

Нахождение простых чисел – Online Щербань В. Л.

Щербань Виктор Леонидович / Scherban Viktor Leonidovich – 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?

Ключевые слова: высшая арифметика, простые числа, числа Фибоначчи.

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 среднеспособного 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 удастся их вычислить, то знающие шифровальщики постоянно обновляют арсенал огромных простых чисел.

Предоставим решение главной задачи всей арифметики. Рассмотрим самый известный ряд чисел Фибоначчи, у которого каждое порядковое число равно сумме двух предыдущих чисел, а первые два числа равны единицам. Первые двадцать чисел этого ряда:
 $V_q = 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 1597, 2584, 4181, 6765, \dots;$

Числовое сравнение: $V_{q+1} + V_{q-1} \equiv 1 \pmod{q}$, [1] разрешимо только тогда, когда порядковое число (q) – простое!!

Примеры: семнадцатое число этого ряда равно 1597, значит
 $\dots V_{18} + V_{16} - 1 = 2584 + 987 - 1 \equiv 0 \pmod{17}$; далее:

$V_{19} + V_{17} - 1 = 4181 + 1597 - 1 \not\equiv 0 \pmod{18}$; девятнадцатое число равно 4181, значит:

$V_{20} + V_{18} - 1 = 6765 + 2584 - 1 \equiv 0 \pmod{19}$...

Ещё раз подтвердим выше найденное числовое свойство ряда Фибоначчи, у которого первое число натуральное и равно единице (ноль не является натуральным числом). Для проверки выберем простое число 53.

Пятьдесят второе число Фибоначчи равно: 32 951 280 099.

Пятьдесят четвертое число Фибоначчи равно: 86 267 571 272.

$(32951280099 + 86267571272) - 1 = 53(2249412290)$.

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

Над натуральными числами существуют только три равновеликих порядка *безграничных* и *беспредельных* арифметических действий, которые можно отобразить в виде бесконечных числовых таблиц.

Числовые таблицы операций сложений: их сумма есть действие сложение.

Числовые таблицы операций умножений или таблицы для быстрого счёта: их сумма есть действие умножение. Эти таблицы нам известны с первого класса начальной школы.

Числовые таблицы операций сравнений (общепринятое понятие – по числовому модулю) или таблицы для сверхбыстрого и мгновенного счёта: их сумма есть действие сравнение.

Простой пример: число сто сравним с числом три или нет? Сложный пример: сравнимость простых чисел в числовых последовательностях [1].

В арифметике, как науке, математическое действие деление натуральных чисел на число 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 [1].

Уникальные таблицы по числовому модулю найдены из треугольника Паскаля, построенного в *трёхмерном* пространстве, где значение чисел можно заменить натуральными предметами.

Все вышеназванные таблицы имеются у автора данной публикации.

Литература

1. Электронный ресурс: URL: (<http://fib45.ru>).