Китайская теорема об остатках и гипотеза Ченцова

Д.ФЛЕЙШМАН

Постановка задачи

Настольной книгой любителей математики является замечательная книга [1]. В ней собраны различные нестандартные задачи по всем разделам школьной программы, в том числе и задачи на делимость чисел.

Полное решение одной из таких задач не было известно авторам. Один из них — молодой талантливый математик, впоследствии член-корреспондент АН СССР Н.Н.Ченцов (1930—1992) — высказал гипотезу о том, что *для любого натурального числа* $k \geq 17$ *можно найти* k *последовательных натуральных чисел, среди которых нет ни одного, взаимно простого со всеми остальными.*

Предварительные замечания

Нетрудно видеть, что любые два последовательных натуральных числа всегда взаимно просты. Из трех последовательных натуральных чисел l, $l+1$ и $l+2$ число $l+1$ всегда взаимно просто с остальными. Из четырех последовательных натуральных чисел l, $l+1$, $l+2$ и $l+3$ в зависимости от четности l либо $l+1$, либо $l+2$ взаимно просто с остальными.

Оказывается, что при любом $5 \leq k \leq 16$ среди k оследовательных натуральных чисел найдется число, взаимно простое с остальными.

Упражнения

1. Докажите это.
2. Докажите, что произведение двух последовательных целых чисел не является n-й степенью никакого целого числа при $n \geq 2$.
3. Докажите утверждение упражнения 2 для произведения а) трех; б) четырех последовательных натуральных чисел.

Однако существуют 17 последовательных натуральных чисел, каждое из которых имеет общий делитель с каким-нибудь из этих 17 чисел.

Случай $k = 17$

Заметим, что если какие-то два из k последовательных натуральных чисел имеют общий делитель, то существует простое число, меньшее чем k, которое является делителем этих чисел.

Будем говорить, что набор из k *последовательных натуральных чисел обладает свойством* (*), *если среди них нет ни одного числа, взаимно простого со всеми остальными.* Мы будем называть такие набор *-*наборами длины* k.

Рассмотрим набор из k последовательных натуральных чисел. Пронумеруем их натуральными числами от 1 до k. Делимость чисел из набора на простые числа от 2 до p_0, где p_0 — наибольшее простое число, не превышающее $k-1$, удобно показывать на рисунке, где слева от черты находится *простое число*, а справа — *номера тех чисел из набора, которые делятся на это простое число.*

Поясним это на примере. Возьмем семь последовательных целых чисел: 100, 101, ..., 106. Простые числа, меньшие 7, т.е. 2, 3, 5, запишем столбиком, затем проведем вертикальную прямую, правее которой напротив каждого из простых чисел выпишем номера чисел из набора, делящихся на это простое число (рис.1).

2	1, 3, 5, 7
3	3, 6
5	1, 6

Рис. 1

Справа от черты ни разу не встречаются числа 2 и 4. Это означает, что числа с этими номерами взаимно просты с остальными.

На рисунке 2 показана делимость чисел от 25 до 44 на простые числа от 2 до 19.

На рисунках 1 и 2 справа от черты находятся арифметические прогрессии, составленные из разного (от 1 до 10) числа членов.

Нетрудно видеть, что эта закономерность носит общий характер. Именно, *набор из* k *последовательных натуральных чисел будет *-набором тогда и только тогда, когда на соответствующем этому набору рисунке каждое из чисел от 1 до* k *встречается справа от черты в одной строчке по*

2	2, 4, 6, 8, 10, 12, 14, 16, 18, 20
3	3, 6, 9, 12, 15, 18
5	1, 6, 11, 16
7	4, 11, 18
11	9, 20
13	2, 15
17	10
19	14

Рис. 2

крайней мере с еще одним числом. На рисунке 2 числа 10 и 14 стоят в последних строчках в гордом одиночестве, а некоторые числа отсутствуют вовсе.

Согласно этому критерию наборы чисел, изображенные на рисунках 1 и 2, не обладают свойством (*). На рисунке 3 изображено, каким мог бы быть

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

Рис. 3

*-набор из 17 последовательных натуральных чисел.

Существование такого набора мы вскоре докажем.

Китайская теорема об остатках

Напомним, что «китайская теорема об остатках» — это известное с глубокой древности утверждение о том, что *если натуральные числа* $a_1, \ldots, a_n$ *попарно взаимно просты, то, каковы бы ни были целые числа* $b_1, \ldots, b_n$ $(0 \leq b_i \leq a_{i-1},\ i = 1, 2, \ldots, n)$, *существует натуральное число, дающее при делении на* a_1 *остаток* b_1, *при делении на* a_2 *остаток* b_2, ..., a_n — *остаток* b_n. *Таких чисел бесконечно много и все они являются членами некоторой арифметической прогрессии* (см. [3]).

Задача. *Постройте набор из 17 последовательных натуральных чисел, обладающий свойством (*), на основе рисунка 3.*

Решение. Пусть a — первое из чисел $*$-набора длины 17. Из рисунка 3 видно, что a должно делиться на 2, 3, 7 и 13, давать при делении на 5 остаток 4, а при делении на 11 — остаток 6. Такое число существует по китайской теореме об остатках, так что задачу о существовании $*$-набора длины 17 можно считать решенной.

Упражнение 4. Найдите наименьшее a, удовлетворяющее условию задачи.

Наборов, обладающих свойством ($*$) и имеющих одинаковое графическое изображение, эквивалентное рисунку 3, бесконечное множество. Наименьшие числа этих наборов принадлежат арифметической прогрессии с начальным членом 2184 и разностью

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030.$$

Рисунок 3 не является единственным графическим изображением $*$-наборов

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

Рис. 4

длины 17. Другая возможность показана на рисунке 4.

Упражнение 5. Постройте наименьший возможный $*$-набор, графическим изображением которого служит рисунок 4.

Хотя рисунки 3 и 4 отличаются друг от друга, методы их построения похожи. На рисунке 3 число 7 встречается в прогрессиях, помещенных справа от 2, 3, 5; число $6 = 7 - 1$ встречается в арифметической прогрессии, расположенной справа от 11; число $8 = 7 + 1$ находится в арифметической прогрессии, расположенной справа от 7. Определим, какие числа от 1 до 17 не встречаются в прогрессиях, расположенных справа от 2, 3, 5, 7, 11. Среди чисел от 1 до 7 таких нет, потому что если таким числом является x, то $7 - x$ не делится ни на 2, ни на 3, ни на 5. А поскольку между 5 и 7 нет простых, $x = 6$. Но 6 встречается в арифметической прогрессии, расположенной справа от 11.

Среди чисел от 8 до 17 только $14 = 7 + 7$ не принадлежит прогрессиям, расположенным справа от 13.

Приведенные объяснения позволяют понять, как возник рисунок 3. Аналогично строится набор чисел, графическое изображение которого приведено на рисунке 4.

Обобщение конструкции

Рассмотренный способ построения $*$-наборов длины 17 можно обобщить. На рисунках 5 и 6 показаны два возможных варианта построения $*$-набора длины k при $k = p_i + p_{i+1} - 1$, где p_i, p_{i+1} — соответственно i-е и $(i+1)$-е простое число. Напомним, что 2 — первое простое число, 3 — второе, 5 — третье и т.д. (например, $17 = p_1 + p_5 - - 1$). Нетрудно видеть, что при $2p_i >> p_{i+2}$, вне зависимости от значений членов арифметических прогрессий, расположенных справа от p_{i+3}, ..., рисунок 5

2	$\ldots, p_i - 2, p_i, p_i + 2, \ldots$
3	$\ldots, p_i - 3, p_i, p_i + 3, \ldots$
$\vdots$	
p_{i-1}	$\ldots, p_i - p_{i-1}, p_i, p_i + p_{i-1}$
p_i	$1, p_{i+1}, \ldots$
p_{i+1}	$p_{i-1}, p_i + p_{i-1} - 1$
p_{i+2}	$2p_i - p_{i+2}, 2p_i$
$\vdots$	

Рис. 5

является графическим изображением $*$-набора из $k = p_i + p_{i+1} - 1$ последовательных чисел. При $p_{i+2} \le \le 2p_i - 1$ аналогичным свойством обладает и рисунок 6. Таким образом, рисунки 5 и 6 являются графическими изображениями $*$-наборов из k последовательных чисел при $p_{i+2} \le 2p_i - 1$.

Убедимся в этом. На рисунке 5 в первых $i - 1$ строках правее черты и левее p_i находятся все числа $l \le p_i - 2$. В самом деле, поскольку $p_i - l < p_i$, число $p_i - l$ *заведомо делится* на одно

2	$\ldots, p_{i+1} - 2, p_{i+1}, p_{i+1} + 2, \ldots$
3	$\ldots, p_{i+1} - 3, p_{i+1}, p_{i+1} + 3, \ldots$
$\vdots$	
p_{i-1}	$\ldots, p_{i+1} - p_{i-1}, p_{i+1}, p_{i+1} + p_{i-1}, \ldots$
p_i	$\ldots, p_{i+1} - 1, p_{i+1} + p_i - 1, \ldots$
p_{i+1}	$1, p_{i+1} + 1$
p_{i+2}	$p_{i+1} - p_i, p_{i+1} + p_{i+2} - p_i$
$\vdots$	

Рис. 6

из простых чисел, *меньших* p_i, и, следовательно, принадлежит одной из прогрессий, стоящих над i-й строчкой таблицы.

Аналогично, числа l, *большие* $p_i + 1$ и не превосходящие $p_i + p_{i+1} - 2$, кроме, может быть, числа $2p_i$, находятся в первых $i - 1$ строчках правее числа p_i. Строчки с номерами i, $i + 1$ обеспечивают наличие общего простого делителя у чисел с номерами 1 и $p_i + 1$, p_{i-1} и $p_i + + p_{i+1} - 1$, а при $2p_i > p_{i+2}$ у чисел с номерами $2p_i$ и $2p_i - p_{i+2}$.

Таким образом, с помощью рисунка 5 и китайской теоремы об остатках мы можем получить $*$-набор длины $p_i + + p_{i+1} - 1$, если $2p_i > p_{i+2}$.

При $p_{i+2} \le 2p_i - 1$ таким же свойством обладает и рисунок 6 для $k = p_{i+1} + + p_{i+2} - 1$.

Упражнение 6. Убедитесь в этом самостоятельно.

Для каждого k, принадлежащего отрезку $[p_{i+1} + p_i - 1, p_{i+1} + p_{i+2} - 1]$, на основе рисунка 6 возможно построение $*$-набора длины k. Если $k = p_{i+1} + p_i$, рисунок 6 необходимо дополнить строчкой

$$p_{i+3} | p_{i+1} + p_i - p_{i+3}, \; p_{i+1} + p_i,$$

а при $k = p_{i+1} + p_{i+1} = 2p_{i+1}$ добавить также строчку

$$p_{i+1} | \, 2p_{i+1} - p_{i+4}, \; 2p_{i+1}.$$

Нетрудно видеть, что приведенные операции возможны при $p_{i+1} + p_i > p_{i+3}$ и $2p_{i+1} > p_{i+4}$. Очевидно, что оба неравенства справедливы, в частности, если между p_i и $2p_i$ и p_{i+1} и $2p_{i+1}$ находится не менее *трех* простых чисел. Следовательно, в этом случае для каждого числа k, принадлежащего отрезку $[p_{i+1} + p_i - 1, p_{i+1} + p_{i+2} - 1]$, можно построить $*$-набор из k чисел. Аналогично получим, что если между p_{i+2} и $2p_{i+2}$ находится не менее трех простых чисел, то и для любого k, принадлежащего $[p_{i+1} + p_{i+2} - 1, p_{i+2} + p_{i+3} - 1]$, можно построить $*$-набор длины k. Следовательно, *если для каждого простого числа p, начиная с p_i, между p и $2p$ находится не менее трех простых чисел, то для любого $k \ge p_i + p_{i+1} - 1$ можно построить $*$-набор длины k.*

Постулат Бертрана

В 1845 году французский математик Ж.Бертран высказал предположение, что между n и $2n$ при $n \ge 2$ *находится, по крайней мере, одно простое число.* Это предположение получило название *постулата Бертрана.*

Доказал постулат Бертрана выдающийся русский математик П.Л.Чебышёв. Более того, он показал, что число $\pi(N)$ простых чисел, не превосходящих N, имеет порядок $N/\ln N$; эта замечательная теорема стала пер-

(Продолжение см. на с. 52)

Китайская теорема об остатках и гипотеза Ченцова

(Начало см. на с. 39)

вым шагом в решении вопроса о распределении простых чисел. Чебышёв показал, что при больших N число $\pi(N)$ заключается в границах $0{,}92N/\ln N < \pi(N) < 1{,}11N/\ln N$. Он доказал также, что если отношение $\pi(N):N/\ln N$ при $N \to \infty$ стремится к какому-либо пределу, то этот предел равен 1.

Доказательство существования этого предела было получено через 50 лет после работ П.Л.Чебышёва французским математиком Ж.Адамаром и потребовало искусного применения теории функций комплексного переменного. Элементарное (но очень сложное) доказательство было найдено замечательным датским математиком А.Сельбергом в 1948 году.

Несколько усовершенствовав доказательство (вполне элементарное, хотя и не простое) постулата Бертрана, можно доказать справедливость «усиленного» постулата Бертрана: *при любом $n \ge 9$ между n и $2n$ находится не менее трех простых чисел.*

Завершение доказательства гипотезы Ченцова

Поскольку $p_5 = 11$, из усиленного постулата Бертрана следует, что при всех простых $p \ge p_5$ между числами p и $2p$ имеется по крайней мере три простых числа, и потому с помощью конструкций рисунков 5 и 6 и китайской теоремы об остатках можно простроить $*$-набор длины $k \ge p_5 + p_6 - 1 = 23$.

Для завершения доказательства достаточно простроить $*$-наборы длины k при $k = 18, 19, 20, 21, 22$. Эти наборы строятся с помощью рисунка 3 (или рисунка 4) добавлением строк (при $k = 18, 19$ добавляется строка 17| 1, 18, а при $k = 20, 21, 22$ — еще и строка 19 | 1, 20).

Гипотеза Ченцова полностью доказана.

Упражнение 7. Выпишите наименьшие числа $*$-наборов при $k = 18, 19, 20, 21, 22$.

Литература

1. *Д.О.Шклярский, Н.Н.Ченцов, И.М.Яглом.* Избранные задачи и теоремы элементарной математики. Арифметика и алгебра. — М.: Физматлит, 1976.

2. *Э.Трост.* Простые числа. — М.: Физматгиз, 1959.

3. *А.Егоров.* Деление с остатком и сравнения по модулю. — «Квант» №6 за 1991 г. или Приложение к «Кванту» №2 за 1994 г.