чисел из-за отсутствия операций промежуточного вычитания и переиндексации чисел, использованных в описанном восьмишаговом циклическом алгоритме;

• упрощает различные оценочные операции работы алгоритма в связи с тем, что разница между стоящими друг против друга q_i^- и q_i^+ всегда равна 2.

При этом итоговые результаты работы по нахождению всех простых чисел вида $\{6k \pm 1\}$, $k =$

= 1, 2, 3, … в интервале (0, n) остаются теми же, что и при применении детализированного восьмишагового алгоритма.

Безусловно, возникают дополнительные вычисления, связанные с нахождением вторичных, третичных и т.д. «пересечений», формирующихся в уравнениях (24). Например, все ПСЧ, формируемые арифметической прогрессией $\left\{C_5^+\right\} = 5 \cdot 5 + 5 \cdot 6 \cdot m$; m = = 0, 1, 2, … , включают все ПСЧ от арифметических прогрессий $\left\{C_{25}^+\right\} = 25 \cdot 25 + 25 \cdot 6 \cdot m$; $\left\{C_{625}^+\right\} = 625 \cdot 625 + 625 \cdot 6 \cdot m$; $m = 0, 1, 2, \ldots$ и т.д.

Однако преимущества использования уравнений (42) вместо (18) и (19) при вычислении простых чисел в смысле скорости и простоты расчетов существенно превышает те издержки, которые возникают в связи с необходимостью учета дополнительных вторичных, третичных и т.д. «пересечений».

В таблице 7 приведен пример работы алгоритма нахождения простых чисел до 1000.

Индекс плюс и минус простых чисел указан курсивом в центральном столбце таблицы. Правый от центрального столбец содержит ППЧ (выделены жирным шрифтом) и ПСЧ. Левый от центрального столбец содержит МПЧ (выделены жирным шрифтом) и МСЧ. Все остальные столбцы справа содержат ПСЧ вида $\{6k+1\}$, $k = 1, 2, 3, \ldots$, образуемые первыми двумя уравнениями (42) и не превышающие 1000.

Соответственно, остальные столбцы слева содержат МСЧ вида $\{6k-1\}$, $k = 1, 2, 3, \ldots$, образуемые последними двумя уравнениями (42) и не превышающие 1000. Нижние индексы составных чисел равны первым членам арифметических прогрессий (42).

Оценим зависимость $q_{i_{\max}}$ от n. Для начала рассмотрим первые два уравнения (42).

Очевидна справедливость следующего равенства:

$$q_i^2 + 6q_i \cdot m + 6q_i \cdot \varepsilon_{q_i} - n = 0; \quad i = 1, 2, 3, \ldots; \; m = 0, 1, 2, 3, \ldots, \tag{43}$$

где $q_i = q_i^-$ или q_i^+ в зависимости от выбора уравнения; ε_{q_i} – коэффициент, отражающий разность между n и последним членом арифметических прогрессий, описываемых первыми двумя уравнениями (42).

По определению:

$$0 < \varepsilon_{q_i} < 1. \tag{44}$$

Уравнение (43) имеет единственный положительный корень:

$$q_i = -3\left(m + \varepsilon_{q_i}\right) + \sqrt{9\left(m + \varepsilon_{q_i}\right)^2 + n}, \tag{45}$$

или

$$q_i = \sqrt{n} \cdot \sqrt{1 + \frac{9\left(m + \varepsilon_{q_i}\right)^2}{n}} - 3\left(m + \varepsilon_{q_i}\right). \tag{46}$$

При $n >> 1$

$$q_i \approx \sqrt{n} \cdot \left\{1 + \frac{1}{2} \cdot \frac{9\left(m + \varepsilon_{q_i}\right)^2}{n}\right\} - 3\left(m + \varepsilon_{q_i}\right). \tag{47}$$

Для $q_{i_{\max}}$ образуется только одно плюс составное число, равное:

$$C_{i_{\max}}^+ = q_{i_{\max}}^2. \tag{48}$$

Оно находится из уравнения (47) при $m = 0$:

$$q_{i_{\max}} = \sqrt{n} \cdot \left\{1 + \frac{1}{2} \cdot \frac{9\varepsilon_{q_i}{}^2}{n}\right\} - 3\varepsilon_{q_i}. \tag{49}$$

При больших n

$$q_{i_{\max}} \approx \sqrt{n} - 3\varepsilon_{q_i}. \tag{50}$$

Из (50) и (44) следует:

$$\sqrt{n} - 3 \le q_{i_{\max}} \le \sqrt{n}. \tag{51}$$

Учитывая

$$q_{i_{\max}} = 6i_{\max} \pm 1, \tag{52}$$

отсюда

$$i_{\max} = \frac{q_{i_{\max}} \mp 1}{6}. \tag{53}$$

Применительно к рассмотренному примеру $n = 1000$:

$$28,6 \le q_{i_{\max}} \le 31,6,$$

т.е.

$$q_{i_{\max}} = 31; \; i_{\max} = 5,$$

что соответствует правой части таблицы 7 для ПСЧ.

Для левой части, оценивая $q_{i_{\max}}^-$, можно использовать и третье, и четвертое уравнения (42).

Из третьего уравнения (42) следует

$$q_i^-\left(q_i^- + 2\right) + 6q_i^- \cdot m + 6q_i^- \cdot \varepsilon_{q_i^-} - n = 0; \quad i = 1, 2, 3, \ldots; \; m = 0, 1, 2, 3, \ldots. \tag{54}$$

Отсюда

$$q_i^- = -\left(1 + 3m + 3\varepsilon_{q_i^-}\right) + \sqrt{\left(1 + 3m + 3\varepsilon_{q_i^-}\right)^2 + n}. \tag{55}$$

По аналогии с предыдущим рассмотрением, применительно к МСЧ

$$q_{i_{\max}}^- = -\left(1 + 3\varepsilon_{q_i^-}\right) + \sqrt{n}\sqrt{1 + \frac{\left(1 + 3\varepsilon_{q_i^-}\right)^2}{n}}, \tag{56}$$

также при $n >> 1$:

$$q_{i_{\max}}^- \approx \sqrt{n} - 1 - 3\varepsilon_{q_i^-}. \tag{57}$$

Отсюда, используя (44),

$$\sqrt{n} - 4 \le q_{i_{\max}}^- \le \sqrt{n} - 1. \tag{58}$$

Учитывая

$$q_{i_{\max}}^- = 6i_{\max} - 1,$$

имеем:

$$\frac{\sqrt{n} - 3}{6} \le i_{\max} \le \frac{\sqrt{n}}{6}. \tag{59}$$

Таблица 7

Пример работы алгоритма нахождения простых чисел до 1000

Минус составные числа до 1000										q_i^-	Индекс, i	q_i^+	Плюс составные числа до 1000									
$C^-_{31\bullet29}$	$C^-_{29\bullet31}$	$C^-_{25\bullet23}$	$C^-_{23\bullet25}$	$C^-_{19\bullet17}$	$C^-_{17\bullet19}$	$C^-_{13\bullet11}$	$C^-_{11\bullet13}$	$C^-_{7\bullet5}$	$C^-_{5\bullet7}$				$C^+_{5\bullet5}$	$C^+_{7\bullet7}$	$C^+_{11\bullet11}$	$C^+_{13\bullet13}$	$C^+_{17\bullet17}$	$C^+_{19\bullet19}$	$C^+_{23\bullet23}$	$C^+_{25\bullet25}$	$C^+_{29\bullet29}$	$C^+_{31\bullet31}$
899	899	575	575	323	323	143	143	35	35	**5**	*1*	**7**	25	49	121	169	289	361	529	625	841	961
		725	713	437	425	221	209	77	65	**11**	*2*	**13**	55	91	187	247	391	475	667	775		
		875	851	551	527	299	275	119	95	**17**	*3*	**19**	85	133	253	325	493	589	805	925		
			989	665	629	377	341	161	125	**23**	*4*	25	115	175	319	403	595	703	943			
				779	731	455	407	203	155	**29**	*5*	**31**	145	217	385	481	697	817				
				893	833	533	473	245	185	35	*6*	**37**	175	259	451	559	799	931				
					935	611	539	287	215	**41**	*7*	**43**	205	301	517	637	901					
						689	605	329	245	**47**	*8*	49	235	343	583	715						
						767	671	371	275	**53**	*9*	55	265	385	649	793						
						845	737	413	305	**59**	*10*	**61**	295	427	715	871						
						923	803	455	335	65	*11*	**67**	325	469	781	949						
							869	497	365	**71**	*12*	**73**	355	511	847							
							935	539	395	77	*13*	**79**	385	553	913							
								581	425	**83**	*14*	85	415	595								
								623	455	**89**	*15*	91	445	637								
								665	485	95	*16*	**97**	475	679								
								707	515	**101**	*17*	**103**	505	721								
								749	545	**107**	*18*	**109**	535	763								
								791	575	**113**	*19*	115	565	805								
								833	605	119	*20*	121	595	847								
								875	635	125	*21*	**127**	625	889								
								917	665	**131**	*22*	133	655	931								
								959	695	**137**	*23*	**139**	685	973								
									725	143	*24*	145	715									
									755	**149**	*25*	**151**	745									
									785	155	*26*	**157**	775									
									815	161	*27*	**163**	805									
									845	**167**	*28*	169	835									
									875	**173**	*29*	175	865									
									905	**179**	*30*	**181**	895									
									935	185	*31*	187	925									
									965	**191**	*32*	**193**	955									
									995	**197**	*33*	**199**	985									
										203	*34*	205										
										209	*35*	**211**										
										215	*36*	217										
										221	*37*	**223**										
										227	*38*	**229**										
										233	*39*	235										
										239	*40*	**241**										
										…	…	…										
										971	*162*	973										
										977	*163*	979										
										983	*164*	985										
										989	*165*	**991**										
										995	*166*	**997**										

Для нашего примера $n = 1000$:

$$31,6 - 4 \le q^{-}_{i_{\max}} \le 31,6 - 1,$$

т.е.

$$q^{-}_{i_{\max}} = 29, \text{ а } q^{+}_{i_{\max}} = 31, \; i_{\max} = 5.$$

И это соответствует левой части таблицы 7 для МСЧ.

Обобщая полученные результаты зависимости $q_{i_{\max}}$ от n, имеем следующую простую оценку – максимальное число q_i^{+} вида $\{6k+1\}$, $k = 1, 2, 3, \ldots$, участвующее в алгоритме формирования составных чисел (МСЧ и ПСЧ), равно целой части $\sqrt{n}$:

$$q^{+}_{i_{\max}} = \left[\sqrt{n}\right]^{1}. \qquad (60)$$

Соответственно,

$$q^{-}_{i_{\max}} = \left[\sqrt{n}\right] - 2. \qquad (61)$$

При этом индекс $i_{\max}$ равен

$$i_{\max} = \left[\sqrt{n}/6\right]. \qquad (62)$$

В заключение отметим, что доказательство теоремы о полном множестве простых чисел вида $\{6k \pm 1\}$, $k = 1, 2, 3, \ldots$ и формальное описание механизма формирования составных чисел в виде аддитивных прогрессий [4, 8] дало возможность предложить и реализовать простой и эффективный алгоритм нахождения всех простых чисел подряд, что выступает фундаментальным достижением в области математики. Представляется, что дальнейшее использование нового математического аппарата, описывающего формирование простых и составных чисел вида $\{6k \pm 1\}$, $k = 1, 2, 3, \ldots$, приведет в ближайшей перспективе к серьезным изменениям и открытиям в теории чисел и прикладных областях, связанных с применением простых чисел.

[1] В уравнениях (60) – (62) обозначение – это обозначение целой части числа, введенное Гауссом, в других местах статьи – обычные квадратные скобки.

Литература

1. Виноградов, И.М. Основы теории чисел. – М. : Наука, 1972.

2. Начала Евклида / перевод с греческого и комментарии Д.Д. Мордухай-Болтовского при редакционном участии И.Н. Веселовского и М.Я. Выгодского. – М.-Л. : ГТТИ, 1949–51.

3. Хренов, В.П. Свидетельство № 2005613012 от 22 сентября 2005 г. о регистрации программы «Линейный генератор простых чисел подряд».

4. Минаев, В.А., Хренов, В.П. Фундаментальная закономерность формирования простых чисел и информационная безопасность // Безопасность информационных технологий. – 2008. – № 3. – С. 20–32.

5. Каленикова, Н.А., Минаев, В.А, Хренов, В.П. Улучшение метода Ферма : новый алгоритм факторизации // Безопасность информационных технологий . – 2010. – № 2. – С. 76–79.

6. Дирихле (Лежен), П.Г. Лекции по теории чисел. – М.-Л. : ОНТИ, 1936.

7. Галочкин, А.И., Нестеренко, Ю.В., Шидловский, А.Б. Введение в теорию чисел. – М. : МГУ, 1984.

8. Minaev, V.A., Khrenov, V.P., Zernov, V.A. Discovery of Natural Number Laws and Some Applied Aspects of Discovery. Recent Advanced in Management and Information Security / 1st International Conference on Management of Technologies & Information Security, 21st – 24th January, 2010. – New Delhi, Shree Publishers & Distributors, 2010.

9. Minaev, V.A. Interval estimations of the prime numbers amount / The 8th Congress of the International Society for Analysis, its Applications, and Computation, 22-27 August 2011 / Peoples Friendship University of Russia, Moscow.

10. Минаев, В.А. Интервальная оценка количества простых чисел / Тезисы докладов Международной конференции «Образование, наука и экономика в вузах. Интеграция в международное образовательное пространство». 26–30 сентября, 2011, Ереван.