

# Незнакомые алгоритмы поиска простых чисел среди нечётных

О.А. Черепанов

В классической теории чисел есть две теоремы с именем Пьера Ферма – Большая  $x^n + y^n = z^n$  и Малая  $a^{p-1} \equiv 1 \pmod{p}$ . Но если о первой знают все как-то образованные в элементарной математике, то вторая не так популярна. Вот ее формулировка: число, на единицу меньше натурального числа  $a$  в степени  $p-1$ , имеет простое число  $p$  делителем, если  $p$  не делит  $a$  нацело.

Убедимся, что с помощью Малой теоремы можно доказать Большую для всех  $n = p-1$ , где  $p > 3$  [1].

Если существуют целые числа  $x$ ,  $y$  и  $z$ , удовлетворяющие уравнению  $x^{p-1} + y^{p-1} = z^{p-1}$ , то они должны удовлетворять эквивалентному уравнению  $(x^{p-1} - 1) + (y^{p-1} - 1) = z^{p-1} - 2$ , части которого разделим на  $p$ :

$$\frac{x^{p-1} - 1}{p} + \frac{y^{p-1} - 1}{p} = \frac{z^{p-1} - 2}{p}.$$

Тогда по Малой теореме левая часть предполагаемого тождества при всех натуральных  $x$  и  $y$ , таких, что  $(x, p) = (y, p) = 1$ , будет суммой двух целых чисел, то есть числом целым. Правая же часть ни при каком натуральном  $z$  целым числом не является, так как если  $(z, p) = 1$ , то  $z^{p-1} - 2$  делится на  $p$  с остатком  $p-1$ , а если  $(z, p) \neq 1$ , то с остатком  $p-2$ . Это значит, что уравнение  $x^{p-1} + y^{p-1} = z^{p-1}$  с условием  $(x, p) = (y, p) = (z, p) = 1$  не имеет решения в целых числах при простых  $p \geq 5$ .

А теперь вспомним, что Малая теорема Ферма обобщена Эйлером:  $a^{\varphi(m)} \equiv 1 \pmod{m}$ , где  $\varphi(m)$  – арифметическая функция, значение которой равно количеству натуральных чисел, не превосходящих числа  $m$  и взаимно простых с ним. Но тогда аналогичным способом можно доказать, что уравнение  $x^{\varphi(m)} + y^{\varphi(m)} = z^{\varphi(m)}$  при  $\varphi(m) > 2$  и  $m > 4$  также не имеет решений в целых положительных числах. При этом показатели вида  $n = \varphi(m)$  являются четными, как и  $n = p-1$ . А теорема Эйлера является частным случаем других теорем. Но для изучения свойств *подпростых* чисел  $p-1$  надо иметь ряд простых  $p$ . Между тем закон, определяющий местоположение простых чисел среди составных, не найден и вряд ли существует. Напротив, составные числа закономерно привязаны к числовой оси и строго позиционированы по отношению к простым, кажущимся строительными блоками натурального ряда. То есть, беспорядок в распределении простых компенсирован предсказуемой расстановкой составных.

Давно известен способ выделения простых из  $N$ -го количества натуральных, начиная с единицы. Его называют решетом Эратосфена. Когда-то этот грек решил задачу вычеркиванием составных, кратных простым, не превышающим  $\sqrt{N}$ . В итоге остаются все простые, меньшие натурального числа  $N$ . Но ручная проверка на делимость трудна и в век компьютеров архаична и не продуктивна. И тем не менее *Excel-2007* не содержит опции, позволяющей машинным способом находить простые среди множества натуральных. Но неужели известные методы распознавания простых не доведены до алгоритма, по которому могли бы работать ПК? И хотя есть несколько способов инициации простых, попробуем по-новому решить задачу их поиска с использованием таблицы *Excel*.

Основой найденного способа является цикличность остатков от деления нечетных чисел столбца на нечетное число в строке так, что делимое равно или больше делителя  $\bar{N}$  с номером  $\mathbb{N} \bar{N}$  [2]. Поэтому на черной полурамке белым цветом выделены номера нечетных чисел, начиная с единицы, последовательно размещенных слева направо в строке ниже черной и сверху вниз в столбце справа от черного. При этом в столбцах, озаглавленных нулем, заметна повторяемость остатков (2-1-0, 2-4-1-3-0, 2-4-6-1-3-5-0, 2-4-6-8-1-3-5-7-0 и т.д.), образующих циклы, где количество чисел (сначала четных, а затем нечетных) равно нечетному числу-делителю  $\bar{N}$ . Ясно, что циклы можно размножить вниз до нечетного числа  $\underline{N}$  с номером  $\mathbb{N} \underline{N}$ , если надо найти все предшествующие ему простые числа. И в этом случае простым будет нечетное число, номер которого озаглавливает строку, где нет ни одного выделенного нуля 0, завершающего каждый цикл независимо от его длины  $L_{\bar{N}} = \bar{N}$ , равной нечетному числу вверху под его номером  $\mathbb{N} \bar{N}$ .







В результате ликвидации строк с маркерами 0 от числового ряда с 1 по 97 остаются все простые числа в количестве 25. Ясно, что способ удаления нечетных составных чисел по нулевому остатку ограничен размерами таблицы *Excel* и может быть реализован в программе для ЭВМ, исключаяющей ручные действия.

№	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	...
1	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	...
2	3	0																
3	5	2	0															
4	7	1	2	0														
5	11	2	1	4	2	0												
6	13	1	3	6	4	2	0											
7	17	2	2	3	8	6	4	2	0									
8	19	1	4	5	1	8	6	4	2	0								
9	23	2	3	2	5	1	10	8	6	4	2	0						
10	29	2	4	1	2	7	3	14	12	10	8	6	4	2	0			
11	31	1	1	3	4	9	5	1	14	12	10	8	6	4	2	0		
12	37	1	2	2	1	4	11	7	3	18	16	14	12	10	8	6	4	...
13	41	2	1	6	5	8	2	11	7	3	20	18	16	14	12	10	8	...
14	43	1	3	1	7	10	4	13	9	5	1	20	18	16	14	12	10	...
15	47	2	2	5	2	3	8	2	13	9	5	1	22	20	18	16	14	...
16	53	2	3	4	8	9	1	8	2	15	11	7	3	26	24	22	20	...
17	59	2	4	3	5	4	7	14	8	2	17	13	9	5	1	28	26	...
18	61	1	1	5	7	6	9	1	10	4	19	15	11	7	3	30	28	...
19	67	1	2	4	4	1	2	7	16	10	4	21	17	13	9	5	1	...
20	71	2	1	1	8	5	6	11	3	14	8	2	21	17	13	9	5	...
21	73	1	3	3	1	7	8	13	5	16	10	4	23	19	15	11	7	...
22	79	1	4	2	7	2	1	4	11	3	8	10	4	25	21	17	13	...
23	83	2	3	6	2	6	5	8	15	7	20	14	8	2	25	21	17	...
24	89	2	4	5	8	1	11	14	4	13	5	20	14	8	2	27	23	...
25	97	1	2	6	7	9	6	7	12	2	13	5	22	16	10	4	31	...
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...

Алгоритм инициации простых чисел по отсутствию нулевых остатков позволяет вычислять номера (№) подлежащих удалению строк выше назначенного нечетного числа  $\bar{N}$ , а не только выделять строки визуально.

Заметим, что начала лучей, соединяющих маркеры 0, принадлежат номерам с шагом 3 по вертикали, начиная с №5, а каждый луч перечеркивает маркеры, связанные с длиной  $L_{\bar{N}} = \bar{N}$  цикла от 2 до 0 из четных и нечетных остатков от деления чисел  $N = 2n - 1$  ( $n = 1, 2, 3, \dots$ ) на  $\bar{N} \leq N$ . При этом можно найти количество циклов той или иной длины в интервале номеров от 5-го, 8-го, 11-го, 14-го и т.д. до конечного номера 49, присвоенного числу 97. Для этого надо выделить целые части чисел, получаемых делением разности  $\text{№}N - \text{№}\bar{N}$  на  $L = 3, 5, 7, 9$  и т.д., где  $\text{№}\bar{N} = 5, 8, 11, 14$  и т.д. Ясно, что количество  $n$  этих чисел ограничено моментом, когда результат деления оказывается меньше единицы. В предложенном примере таких чисел девять. Запишем их в порядке вычисления: 15, 8, 5, 4, 3, 2, 1, 1 и 1. Это значит, что цикл длиной 3 (2-1-0) укладывается 15 раз между номерами № = 5 и № = 49, а цикл длиной 5 (2-4-1-3-0) уместится 8 раз в интервале от № = 8 до № = 49 и т.д. В итоге все нули-маркеры по одному, по два и больше оказываются привязанными к номерам, за которыми стоят нечетные составные числа. Это строки 5, 8, 11, 13, 14, 17, 18, 20, 23, 25, 26, 28, 29, 32, 33, 35, 38, 39, 41, 43, 44, 46, 47 и 48, ранее определенные визуально. Выделяя их заливкой и фильтруя по цвету, сократим «трапецию» остатков до 25 строк с простыми числами меньше 97 в столбце № = 1.

Пример с выделением составных чисел из ряда нечетных представим в виде алгоритма, отличающегося от известных методов, называемых решетом Эратосфена, решетом Сундарама и решетом Аткина.

1. Нечетным числам  $N = 2n - 1$  ( $n = 1, 2, 3, \dots$ ), меньшим назначенного числа  $\underline{N}$ , присвоим номера  $\mathcal{N}_n = 1, 2, 3, \dots$  по порядку их следования, начиная с единицы. При этом  $N = 2\mathcal{N}_n - 1$ .

2. Зная длину  $L_{\bar{N}} = \bar{N}$  цикла из четных и нечетных остатков от деления нечетных чисел  $N > \bar{N}$  на  $\bar{N} = 2\mathcal{N}_{\bar{N}} - 1$  найдем количество циклов в интервале от номера  $\mathcal{N}_{\bar{N}} = \frac{\bar{N} + 1}{2}$  делителя  $\bar{N}$  до числа  $\underline{N}$  как целую часть  $\underline{m}$  дробного числа  $m = \frac{N - [5 + 3(n-1)]}{2n-1}$ , где  $m(n)$  ограничено значением  $n = 1, 2, 3, \dots$ , для которого  $m$  не меньше единицы.

3. Имея число  $\underline{m}(\bar{N})$ , выражающее количество циклов от делителя  $\bar{N}$ , предшествующее назначенному числу  $\underline{N}$ , по формуле  $\mathcal{N}_{\bar{N}} + M(\bar{N}) \times L_{\bar{N}} = \mathcal{N}_{(N^*)}$ , где множитель  $M(\bar{N})$  принимает значения от 1 до  $\underline{m}(\bar{N})$ , получим номера  $\mathcal{N}_{(N^*)}$  всех чисел  $N^* = 2\mathcal{N}_{(N^*)} - 1$  интервала  $[\bar{N}, \underline{N}]$ , делящихся на  $\bar{N}$  нацело.

4. Номера нечетных чисел, имеющих два и более делителей  $\bar{N} < \underline{N}$ , дублируются и также подлежат изъятию, после которого в интервале от 1 до  $\underline{N}$  иницируются номера простых чисел, а значит и сами простые  $P = 2\mathcal{N}_P - 1$ .

Подчеркнем, что сепарация простых чисел  $P$  из множества нечетных  $N$ , меньших назначенного числа  $\underline{N}$ , основана на выделении составных чисел, расположение которых на числовой оси закономернее распределения простых. И, как видно, предлагаемое решето не сводится к тестированию назначенного числа  $n$  на делимость простыми  $p < \sqrt{n}$  и поэтому имеет смысл его оформление и опробывание в виде программы для ЭВМ.

Выборка простых чисел от единицы до нечетного числа  $\underline{N}$  позволяет создать массив *подпростых* чисел  $p - 1$  с целью исследования общих свойств его элементов в связи с поиском элементарного доказательства Большой теоремы П. Ферма, начатого использованием его Малой теоремы. Но особенно важно то, что найденный алгоритм исключает число 2 из множества простых. Более того, это число играет основную роль в бинарной арифметике, единицы которой определены дихотомией, то есть делением двойки пополам [3].

## Литература

- Черепанов О.А. Задачи наших читателей. // Квант. – 1986. – №6. – С. 19. – №10. – С. 64
- Черепанов О.А. Где начало того конца?... От философии науки до основания физики. Геометрия и Арифмометрия. Изд. «М.: Нефтегазовое дело», 2013. - 280 с. - 52. (ISBN 5-88541-010-0; ISBN 978-5-98755-165-6) (<http://www.trinitas.ru/rus/doc/0009/001a/1092-chr.pdf>)
- Черепанов О.А. Секстетные структуры над числами Фидия-Фибоначчи-Люка и остепененные единицы в тригонометрии. (<http://www.trinitas.ru/rus/doc/0016/001d/2214-chr.pdf>)