Доклады Академии Наук СССР
1952. Том LXXXVII, № 2

МАТЕМАТИКА

А. В. МАЛЫШЕВ

О ПРЕДСТАВЛЕНИИ БОЛЬШИХ ЧИСЕЛ ПОЛОЖИТЕЛЬНЫМИ ТЕРНАРНЫМИ КВАДРАТИЧНЫМИ ФОРМАМИ

(Представлено академиком И. М. Виноградовым 20 IX 1952)

В настоящей заметке мы, пользуясь методом Ю. В. Линника ([1]), доказываем следующие теоремы:

Теорема 1. *Пусть $f(x, y, z)$ — положительная тернарная собственно примитивная квадратичная форма инвариантов $[k, 1]$, где k — нечетное бесквадратное число, принадлежащее роду с характерами:*

$$\left(\frac{f}{p_i}\right) = \left(\frac{-1}{p_i}\right) \quad \text{для всех } p_i \nmid k,$$

и пусть m — достаточно большое число, взаимно простое с k и удовлетворяющее родовым условиям формы f. Тогда m примитивно представимо формой f, причем число примитивных представлений $r(f, m)$ оценивается неравенствами

$$c''h(-m) > r(f, m) > c'h(-m), \tag{1}$$

где $h(-m)$ — число классов бинарных форм определителя $-m$, а постоянные c' и c'' зависят лишь от k.

Теорема 2. *Пусть k — любое нечетное число, а x_0, y_0, z_0 — целые числа, удовлетворяющие условию:*

$$\left(\frac{x_0^2 + y_0^2 + z_0^2}{p_i}\right) = \left(\frac{-1}{p_i}\right) \quad \text{для все простых } p_i \nmid k.$$

Тогда среди $r(m)$ примитивных представлений числа m суммой трех квадратов имеется

$$> cr(m) \tag{2}$$

таких, которые $\equiv (x_0, y_0, z_0) \pmod{k}$; здесь $c = c(k)$.

Эти теоремы были доказаны Линником ([1]) с более слабыми оценками, чем (1) и (2). Согласно ([1]), их доказательство сводится к доказательству следующей леммы:

Лемма. *Пусть дано произвольное нечетное число k и число m с условиями:*

а) $(m, k) = 1$;

б) $\left(\frac{-m}{p_i}\right) = \pm 1$ *для всех* $p_i \nmid k$; (3)

в) $m \neq 4^a b;\ 8b + 7$, *где* $a \geqslant 1$, b *целые.*

Пусть K — кватернион нормы k. Обозначим $r(K, m)$ число примитивных векторов L нормы m, для которых имеют место равенства

$$l_0 + L = KU, \tag{4}$$

где l_0 — целое число, а U — целый кватернион.

Тогда найдется такое $c' > 0$, зависящее только от k, что

$$r(K, m) > c' h(-m). \tag{5}$$

Доказательство. 1°. Обозначим ради краткости

$$\tau = -\frac{\ln\left(1 - \frac{1}{2(\sigma(k)-1)}\right)}{\ln(\sigma(k)-1)} = \tau(k) > 0,$$

где $\sigma(k)$ — сумма делителей числа k, и подберем целое число l_0 так, чтобы

$$\text{а) } l_0^2 + m \equiv 0 \pmod{k^s}; \qquad \text{б) } \left(\frac{l_0^2+m}{k^s},\ k\right) = 1; \qquad \text{в) } |l_0| < k^{s+1}, \tag{6}$$

где s — целое число, определяемое неравенствами:

$$\left(\frac{1}{2}+\tau\right)\frac{\ln m}{\ln(\sigma(k)-1)} \leqslant s < \left(\frac{1}{2}+\tau\right)\frac{\ln m}{\ln(\sigma(k)-1)} + 1. \tag{7}$$

В силу условий, налагаемых на m и k, это возможно.

2°. Пусть теперь $L_1, L_2, \ldots, L_{r(m)}$ — все различные примитивные векторы нормы m. В силу сравнения (6) и основной теоремы арифметики кватернионов мы можем написать $r(m)$ равенств:

$$l_0 + L_i = B_i V_i, \quad i = 1, \ldots, r(m), \tag{8}$$

где B_i — целый кватернион нормы k^s:

$$B_i = K_{i1} \cdot K_{i2} \cdot \ldots \cdot K_{is}, \quad N(K_{ij}) = k. \tag{9}$$

По типу рассуждений §§ 10—15 работы [1] можно показать, что число w различных B_i в равенствах (8) будет

$$w > c_\varepsilon m^{1/2-\varepsilon}, \tag{10}$$

даже если взять не все эти равенства, а только какие-либо $> c'_\varepsilon m^{1/2-\varepsilon'}$, $\varepsilon' < \varepsilon$, из них.

3°. Наконец, докажем нашу оценку. Пусть для некоторого L_{i_0} найдется $> c \ln m$ индексов j, для которых $K_{i_0 j} = K$. Из ряда $L_1, L_2, \ldots, L_{r(m)}$ выбросим следующие $(2s+1)$ вектора:

$$\begin{aligned} &L_{i_0}, \\ &L_{i_0}^{(j)} = (K_{i_0 1} \ldots K_{i_0 j})^{-1} L_{i_0} (K_{i_0 1} \ldots K_{i_0 j}), \quad j = 1, \ldots, s, \\ &L_{i_0}^{(-j)} = (K'_{i_0 j} \ldots K'_{i_0 s}) L_{i_0} (K'_{i_0 j} \ldots K'_{i_0 s})^{-1}, \quad j = 1, \ldots, s, \end{aligned} \tag{11}$$

где $K'_{i1}, \ldots, K'_{is}$ определяются равенством $V_i K'_{i1} \ldots K'_{is} = K_{is} \ldots K_{is} V_i$. Если среди оставшихся $L_{i'}$ найдется $L_{i_0'}$, для которого число $K_{i_0' j} = K$ более $c \ln m$, то к этому $L_{i_0'}$ применим уже описанную конструкцию выбрасывания, и т. д.

Докажем, что найдется такое c, не зависящее от m, что мы сможем повторить нашу конструкцию (для $m > m_0$) более $\frac{r(m)}{4s}$ раз. Пред-

положим противное. Тогда после не более чем $\frac{r(m)}{4s}$-кратного применения нашей конструкции у нас останутся $r' \geqslant r(m) - \frac{r(m)}{4s}(2s+1) > c'_\varepsilon m^{1/2-\varepsilon'}$ равенств (8) таких, что для каждого i количество j с условием $K_{ij} = K$ будет $< c \ln m$ для любого c. Докажем тогда, что число w различных B_l в этих равенствах будет

$$w < c_\eta m^{1/2-2\tau^2+\eta}, \tag{12}$$

где $\eta > 0$ произвольно мало при достаточно малых c. Действительно, как легко показать,

$$w < s \times C_s^{[c \ln m]} \times w_1, \tag{13}$$

где w_1 — число индексов i, для которых $K_{ij} \neq K$ при всех j.

Оценим каждый сомножитель отдельно.

а) Положим

$$s = c_1 \ln m, \text{ где } \frac{1/2+\tau}{\ln(\sigma(k)-1)} \leqslant c_1 < \frac{1/2+\tau}{\ln(\sigma(k)-1)} + \frac{1}{\ln m}.$$

Таким образом,

$$s < c_\varepsilon m^\varepsilon. \tag{14а}$$

б) Рассуждая аналогично § 4 работы [1], докажем, что

$$w_1 < c_3 m^{1/2-2\tau^2}. \tag{14б}$$

в) Оценим $C_s^{[c \ln m]}$, применяя формулу Стирлинга:

$$C_s^{[c \ln m]} = \frac{s!}{[c \ln m]!\,(s-[c \ln m])!} <$$

$$< \frac{2\sqrt{2\pi s}\left(\frac{s}{e}\right)^s}{\sqrt{2\pi[c \ln m]}\left(\frac{[c \ln m]}{e}\right)^{[c \ln m]}\sqrt{2\pi(s-[c \ln m])}\left(\frac{s-[c \ln m]}{e}\right)^{s-[c \ln m]}} <$$

$$< c_\varepsilon m^\varepsilon \frac{s^s}{[c \ln m]^{[c \ln m]}(s-[c \ln m])^{s-[c \ln m]}}.$$

Положим $[c \ln m] = c_2 \ln m$; $c_2 < c$. Тогда мы сможем переписать:

$$C_s^{[c \ln m]} < c_\varepsilon m^\varepsilon \frac{(c_1 \ln m)^{c_1 \ln m}}{(c_2 \ln m)^{c_2 \ln m}((c_1-c_2)\ln m)^{c_1 \ln m - c_2 \ln m}} =$$

$$= c_\varepsilon m^\varepsilon \left(\frac{c_1}{c_1-c_2}\right)^{c_1 \ln m}\left(\frac{c_1-c_2}{c_2}\right)^{c_2 \ln m} = c_\varepsilon m^{\varepsilon + \ln\left\{\left(\frac{c_1}{c_1-c_2}\right)^{c_1}\left(\frac{c_1-c_2}{c_2}\right)^{c_2}\right\}}.$$

Но при малых c каждое из $\left(\frac{c_1}{c_1-c_2}\right)^{c_1}$, $(c_1-c_2)^{c_2}$, $c_2^{c_2}$ близко к 1. Поэтому по $\eta_1 > 0$ можно найти такое $c_0 > 0$, что при $c < c_0$

$$\ln\left\{\left(\frac{c_1}{c_1-c_2}\right)^{c_1}\left(\frac{c_1-c_2}{c_2}\right)^{c_2}\right\} < \eta_1.$$

Тем самым мы доказали, что

$$C_s^{[c \ln m]} < c'_\eta m^\eta, \tag{14в}$$

где η мало вместе с c'_η.

Оценки (13), (14а), (14б), (14в) и дают оценку (12). Но при соответствующем выборе η при достаточно больших m оценка (12) противоречит оценке (10). Поэтому наше предположение неверно, и мы найдем такое $c>0$, что для более чем $\frac{r(m)}{4s}$ шагов нашей конструкции будет $>c\ln m$ таких индексов j, что $K_{ij}=K$.

Но тогда мы сможем образовать более чем $\frac{r(m)}{4s}\,c\ln m>c'h(-m)$ равенств типа (4) следующим образом:

$$l_0+L_i=(K_{i1}\ldots K_{ij-1}KK_{ij+1}\ldots K_{is})\,V_i,$$

$$l_0+(K_{i1}\ldots K_{ij-1})^{-1}L_i(K_{i1}\ldots K_{ij-1})=K(K_{ij+1}\ldots K_{is}V_iK_{i1}\ldots K_{ij-1}),$$

$$l_0+L_i^{(j-1)}=KV_i^{(j-1)}.$$

Пользуясь условиями конструкции отбрасывания, можно доказать, что для $m>m_0$ все $L_i^{(j-1)}$ получаются разными.

Тем самым $r(K,m)>c'h(-m)$, и лемма доказана.

Ленинградское отделение
Математического института им. В. А. Стеклова
Академии наук СССР

Поступило
18 IX 1952

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] Ю. В. Линник, Изв. АН СССР, сер. матем., 4, 363 (1940).