ИЗВЕСТИЯ
ТОМСКОГО ОРДЕНА ТРУДОВОГО КРАСНОГО ЗНАМЕНИ ПОЛИТЕХНИЧЕСКОГО ИНСТИТУТА имени С. М. КИРОВА

Том 139 1965

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

Таким образом, $\varphi_2(l, N) = N \prod\limits_{\substack{p/N \\ p/l}} \left(1-\frac{1}{p}\right) \prod\limits_{\substack{p/N \\ p\times l}} \left(1-\frac{2}{p}\right)$.

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

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

так что

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

3. Для функции $\varphi_m(l_1,\ldots, l_{m-1}, N)$, выражающей число m-чисел $n,\ldots, n+l_{m+1}$, 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 $p_1,\ldots, p_\kappa$ и непревосходящих $Q=p_1\cdots p_\kappa$, равно

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

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, что

$$\frac{\pi_2(l_1, n)}{\pi_2(l_2, n)} \to \frac{E_2(l_1, Q)}{E_2(l_2, Q)} \qquad (n \to \infty)$$

Так,

$$\frac{\pi_2(6, n)}{n_2(2, \pi)} \to 2, \qquad \frac{\pi_2(10, n)}{\pi_2(2, n)} \to \frac{4}{3}, \qquad \frac{\pi_2(2^i, n)}{\pi_2(2, n)} \to 1.$$

Следующая таблица дает представление об этой гипотезе.

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

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

$$E_2(l, n) \geqslant \left[\left[\left[n \frac{p_1 - 1}{p_1}\right] \frac{p_2 - 2}{p_2}\right] \cdots \frac{p_\kappa - 2}{p_\kappa}\right] \geqslant \frac{n}{2p_\kappa}.$$

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 дальше; после $\kappa = 1$ шага получаем последовательность чисел, в которой на каждые p_κ, начинающихся с 1, чисел не более одного делится на p_κ. Это можно показать, во-первых, тем фактом, что среди $Q = p_1 \cdots p_\kappa$ первых чисел количество чисел, взаимно простых с $p_1, \ldots, p_\kappa$, равно $(p_1 - 1)(p_2 - 1) \cdots (p_\kappa - 1)$ (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 $Q_1 = \left[Q \frac{p_1 - 1}{p_1}\right] = (p_1 - 1) p_2 \cdots p_\kappa$; далее, из оставшихся чисел взаимно простых с p_2 равно величине

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

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

$$Q_i = (p_1 - 1) \cdots (p_i - 1) p_{i+1} \cdots p_\kappa$$

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

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

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 κ. 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:

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

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

$$p_i p_{i+1},\qquad p_i p_{i+1}^2,\qquad p_i p_{i+1} p_{i+2},\ldots,\leqslant n,$$

таких чисел не меньше числа членов f геометрической прогрессии с первым членом p_{i+1}. и со знаменателем p_κ. 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 учитывании того, что при $(l,p)=1$ из p_i чисел „высеваются" по два числа n' и $n'+r$, где $r\equiv l\,(\mathrm{mod}\,p)$, $r<p$.

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

Доказательство. Найдется такое κ, что $p_\kappa\leqslant n<p_{\kappa+1}$. Число пар чисел, взаимно простых с $p_1,\ldots,p_\kappa$ в $[1,2n]$ по лемме 1 не меньше $\frac{n}{p_\kappa}\geqslant 1$. Но среди первых чисел нет искомой пары: $(p_\kappa\leqslant n<p_{\kappa+1})$. Поэтому пара чисел (быть может большее число), взаимно простых с $p_1,\ldots,p_\kappa$, находится между n и $2n$. Но они меньше $p_{\kappa+1}^2$, 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_κ и n (таких p_κ и n при фиксированном l будет бесконечное множество), что будут выполняться неравенства:

$$n+l<p_{\kappa+1}^2,\qquad n>4p_\kappa.$$

Для $n \geqslant 4p_\kappa$ имеем $E_2(l, \kappa, n) \geqslant 2$ (больше 1 нам недостаточно, так как такой парой могут оказаться числа 1 и $1+l$), следовательно между p_κ 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 $p_1,\ldots,p_\kappa$, расположены симметрично относительно числа $p_2\cdots p_\kappa$ в интервале $[1, p_1\cdots p_\kappa]$, 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

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

Доказательство. По лемме 2 число решений уравнения $P_1+P_2=2N$ в простых числах равно числу пар чисел n и $n+p_1\cdots p_\kappa-2N$, одновременно взаимно простых с $p_1,\ldots,p_\kappa$, где $p_\kappa \leqslant \sqrt{2N-1} < p_{\kappa+1}$. Действительно, если n и $n+p_1\cdots p_\kappa-2N$ взаимно простые с $p_1,\ldots,p_\kappa$, то n и $2N-n$ также взаимно просты с $p_1,\ldots,p_\kappa$ и, следовательно, ($n<p_{\kappa+1}^2$, $2N-n<p_{\kappa+1}^2$) 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 $p_1,\ldots,p_\kappa$ и непревосходящих $p_1\cdots p_\kappa+l$, равно

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

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

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

Дополнение к доказательству леммы 1

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

$$A_1 \quad 1, 2, 3, 4,\ldots, n^{(1)}, \qquad n^{(1)}\leqslant x.$$

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 высевается и $\frac{1}{p_1}$ часть чисел, кратных $p_2,\ldots,p_\kappa$. В результате получаем последовательность

$$A_2 \quad 1, 3, 5, 7, 9,\ldots, n^{(2)}, \qquad n^{(2)}\leqslant x,$$

содержащую не менее $Q_1 = \left[x \frac{p_1 - 1}{p_1} \right]$ членов вида $2\kappa + 1 \leqslant x$. На втором шаге будут высеваться члены последовательности A_2, кратные p_2, непревосходящие x и равные первым ее членам, умноженным на p_2. На каждые $p_i (i = 2, 3, \ldots)$ 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

$$[x] - 1 \leqslant 2n^i + 1 \leqslant [x], \qquad n \geqslant \frac{[x] - 2}{2}$$

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

заключаем, что $n^* \leqslant \frac{n}{p_i}$.

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

$$A_3 \quad 1, 5, 7, \ldots, 25, \ldots, n^{(3)}, \qquad n^{(3)} \leqslant x,$$

содержащую не менее $Q_2 = \left[Q_1 \frac{p_2 - 1}{p_2} \right]$ членов, которые имеют вид $mp_1p_2 + b$, где $(b, p_1 \cdot p_2) = 1$, $b < p_1 \cdot p_2$, то есть $b = 1{,}5$. Будем высевать числа, кратные p_3, равные первым членам A_3, умноженным на p_3 и непревосходящие x. Точно так же можно показать, что на каждые $p_i (i \geqslant 3)$ чисел последовательности A_3 приходится не более одного числа, кратного p_i.

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

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

в которой на каждые $p_j (j \geqslant i)$ чисел приходится не более одного числа, делящегося на p_j. Покажем, что в результате высевания чисел, кратных p_i, получим последовательность A_{i+1}, в которой на каждые $p_j (j \geqslant i + 1)$ чисел приходится не более одного числа, делящегося на p_j. Числа последовательности A_i, подлежащие высеванию, то есть кратные p_i, образуются из первых ее членов, непревосходящих $\left[\frac{x}{p_i} \right]$, путем умножения их на p_i. При высевании чисел, кратных p_i, из последовательности A_i, содержащей ν групп по p_i чисел в каждой, будут высеваться и числа, кратные $p_{i+1}, p_{i+2}, \ldots$ ν высевающихся чисел образованы из ν первых чисел последовательности A_i, поэтому среди ν высевающихся чисел кратных p_{i+1} будет либо $\left[\frac{\nu}{p_{i+1}} \right]$, либо $\left[\frac{\nu}{p_{i+1}} \right] + 1$, причем равным $\left[\frac{\nu}{p_{i+1}} \right]$ будет при $p_{i+1} | \nu$ и равным $\left[\frac{\nu}{p_{i+1}} \right] + 1$ при $\nu = c \cdot p_{i+1} + r$, $1 \leqslant r \leqslant p_{i+1} - 1$ и среди r чисел будет одно число, кратное p_{i+1}.

В обоих случаях: $\left[\frac{\nu p_i}{p_{i+1}} \right] - \left[\frac{\nu}{p_{i+1}} \right] \leqslant \frac{\nu p_i - \nu}{p_{i+1}}$ при $p_{i+1} | \nu$,

$$\left[\frac{\nu p_i}{p_{i+1}} \right] - \left[\frac{\nu}{p_{i+1}} \right] - 1 \leqslant \frac{\nu p_i - \nu}{p_{i+1}} \text{ при } \nu = cp_{i+1} + r.$$

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 $p_j (j \geqslant i+1)$ 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 решету Эратосфена. Мат. сб. 41, 1957.