The formula for finding primes
Scherban V.
Формула нахождения простых чисел
Щербань В. Л.

Щербань Виктор Леонидович / Scherban Viktor – дипломированный специалист,
кафедра информатики, факультет математики и информационных технологий,
Курганский государственный университет,
ведущий аудитор,
Компания «ВИЗАВИ Консалт», г. Курган

Аннотация: *огромные простые числа лежат в основе защиты электронной коммерции и электронной почты как шифр: произведение двух простых чисел. Время от времени их надо менять. Как найти их сразу и сейчас?*
Abstract: *huge prime numbers are the basis of secure e-Commerce and e-mail code: the product of two primes. From time to time they need to change. How to find them right now?*

Ключевые слова: *высшая арифметика, простые числа, числа Фибоначчи.*
Keywords: *the higher arithmetic, prime numbers, Fibonacci numbers.*

Нахождение очень больших простых чисел до сих пор считается трудоемкой работой. Существующие алгоритмы уже используют разложение на простые множители чисел, которые превышают 10^{110}. Это целые сутки непрерывной работы самого мощного в мире ЭВМ. Теперь мы убедимся в обратном – никаких алгоритмов простоты произвольного числа не требуется. Непродолжительная работа среднемощного компьютера и результат готов! Огромные простые числа лежат в основе защиты электронной коммерции и электронной почты. Дело в том, что для шифра удобно использовать произведение двух простых чисел. И чтобы найти ключ к шифру, надо определить эти сомножители. Поскольку некоторым злоумышленникам со временем все же удается их вычислить, то знающие шифровальщики постоянно обновляют арсенал огромных простых чисел – это практика, а простая любознательность и научный престиж будет стимулировать охотников за большими простыми числами, так это теория.

Для этого предоставим уникальное решение главной задачи всей арифметики, которое было приведено в авторской работе, но без **полного** и **исчерпывающего** доказательства [3, 4]. Рассмотрим самый известный ряд чисел Фибоначчи, у которого каждое порядковое число равно сумме двух предыдущих чисел, а первые два числа равны *нулю* и *единице*. Первые двадцать одно число этой возвратной последовательности, следующие:

V_q *=0,1,1,2,3,5,8,13,21,34,55,89,144,233,377,610,987,1597,2584,4181,6765…*

Числовое сравнение:

$$V_q + V_{q+2} \equiv 1(\mathrm{mod}\ q), \qquad (1)$$

разрешимо только тогда, когда порядковое число (q) - простое!!

Примеры: семнадцатое число этого ряда равно *987*, значит $V_{17} + V_{19} - 1 = 987 + 2584 - 1 \equiv 0(\mathrm{mod}\ 17)$,

далее: $V_{18} + V_{20} - 1 = 1597 + 4181 - 1 \not\equiv 0(\mathrm{mod} 18)$,

девятнадцатое число равно *2584*, значит $V_{19} + V_{21} - 1 = 2584 + 6765 - 1 \equiv 0(\mathrm{mod}\ 19)$;

Ещё раз подтвердим выше найденное числовое свойство ряда Фибоначчи, у которого первое число не натуральное и равно *нулю* (очень важное уточнение, что нуль не является натуральным числом).

Для проверки выберем простое число *53*.

Пятьдесят третье число Фибоначчи равно: *32 951 280 099*.

Пятьдесят пятое число Фибоначчи равно: *86 267 571 272*.

(*32951280099 + 86267571272) – 1 = 53(2249412290*).

Множество числовых рядов с нахождением простых чисел бессчетно, так как они взяты (включая числа Фибоначчи) из арифметического треугольника Паскаля, который бесконечен. Автору данной публикации известно происхождение всех подобных *возвратных* числовых рядов. Воспользовавшись только тремя (!) – следующими числовыми свойствами, наконец, удалось последнюю по счету арифметическую задачу ушедшего тысячелетия успешно решить.

Над натуральными числами существуют только *три* равновеликих по сути *безграничных* и *беспредельных* арифметических действий, которые можно отобразить в виде бесконечных (бессчетных) арифметических таблиц.

1. Числовые таблицы операций сложений: их сумма есть действие сложение.

2. Числовые таблицы операций умножений или таблицы для быстрого счета: их сумма есть действие умножение. Они же служат для направленного нахождения всех составных чисел. Эти таблицы нам известны с первого класса начальной школы. 3. Числовые таблицы операций сравнений (общепринятое понятие – по числовому модулю) или таблицы для сверхбыстрого и мгновенного счета: их сумма есть действие сравнение. Они же служат для направленного нахождения всех простых чисел.

Сверхбыстрый простой пример: число сто сравнимо с числом три или нет? Сложный, но тоже быстрый по результату пример: сравнимость простых чисел в числовых последовательностях (1). Первая из множества таких таблиц рассмотрена – далее (2).

В арифметике как науке, математическое действие деление натуральных чисел на числа отсутствует, потому что фактически оно не определено. Так как в числовых таблицах отсутствует операция деления, тогда сравнимость чисел *(a)* и *(b)* по модулю *(q)*, означает только возможность представить *(a)* в виде *(a = b + qt)*, где число *(t)*-целое.

Уникальные по значимости и объёму таблицы по числовому модулю найдены из треугольника Паскаля, построенного в *трёхмерном* пространстве, где значение чисел можно заменить натуральными предметами. Все выше названные числовые таблицы, имеются у автора данной публикации.

Треугольник Паскаля предсказывает существование абсолютного Закона – «возмущения», по которому составляются так называемые – *первородные* ряды чисел:

0 1 1
0 0 1 1 1
0 0 0 1 1 1 1

Рассмотрим общий принцип составления арифметических таблиц и как ими пользоваться. Начнем с самой известной возвратной последовательности чисел – ряда Фибоначчи. Каждое число Фибоначчи (V_q) равно сумме двух предыдущих чисел: *0,1,1,2,3,5,8,13,21,34,55,89,…* ($V_q = V_{q-1} + V_{q-2}$).

Следующий второй (W_q) возвратный числовой ряд имеет возвратное уравнение с прибавлением единицы: *0,1,2,4,7,12,20,33,54,88,…* ($W_q = W_{q-1} + W_{q-2} + 1$). Теперь составим общую числовую таблицу Третьего Порядка для нахождения всех простых чисел (2).

Таблица 1. Нахождение простых чисел

	V_q	W_q	q		V_q	W_q	q		V_q	W_q	q
1	0	0	**1**	1	55	143	**11**	1	6765	17710	**21**
1	1	1	**2**	1	89	232	**12**	1	10946	28656	**22**
1	1	2	**3**	1	144	376	**13**	1	17711	46367	**23**
1	2	4	**4**	1	233	609	**14**	1	28657	75024	**24**
1	3	7	**5**	1	377	986	**15**	1	46368	121392	**25**
1	5	12	**6**	1	610	1596	**16**	1	75025	196417	**26**
1	8	20	**7**	1	987	2583	**17**	1	121393	317810	**27**
1	13	33	**8**	1	1597	4180	**18**	1	196418	514228	**28**
1	21	54	**9**	1	2584	6764	**19**	1	317811	832039	**29**
1	34	88	**10**	1	4181	10945	**20**	1			

Числовое сравнение: $(1)\ V_q + W_q \equiv 0(\mathrm{mod}\ q)$, разрешимо только тогда, когда *(q)*, есть число простое. Примеры: $(1)\ V_{17} + W_{17} = 987 + 2583 \equiv 0(\mathrm{mod}17)$, $(1)V_{18} + W_{18} = 1597 + 4180 \not\equiv 0(\mathrm{mod}18)$, $(1)\ V_{19} + W_{19} = 2584 + 6764 \equiv 0(\mathrm{mod}19)$ …;

Теперь находим очевидное числовое равенство: $V_q = W_{q-2} + 1$. Тогда: $V_{q+2} + V_q \equiv 1(\mathrm{mod}\ q)$, что соответствует конкретному ряду чисел Фибоначчи.

Числовые таблицы сравнений по реальному модулю являются таблицами Третьего Порядка (суммы существующих арифметических операций таблиц Первого и Второго Порядка). В основе любой отдельно взятой числовой таблицы должен лежать первородный возвратный ряд чисел – любые два соседних числа такой последовательности равны *нулю* и *единице*.

Первородный ряд чисел имеет возвратное уравнение: ($V_q = V_{q-k} + V_{q-S}$). Количество классов определяется числом *(k)*. Каждый класс имеет свою группу подклассов *(s)*. Эти таблицы также имеются у автора данной публикации.

В заключение темы необходимо отметить, что не все числовые свойства возвратных рядов могут быть закодированы в арифметическом пространстве для натуральных чисел, это, например, следующий числовой ряд: (V_n) =*7,7,31,79,151,247,…* ($V_n = 3V_{n-1} - 3V_{n-2} + V_{n-3}$). Данная числовая

последовательность имеет исключительное числовое свойство. Все простые сомножители каждого порядкового члена имеют только вид: $(p-1) \equiv 0(\mathrm{mod}\ 3)$, например, $(V_6 = 247 = 13 \cdot 19)$, $(V_{16} = 2527 = 7 \cdot 19 \cdot 19)$.

Современные арифметические числовые таблицы сложения реально и разумно изъяты из безусловного закона Паскаля – «возмущения», действующего в одноименной арифметической таблице – треугольника, но само понятие сложение так формально и не определено. Теперь будет ясно почему. Действующие числовые таблицы сложения, а далее таблицы для быстрого счета (умножения), лишены беспредельной числовой памяти – первородных возвратных рядов, поэтому для умноженных чисел, это таблицы Второго Порядка, действие (не операция!) сложения НЕ равносильна умножению.

Литература

1. *Воронин С. М*. Простые числа. М.: Знание, 1978.
2. *Маркушевич А. И.* Возвратные последовательности. М.: Наука, 1983.
3. *Щербань В. Л.* Нахождение простых чисел – Online. // Вестник науки и образования, 2016. № 9 (21). С 15-17.
4. *Щербань В. Л.* Нахождение простых чисел – ONLINE. // Теория. Практика. Инновации, 2016. № 9.