

О ПРЕДСТАВИМОСТИ ЧЕТНОГО ЧИСЛА СУММОЙ ДВУХ ПРОСТЫХ ЧИСЕЛ

В. И. ЛЕКОНЦЕВ

(Представлена научным семинаром факультета автоматики и телемеханики)

1. Пусть $\varphi_2(l, N)$ выражает число пар чисел n и $n + l$, одновременно взаимно простых с N , первое из которых не превосходит N . Очевидно, что $\varphi_2(l, 1) = 1$. Легко доказать следующие свойства функции: Функция φ_2 мультипликативна.

При p простом $\varphi_2(l, p^a) = \begin{cases} p^{a-1}(p-2), & \text{если } (l, p) = 1, \\ p^{a-1}(p-1), & \text{если } (l, p) = p. \end{cases}$

Таким образом, $\varphi_2(l, N) = N \prod_{\substack{p|N \\ p \nmid l}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p|N \\ p \times l}} \left(1 - \frac{2}{p}\right)$.

2. Пусть $\varphi_3(l_1, l_2, N)$ выражает число троек чисел $n, n + l_1, n + l_2$, одновременно взаимно простых с N , первое из которых не превосходит N . Функция φ_3 мультипликативна и

$\varphi_3(l_1, l_2, p^a) = \begin{cases} p^{a-1}(p-3), & \text{если } (l_1, p) = 1, (l_2, p) = 1, \\ p^{a-1}(p-2), & \text{если одно из } l \text{ взаимно просто с } p, \\ p^{a-1}(p-1), & \text{если } (l_1, p) = p \text{ и } (l_2, p) = p, \end{cases}$

так что

$\varphi_3(l_1, l_2, N) = N \prod_{\substack{p|N \\ p \nmid l_1 \\ p \nmid l_2}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p|N \\ p \times l_1 \\ p \times l_2}} \left(1 - \frac{2}{p}\right) \prod_{\substack{p|N \\ p \times l_1 \\ p \times l_2}} \left(1 - \frac{3}{p}\right). \quad (p|N)$

3. Для функции $\varphi_m(l_1, \dots, l_{m-1}, N)$, выражающей число m -чисел $n, \dots, n + l_{m+1}$, взаимно простых с N , первое из которых не превосходит N , справедливы аналогичные свойства.

Из п. 1 следует, что число пар чисел n и n' ($n' - n = l$), взаимно простых с $p_1, \dots, p_k$ и непревосходящих $Q = p_1 \cdots p_k$, равно

$$E_2(l, \kappa, Q) = \prod_{p|l} (p-1) \prod_{p \times l} (p-2) \quad (p|Q), \quad (1)$$

откуда следует приближенная формула для числа пар простых чисел в $[1, n]$, полученная также в работах [1], [2],

$$\pi_2(l, n) \approx \frac{n}{Q} \prod_{\substack{p|l \\ p|Q}} (p-1) \prod_{\substack{p \times l \\ p|Q}} (p-2) \sim c \frac{n}{\ln^2 n},$$

где c — некоторая постоянная. Из (1) можно также предположить,

$$\frac{\pi_2(l_1, n)}{\pi_2(l_2, n)} \rightarrow \frac{E_2(l_1, Q)}{E_2(l_2, Q)} \quad (n \rightarrow \infty)$$

Так,

$$\frac{\pi_2(6, n)}{\pi_2(2, n)} \rightarrow 2, \quad \frac{\pi_2(10, n)}{\pi_2(2, n)} \rightarrow \frac{4}{3}, \quad \frac{\pi_2(2^i, n)}{\pi_2(2, n)} \rightarrow 1.$$

Следующая таблица дает представление об этой гипотезе.

$n \backslash \pi$	$\pi_2(2, n)$	$\pi_2(8, n)$	$\pi_2(6, n)$	$\pi_2(10, n)$
1000	35	39	73	52
4000	103	106	197	135
6000	143	137	274	180

Лемма 1. Число пар чисел, взаимно простых с $p_1, \dots, p_k$ и непревосходящих $n + l$, имеет оценку снизу

$$E_2(l, n) \geq \left[\left[\left[n \frac{p_1 - 1}{p_1} \right] \frac{p_2 - 1}{p_2} \right] \dots \frac{p_k - 1}{p_k} \right] \geq \frac{n}{2p_k}.$$

Доказательство. Для доказательства этого неравенства необходимо показать справедливость следующего утверждения: после вычеркивания из общего числа n чисел, кратных p_1 , среди каждых p_2 чисел последовательности, получившейся в результате первого „высевания“, не более одного числа делится на p_2 ; в результате „высевания“ чисел, кратных p_2 , получаем последовательность, в которой на каждые p_3 чисел приходится не более одного числа, делящегося на p_3 и так далее; после $k = 1$ шага получаем последовательность чисел, в которой на каждые p_k , начинающихся с 1, чисел не более одного делится на p_k . Это можно показать, во-первых, тем фактом, что среди $Q = p_1 \dots p_k$ первых чисел количество чисел, взаимно простых с $p_1, \dots, p_k$, равно $(p_1 - 1)(p_2 - 1) \dots (p_k - 1)$ (Эйлер). Это же значение получим при указанном способе подсчета, то есть с помощью постепенного „высевания“ из оставшихся чисел, кратных следующему простому числу. Действительно, после первого шага — „высевания“ чисел, кратных p_1 , получаем число чисел, взаимно простых с p_1 , которое равно $Q_1 = \left[Q \frac{p_1 - 1}{p_1} \right] = (p_1 - 1)p_2 \dots p_k$; далее, из оставшихся чисел взаимно простых с p_2 равно величине

$$Q_2 = (p_1 - 1)(p_2 - 1)p_3 \dots p_k = \left[\left[Q \frac{p_1 - 1}{p_1} \right] \frac{p_2 - 1}{p_2} \right],$$

а это возможно лишь благодаря тому, что из каждых p_2 , оставшихся после первого „высевания“ чисел, не более одного числа делится на p_2 . На i шаге „высевания“ получаем величину

$$Q_i = (p_1 - 1) \dots (p_i - 1)p_{i+1} \dots p_k$$

— число чисел, взаимно простых с $p_1, \dots, p_i$. Из оставшихся чисел количество чисел, взаимно простых с p_{i+1} , равно величине

$$(p_1 - 1) \dots (p_i - 1)(p_{i+1} - 1)p_{i+2} \dots p_k = \left[Q_i \frac{p_{i+1} - 1}{p_{i+1}} \right].$$

Это опять же возможно лишь благодаря тому, что на каждые p_{i+1} оставшихся чисел приходится не более одного числа, делящегося на p_{i+1} . Но вследствие того, что не более одного числа, кратного p_i , приходится на каждые p_i чисел, мы можем применить это свойство при произвольном n , при этом последняя группа чисел, если она окажется неполной, при применении знака $[]$ отпадает, от чего мы только усилим неравенство. Это рассуждение дополним индукцией по k . Составим последовательность, получающуюся после $i-1$ шага „высевания“, состоящую из ν полных групп чисел по p_i в каждой, неполную группу, если она окажется, отбрасываем:

$$\overbrace{1, p_i, p_{i+1}, \dots, \alpha_1, \alpha_2, \dots, p_i^2, \dots, \alpha_3, \alpha_4, \dots, p_i, p_{i+1}, \dots}^{\nu p_i}$$

Предположим, что из каждых p_i чисел этой последовательности одно делится на p_i , из каждых p_{i+1} одно делится на p_{i+1} и т. д. „Высеваем“ числа, кратные p_i , после чего в последовательности остается $\nu p_i - \nu$ чисел. Первоначально среди νp_i чисел, кратных p_{i+1} , было $\left[\frac{\nu p_i}{p_{i+1}} \right]$, но при высевании чисел, кратных p_i , отпали и числа

$$p_i p_{i+1}, \quad p_i p_{i+1}^2, \quad p_i p_{i+1} p_{i+2}, \dots, \leq n,$$

таких чисел не меньше числа членов f геометрической прогрессии с первым членом p_{i+1} и со знаменателем p_k . Тогда на долю $\nu p_i - \nu$ чисел, кратных p_{i+1} , останется не больше

$$\left[\frac{\nu p_i}{p_{i+1}} \right] - f.$$

Теперь уже нетрудно показать, что на каждые p_{i+1} из оставшихся чисел приходится не более одного числа, делящегося на p_{i+1} . Этим наше утверждение о том, что на i -шаге „высевания“ на долю каждых p_i чисел приходится не более одного числа, кратного p_i , доказано.

Лемма получается из этого утверждения при учетывании того, что при $(l, p) = 1$ из p_i чисел „высеваются“ по два числа n' и $n' + r$, где $r \equiv l \pmod{p}$, $r < p$.

Этот метод решета несколько отличается от ранее применяемых, например, в [1], [2] и других тем, что в отличие от „высевания“ чисел, кратных последовательным простым из общего числа n , здесь „высевание“ происходит на каждом шаге из оставшихся чисел. Но при ближайшем рассмотрении получается одна и та же картина: „высевание“ чисел, кратных простым.

Теорема 1. При $n \geq 6$ между n и $2n$ существует по меньшей мере одна пара простых чисел близнецов p', p'' ($p'' - p' = 2$).

Доказательство. Найдется такое k , что $p_k \leq n < p_{k+1}$. Число пар чисел, взаимно простых с $p_1, \dots, p_k$ в $[1, 2n]$ по лемме 1 не меньше $\frac{n}{p_k} \geq 1$. Но среди первых чисел нет искомой пары: ($p_k \leq n < p_{k+1}$). Поэтому пара чисел (быть может большее число), взаимно простых с $p_1, \dots, p_k$, находится между n и $2n$. Но они меньше p_{k+1}^2 , поэтому оба числа из пары будут простыми.

Теорема 2. Четное число представимо разностью двух простых чисел, и число таких представлений бесконечно.

Доказательство. Каково бы ни было четное число l , найдутся такие p_k и n (таких p_k и n при фиксированном l будет бесконечное множество), что будут выполняться неравенства:

$$n + l < p_{k+1}^2, \quad n > 4p_k.$$

Для $n \geq 4p_k$ имеем $E_2(l, k, n) \geq 2$ (больше 1 нам недостаточно, так как такой парой могут оказаться числа 1 и $1+l$), следовательно между p_k и n существует первое число по крайней мере одной пары простых чисел p' и p'' таких, что $p'' - p' = l$.

Лемма 2. Числа, взаимно простые с $p_1, \dots, p_k$, расположены симметрично относительно числа $p_2 \cdots p_k$ в интервале $[1, p_1 \cdots p_k]$, и такая симметрия повторяется в последующих интервалах такой же длины.

Теорема 3. Четное число представимо суммой двух простых чисел, и число таких представлений не меньше

$$\left[\left[N \frac{p_2 - 2}{p_2} \right] \cdots \frac{p_k - 2}{p_k} \right].$$

Доказательство. По лемме 2 число решений уравнения $P_1 + P_2 = 2N$ в простых числах равно числу пар чисел n и $n + p_1 \cdots p_k - 2N$, одновременно взаимно простых с $p_1, \dots, p_k$, где $p_k \leq \sqrt{2N - 1} < p_{k+1}$. Действительно, если n и $n + p_1 \cdots p_k - 2N$ взаимно простые с $p_1, \dots, p_k$, то n и $2N - n$ также взаимно просты с $p_1, \dots, p_k$ и, следовательно, ($n < p_{k+1}^2$, $2N - n < p_{k+1}^2$) будут простыми. По лемме 1 число таких пар чисел оценивается указанным выражением.

Из п. 2 следует, что число троек чисел n , $n + l_1$, $n + l_2$, одновременно взаимно простых с $p_1, \dots, p_k$ и непревосходящих $p_1 \cdots p_k + l$, равно

$$E_3(l_1, l_2, k, Q) = \prod_{\substack{p/l_1 \\ p/l_2}} (p-1) \prod_{\substack{p/l_1 \\ p \times l_2}} (p-2) \prod_{\substack{p \times l_1 \\ p \times l_2}} (p-3) \quad (p/Q).$$

и, следовательно, имеем приближенную формулу для числа троек простых чисел указанного вида в $[1, n]$

$$\pi_3(l_1, l_2, n) \approx \frac{n}{Q} \prod_{\substack{p/l_1 \\ p/l_2}} (p-1) \prod_{\substack{p/l_1 \\ p \times l_2}} (p-2) \prod_{\substack{p \times l_1 \\ p \times l_2}} (p-3) \sim c \frac{n}{\ln^3 n},$$

где c — некоторая постоянная и $p_k \leq n < p_{k+1}^2$. Из п. 3 следует, что число четверок чисел, например, вида n , $n + 2$, $n + 6$, $n + 8$, одновременно взаимно простых с $p_1, \dots, p_k$, и непревосходящих $p_1 \cdots p_k$, равно $(p_1 - 1)(p_2 - 2)(p_3 - 4) \cdots (p_k - 4)$, поэтому можно принять число четверок простых чисел указанного вида из $[1, n]$ приближенно за величину

$$\frac{n}{p_1 \cdots p_k} (p_4 - 4) \cdots (p_k - 4) \approx c \frac{n}{\ln^4 n}, \quad n < p_{k+1}^2.$$

Дополнение к доказательству леммы 1

Применяем принцип решета к последовательности A_1 натуральных чисел, непревосходящих x ,

$$A_1 \quad 1, 2, 3, 4, \dots, n^{(1)}, \quad n^{(1)} \leq x.$$

На первом шаге высеваются числа, кратные p_1 , то есть числа, равные первым членам последовательности A_1 , умноженные на p_1 и непревосходящие x . При этом высеивается и $\frac{1}{p_1}$ часть чисел, кратных $p_2, \dots, p_k$.

В результате получаем последовательность

$$A_2 \quad 1, 3, 5, 7, 9, \dots, n^{(2)}, \quad n^{(2)} \leq x,$$

содержащую не менее $Q_1 = \left\lceil x \frac{p_1 - 1}{p_1} \right\rceil$ членов вида $2k + 1 \leq x$. На втором шаге будут высеиваться члены последовательности A_2 , кратные p_2 , не превосходящие x и равные первым ее членам, умноженным на p_2 . На каждые $p_i (i = 2, 3, \dots)$ членов последовательности A_2 приходится не более одного члена, кратного p_i . Действительно, члены, кратные p_i , образуются последовательно из первых членов A_2 путем умножения их на p_i , так что если n — общее число членов A_2 , n^* — число ее членов, кратных p_i , то из неравенств

$$[x] - 1 \leq 2n^i + 1 \leq [x], \quad n \geq \frac{[x] - 2}{2}$$

$$(2n^* + 1)p_i \leq [x], \quad n^* \leq \frac{[x] - p_i}{2p_i}$$

закключаем, что $n^* \leq \frac{n}{p_i}$.

В результате высеивания чисел последовательности A_2 , кратных $p_2 = 3$, получаем последовательность

$$A_3 \quad 1, 5, 7, \dots, 25, \dots, n^{(3)}, \quad n^{(3)} \leq x,$$

содержащую не менее $Q_2 = \left\lceil Q_1 \frac{p_2 - 1}{p_2} \right\rceil$ членов, которые имеют вид $mp_1p_2 + b$, где $(b, p_1p_2) = 1$, $b < p_1p_2$, то есть $b = 1, 5$. Будем высеивать числа, кратные p_3 , равные первым членам A_3 , умноженным на p_3 и не превосходящие x . Точно так же можно показать, что на каждые $p_i (i \geq 3)$ чисел последовательности A_3 приходится не более одного числа, кратного p_i .

Предположим, что в результате высеивания чисел, кратных $p_1, \dots, p_{i-1}$, получаем последовательность

$$A_i \quad 1, p_i, p_{i+1}, \dots, p_i^2, \dots, p_i, p_{i+1}, \dots, n^{(i)}, \quad n^{(i)} \leq x,$$

в которой на каждые $p_j (j \geq i)$ чисел приходится не более одного числа, делящегося на p_j . Покажем, что в результате высеивания чисел, кратных p_i , получим последовательность A_{i+1} , в которой на каждые $p_j (j \geq i + 1)$ чисел приходится не более одного числа, делящегося на p_j . Числа последовательности A_i , подлежащие высеиванию, то есть

кратные p_i , образуются из первых ее членов, не превосходящих $\left\lceil \frac{x}{p_i} \right\rceil$,

путем умножения их на p_i . При высеивании чисел, кратных p_i , из последовательности A_i , содержащей ν групп по p_i чисел в каждой, будут высеиваться и числа, кратные $p_{i+1}, p_{i+2}, \dots$ и высеивающихся чисел образованы из ν первых чисел последовательности A_i , поэтому среди

ν высеивающихся чисел кратных p_{i+1} будет либо $\left\lceil \frac{\nu}{p_{i+1}} \right\rceil$, либо $\left\lceil \frac{\nu}{p_{i+1}} \right\rceil + 1$,

причем равным $\left\lceil \frac{\nu}{p_{i+1}} \right\rceil$ будет при p_{i+1}/ν и равным $\left\lceil \frac{\nu}{p_{i+1}} \right\rceil + 1$ при $\nu = c \cdot p_{i+1} + r$, $1 \leq r \leq p_{i+1} - 1$ и среди r чисел будет одно число, кратное p_{i+1} .

В обоих случаях: $\left\lceil \frac{\nu p_i}{p_{i+1}} \right\rceil - \left\lceil \frac{\nu}{p_{i+1}} \right\rceil \leq \frac{\nu p_i - \nu}{p_{i+1}}$ при p_{i+1}/ν ,

$$\left\lceil \frac{\nu p_i}{p_{i+1}} \right\rceil - \left\lceil \frac{\nu}{p_{i+1}} \right\rceil - 1 \leq \frac{\nu p_i - \nu}{p_{i+1}} \quad \text{при } \nu = cp_{i+1} + r.$$

Откуда заключаем, что на каждые p_{i+1} чисел последовательности A_{i+1} приходится не более одного числа кратного p_{i+1} . Таким же образом можно показать, что из каждых p_j ($j \geq i+1$) чисел A_{i+1} не более одного кратно p_j .

ЛИТЕРАТУРА

1. А. О. Гельфонд, Ю. В. Линник. Элементарные методы в аналитической теории чисел. М., 1962.
 2. А. И. Виноградов. Применение $\zeta(s)$ к решетке Эратосфена. Мат. сб. 41, 1957.
-