Доклады Академии Наук СССР
1949. Том LXVII, № 1

МАТЕМАТИКА

А. А. БУХШТАБ

О ЧИСЛАХ АРИФМЕТИЧЕСКОЙ ПРОГРЕССИИ, У КОТОРЫХ ВСЕ ПРОСТЫЕ МНОЖИТЕЛИ МАЛЫ ПО ПОРЯДКУ РОСТА

(Представлено академиком И. М. Виноградовым 29 IV 1949)

При рассмотрении задач в области целых чисел таких, что сами числа ограничены величиной x, а их простые множители p таковы, что $x^{1/\beta} < p \leqslant x^{1/\alpha}$, приходится рассматривать решения интегро-разностных уравнений специального вида. Это одинаково относится как к задачам распределения таких чисел, так и к аддитивным задачам в области таких чисел. Некоторые задачи такого типа рассматривались мною раньше ([1,2]).

В настоящей статье я рассматриваю совокупность чисел, меньших или равных x, все простые множители которых ограничены величиной $x^{1/\alpha}$, где α — сколько угодно большое число. Имеет место следующая теорема.

Теорема. *Пусть $l < k$, $(l, k) = 1$. Обозначим через $B_l\,(k, x, x^{1/\alpha})$ число чисел в прогрессии $l + kt$, меньших или равных x, все простые множители которых меньше или равны $x^{1/\alpha}$.*

Тогда при всяком $\alpha \geqslant 1$

$$B_l(k, x, x^{1/\alpha}) = \frac{x}{k}\,\omega(\alpha) + O\left(\frac{x}{\sqrt{\ln x}}\right),$$

где

$$\omega(\alpha) = 1 - \int_1^\alpha \frac{dz_1}{z_1} + \int_2^\alpha \int_1^{z_1-1} \frac{dz_1\,dz_2}{z_1 z_2} - \ldots$$

$$\ldots + (-1)^{[\alpha]} \int_{[\alpha]}^{\alpha} \int_{[\alpha-1]}^{z_1-1} \cdots \int_1^{z_{[\alpha-1]}-1} \frac{dz_1\,dz_2 \ldots dz_{[\alpha]}}{z_1 z_2 \ldots z_{[\alpha]}}. \qquad (1)$$

Для функции $\omega(\alpha)$, которая стремится к нулю при увеличении α, дается оценка снизу. Эта оценка существенна для многих вопросов, возникающих в теории чисел, и, в частности, позволяет улучшить оценку для верхней границы наименьшего невычета степени m по простому модулю при больших значениях m.

1. Доказательство теоремы 1 основано на том, что

$$B_l(k, x, p_{i-1}) = B_l(k, x, p_i) - B_{l_{p_i}}\left(k, \frac{x}{p_i}, p_i\right),$$

где p_{i-1} и p_i — последовательные простые числа, p_i не делитель k и $0 \leqslant l_{p_i} < k$, так что при $1 \leqslant \beta \leqslant \alpha$

$$B_l(k, x, x^{1/\alpha}) = B_l(k, x, x^{1/\beta}) - \sum_{x^{1/\alpha} < p \leqslant x^{1/\beta}} B_{l_p}\left(k, \frac{x}{p}, p\right). \qquad (2)$$

Это соотношение позволяет доказать теорему по индукции.

Из (2) при $1 \leqslant \alpha \leqslant 2$, $\beta = 1$ непосредственно вытекает, что

$$B_l(k, x, x^{1/\alpha}) = \frac{x}{k}\,\omega(\alpha) + O\left(\frac{x}{\sqrt{\ln x}}\right), \text{ где } \omega(\alpha) = 1 - \int_1^\alpha \frac{dz_1}{z_1}. \qquad (3)$$

Предположим, что для всех α таких, что $N - 1 \leqslant \alpha \leqslant N$ $(N \geqslant 2)$, где α может зависеть и от x, доказано, что

$$B_l(k, x, x^{1/\alpha}) = \frac{x}{k}\,\omega(\alpha) + O\left(\frac{x}{\sqrt{\ln x}}\right), \qquad (4)$$

где $\omega(\alpha) > 0$ — непрерывная монотонно невозрастающая функция от α. Из этого предположения можно вывести, что формула (4) имеет место и для значений α таких, что $N \leqslant \alpha \leqslant N + 1$, причем в этом новом интервале

$$\omega(\alpha) = \omega(N) - \int_N^\alpha \frac{\omega(z-1)}{z}\,dz, \qquad (5)$$

что, очевидно, снова обеспечивает непрерывность и монотонное невозрастание $\omega(\alpha)$ в этом новом интервале. Для того чтобы доказать это, нужно заметить, что для простых чисел p таких, что $x^{1/u_{s+1}} < p \leqslant x^{1/u_s}$, где $N \leqslant u_s < u_{s+1} \leqslant N + 1$, будет $N - 1 \leqslant \frac{\ln(x/p)}{\ln p} \leqslant N$, так что, в силу сделанного предположения, формула (4) применима для оценки функции $B_{l_p}\left(k, \frac{x}{p}, p\right)$ при таких p. Это дает возможность получить оценку величины $B_s = \sum_{x^{1/u_{s+1}} < p \leqslant x^{1/u_s}} B_{l_p}\left(k, \frac{x}{p}, p\right)$, а именно

$$B_s = \frac{x}{k}\,\omega(\eta_s - 1)\ln\frac{u_{s+1}}{u_s} + O\left(\frac{x}{\ln x}\right) + O\left(\frac{x}{\sqrt{\ln x}}\ln\frac{u_{s+1}-1}{u_s-1}\right),$$

где $u_s < \eta \leqslant u_{s+1}$.

Выбирая $u_s = N + \frac{\alpha - N}{n}s$ $(s = 0, 1 \ldots, n)$, $c_1\sqrt{\ln x} \leqslant n \leqslant c_2\sqrt{\ln x}$, легко получить, что

$$\sum_{s=0}^{s=n-1} \omega(\eta_s - 1)\ln\frac{u_{s+1}}{u_s} = \int_N^\alpha \frac{\omega(z-1)}{z}\,dz + O\left(\frac{1}{\sqrt{\ln x}}\right),$$

так что, суммируя по всем s, получаем, что

$$\sum_{x^{1/\alpha} < p \leqslant x^{1/N}} B_{l_p}\left(k, \frac{x}{p}, p\right) = \sum_{s=0}^{s=n-1} B_s = \frac{x}{k}\int_N^\alpha \frac{\omega(z-1)}{z}\,dz + O\left(\frac{x}{\sqrt{\ln x}}\right),$$

и формула (2) при $\beta = N$ дает, что при $N \leqslant \alpha \leqslant N + 1$

$$B_l(k, x, x^{1/\alpha} = \frac{x}{k}\left\{\omega(N) - \int_N^\alpha \frac{\omega(z-1)}{z}\,dz\right\} + O\left(\frac{x}{\sqrt{\ln x}}\right),$$

т. е. искомое соотношение в этом новом интервале.

Последовательное применение формулы (5) дает возможность доказать формулу (1) по индукции. При $1 \leqslant \alpha \leqslant 2$ она верна, а если предположить справедливость формулы (1) при $N-1 \leqslant \alpha \leqslant N$, то, подставляя выражения для $\omega(N)$ и $\omega(z-1)$ в (2), получаем справедливость формулы (1) уже для интервала $N \leqslant \alpha \leqslant N+1$. Согласно принципу полной математической индукции, теорема таким образом доказана для всех $\alpha \geqslant 1$.

2. Оценим функцию $\omega(\alpha)$ снизу. Для этой функции при $2 \leqslant \beta \leqslant \alpha$, как легко видеть, имеет место соотношение

$$\omega(\alpha) = \omega(\beta) - \int_{\beta}^{\alpha} \frac{\omega(z-1)}{z}\, dz. \tag{6}$$

Это соотношение будет верно и при $1 \leqslant \beta \leqslant \alpha$, если положить $\omega(z) = 1$ при $0 \leqslant z \leqslant 1$. Арифметический смысл функции $B_l(k, x, x^{1/\alpha})$ показывает, что $\omega(\alpha)$ неотрицательна. Дифференцируя (6) по α, получаем, что $\omega'(\alpha) = -\frac{\omega(\alpha-1)}{\alpha}$ при $\alpha > 1$, т. е. мы видим, что $\omega(\alpha)$ — убывающая положительная функция от α.

Возьмем $0 < \delta < \frac{1}{3}$. Из (2) получаем, что $\omega(2-3\delta) > \frac{3}{2}\,\frac{\delta}{1-\delta}$. Если теперь предположить, что

$$\omega(k-1-k\delta) > \frac{3}{(k-1)!}\left(\frac{\delta}{1-\delta}\right)^{k-2}, \tag{7}$$

то, полагая в (6) $\alpha = k - k\delta$, $\beta = k-(k+1)\delta$, получаем, что

$$\omega(k-(k+1)\delta) \geqslant \int_{k-(k+1)\delta}^{k-k\delta} \frac{\omega(z-1)}{z}\, dz \geqslant \frac{\omega(k-1-k\delta)}{k(1-\delta)}\,\delta > \frac{3}{k!}\left(\frac{\delta}{1-\delta}\right)^{k-1},$$

т. е. оценка (7) доказана для всех $k \geqslant 2$.

Возьмем $\alpha \geqslant 6$, $\delta = \dfrac{1}{\ln\alpha + 1 + \dfrac{\ln\alpha}{\alpha}} < \dfrac{1}{3}$, $k = \left[\dfrac{\alpha+1}{1-\delta}\right] = \left[\alpha + 1 + \dfrac{1}{\ln\alpha}\right] \geqslant 10$;

тогда $(k-1)! < \left(\frac{k-1}{e}\right)^{k-1} k$.

Мы получаем, что

$$\omega(\alpha) \geqslant \omega(k-(k+1)\delta) > \frac{3}{k!}\left(\frac{\delta}{1-\delta}\right)^{k-1} > \frac{3}{k^2}\left(\frac{e\delta}{(k-1)(1-\delta)}\right)^{k-1} >$$

$$> \frac{1}{\alpha^2}\left(\frac{e\delta}{\alpha+\delta}\right)^{\alpha + \frac{\alpha}{\ln\alpha}} = e^{-\alpha\left(1+\frac{1}{\ln\alpha}\right)\left(\ln(\alpha+\delta) + \ln\frac{1}{\delta} - 1\right) - 2\ln\alpha},$$

что после ряда простых оценок дает

$$\omega(\alpha) > e^{-\alpha\left(\ln\alpha + \ln\ln\alpha + 6\,\frac{\ln\ln\alpha}{\ln\alpha}\right)}. \tag{8}$$

3. С помощью этой оценки можно усилить результаты И. М. Виноградова о наименьшем невычете степени m по простому модулю p при больших значениях m ([3],[4]). Теорему И. М. Виноградова о наименьшем невычете степени m можно сформулировать в следующем виде.

Если m — целое число $\geqslant 2$, $m / p - 1$ и $\omega(\alpha) > \frac{1}{m} + \varepsilon$, где $\varepsilon > 0$ сколь угодно мало, то наименьший невычет степени m по простому модулю p при $p > p_0$ будет меньше, чем $p^{1/2\alpha}$.

Действительно, если бы среди чисел, меньших $p^{1/2\alpha}$, не было ни одного невычета степени m по модулю p, то все $M = B_0(1, \sqrt{p}(\ln p)^2; p^{1/2\alpha})$ чисел, делящихся лишь на простые числа, меньшие, чем $p^{1/2\alpha}$, были бы также вычетами степени m, т. е. было бы $M \leqslant R$, где R — число всех вычетов степени m по модулю p, меньших, чем $\sqrt{p}(\ln p)^2$. И. М. Виноградов доказал, что при достаточно большом p $R = \frac{\sqrt{p}}{m}(\ln p)^2 + O(\sqrt{p}\ln p)$, а из (4), как легко видеть, имеем $M > \left(\omega(\alpha) - \frac{1}{2}\varepsilon\right)\sqrt{p}(\ln p)^2$, что при $\omega(\alpha) > \frac{1}{m} + \varepsilon$ противоречит тому, что $M \leqslant R$.

Вычисление функции $\omega(\alpha)$ дает, что: 1) невычеты степеней $m > 20$ меньше, чем $p^{1/6}$; 2) невычеты степеней $m > 203$ меньше, чем $p^{1/8}$; 3) невычеты степеней $m > 2825$ меньше, чем $p^{1/10}$; 4) невычеты степеней $m > 52631$ меньше, чем $p^{1/12}$, и т. д.

При больших значениях $m > e^{33}$ можно взять $\alpha = \frac{\ln m}{\ln\ln m + 2}$; тогда можно доказать, что для каждого такого m можно подобрать $\varepsilon > 0$ так, чтобы выполнялось неравенство

$$\alpha\left(\ln\alpha + \ln\ln\alpha + 6\frac{\ln\ln\alpha}{\ln\alpha}\right) < \ln m - \ln(1 + \varepsilon m).$$

Неравенство (8) дает теперь, что

$$\omega\left(\frac{\ln m}{\ln\ln m + 2}\right) > \frac{1}{m} + \varepsilon.$$

Мы получаем таким образом следующий результат:

Для всех достаточно больших простых чисел p и чисел m, являющихся делителями p, таких, что $m > e^{33}$, наименьший невычет степени m по модулю p будет меньше, чем $p^{\frac{\ln\ln m + 2}{2\ln m}}$.

Московский государственный педагогический институт им. В. И. Ленина

Поступило 21 IV 1949

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] А. А. Бухштаб, Математ. сб., нов. сер., 2, в. 6 (1937). [2] А. А. Бухштаб, Математ. сб., нов. сер., 4, в. 2 (1938). [3] И. М. Виноградов, Изв. АН СССР, 20, № 1/2 (1926). [4] И. М. Виноградов, Trans. Am. Math. Soc., 29 (1927).