

МАТЕМАТИКА

Член-корреспондент АН СССР Ю. В. ЛИННИК

АСИМПТОТИЧЕСКОЕ РАСПРЕДЕЛЕНИЕ ЦЕЛЫХ ТОЧЕК НА СФЕРЕ

Количество целых точек внутри сферы $S\phi_3: x^2 + y^2 + z^2 = m$ при большом m изучалось еще Гауссом; наиболее точные результаты получены И. М. Виноградовым ⁽¹⁾. Это количество интересно своей тесной связью с сумматорными функциями для числа классов положительных бинарных квадратичных форм. Естественно возникает вопрос о распределении целых точек на поверхности сферы $S\phi_3$ при большом целом m . Некоторые предварительные результаты по этому поводу были получены в заметке автора и А. В. Малышева ⁽³⁾; они наводили на мысль, что имеет место асимптотически равномерное распределение; в настоящей заметке такая гипотеза в основном подтверждается.

Обозначим через $H(m)$ число целых точек на сфере $S\phi_3$ и через $H_0(m)$ — число примитивных точек (под условием: $(x, y, z) = 1$). Классические исследования Гаусса ⁽²⁾; art. 291) связывают $H_0(m)$ с числом классов положительных бинарных форм детерминанта $(-m)$. Число $H_0(m) \neq 0$ тогда и только тогда, если $m \equiv 1; 2 \pmod{4}$ или $m \equiv 3 \pmod{8}$, что мы и будем предполагать.

Исследование $H_0(m)$ представляет большие трудности. Лишь в 1934 г. из исследований Г. Гейльбронна ⁽⁴⁾ выяснилось, что $H_0(m) \rightarrow \infty$ при $m \rightarrow \infty$, а К. Л. Зигель ⁽⁵⁾ доказал в том же году, что

$$\ln H_0(m) \sim \frac{1}{2} \ln m \quad (1)$$

при $m \rightarrow \infty$. Этот результат К. Л. Зигеля играет основную роль в развитой автором и А. В. Малышевым аналитической теории для исследования тернарных квадратичных форм ⁽⁶⁾.

В настоящей заметке используются некоторые соображения, аналогичные доказательству асимптотического закона А. В. Малышева ⁽⁷⁾, теоретико-вероятностные соображения, в частности оценки для вероятностей больших отклонений от среднего ⁽⁸⁾, и одна геометрическая лемма В. А. Залгаллера. Здесь будут указаны основные этапы доказательства следующей теоремы:

Теорема 1. Пусть $m \equiv 1; 2 \pmod{4}$ или $m \equiv 3 \pmod{8}$. Пусть на $S\phi_3: x^2 + y^2 + z^2 = m$ задана выпуклая сферическая область Γ с кусочно-гладкой границей. Пусть q — нечетное простое число такое, что $\left(\frac{-m}{q}\right) = +1$; $H_0(\Gamma)$, $H(\Gamma)$ — соответственно, числа примитивных и любых целых точек, лежащих на Γ . Тогда при $m \rightarrow \infty$ и фиксированном q имеем:

$$H_0(\Gamma) = \frac{\text{mes } \Gamma}{4\pi m} H_0(m) (1 + \chi_0(\lambda, m, q)), \quad (2)$$

$$H(\Gamma) = \frac{\text{mes } \Gamma}{4\pi m} H(m) (1 + \chi(\lambda, m, q)), \quad (3)$$

где $\text{mes } \Gamma$ — площадь области Γ ; $\lambda > 0$ — любая константа под условием $\text{mes } \Gamma / 4\pi m > \lambda$, и $\chi_0(\lambda, m, q) \rightarrow 0$, $\chi(\lambda, m, q) \rightarrow 0$ при данных λ , q и $m \rightarrow \infty$.

Здесь число q является явно посторонним фактором, но доказательство не может без него обойтись. Не вводя постороннего числа q , можно лишь доказать следующую условную теорему:

Теорема 2. Пусть $X_m(n)$ — *реальный неглавный характер*, построенный для модуля m , и пусть ряд $L(s, X_m) = \sum_{n=1}^{\infty} X_m(n) n^{-s}$ не имеет нулей при $|s-1| < 1/4$. Тогда соотношения (2) и (3) верны с заменой $\chi_0(\lambda, m, q)$ и $\chi(\lambda, m, q)$ на $\chi_0(\lambda, m)$, $\chi(\lambda, m)$, стремящиеся к 0 при фиксированном λ и $m \rightarrow \infty$.

Здесь мы будем заниматься только теоремой 1. Легко выводится, что из (2) следует (3), так что можно заниматься только выводом (2).

При заданных λ и q фиксируем также малое число ε_0 и будем доказывать, что $|\chi_0(\lambda, m, q)| < \varepsilon_0$ при достаточно большом m . Применим следующую геометрическую лемму:

Лемма (В. А. Залгаллер). Поверхность сферы единичного радиуса можно полностью покрыть равносторонними сферическими треугольниками сколь угодно малого диаметра так, что общая площадь их перекрытий не будет превышать заданного сколь угодно малого числа, а кратность перекрытий не превышает 6.

По числу ε_0 выбирается подходящим образом малое ε_1 и производится покрытие сферы единичного радиуса треугольниками указанного в лемме типа диаметров $< \varepsilon_1$ и с общей площадью перекрытия $< \varepsilon_2$ (в дальнейшем $\varepsilon_n = \varepsilon_n(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{n-1})$ — малые положительные константы, выбираемые по предыдущим). Гомотетично расширяя наше покрытие, получаем покрытие из $g_1 = g_1(\varepsilon_1, \varepsilon_2)$ треугольников $\Delta_1, \Delta_2, \dots, \Delta_{g_1}$ на $S\phi_3$. Из этих треугольников выбираем только те, которые целиком расположены внутри области $\mathfrak{U}$, составленной из точек $S\phi_3$, под условием $x > y > z > 0$ или ее отражения в центре сферы, пусть это будут треугольники $\Delta_1, \dots, \Delta_g$. Имеем: $H_0(\mathfrak{U}) = 1/12 H_0(m) + O(m^\varepsilon)$. Можно доказать, что (2) будет следовать из соотношения

$$H_0(\Gamma) = \frac{\text{mes } \Gamma}{4\pi m} \cdot 12 \left(\sum_{i=1}^g H_0(\Delta_i) \right) (1 + \theta \varepsilon_3). \quad (4)$$

(В дальнейшем θ — число под условием $|\theta| \leq 1$, не всегда одно и то же.)

Выберем числа $k = k(\varepsilon_1, \varepsilon_2, \varepsilon_3)$, s так, что $q^{ks} \geq m^{1/2 + \varepsilon_4}$, $q^{(k-1)s} \leq m^{1/2 + \varepsilon_4}$; число l под условием $l^2 + m \equiv 0 \pmod{q^{ks}}$; $0 < l < q^{ks}$ (что возможно в силу условия $\left(\frac{-m}{q}\right) = +1$). Затем, аналогично уравнениям заметки (3), составим равенства вида:

$$l + L_\alpha = R_{\alpha 1} R_{\alpha 2} \dots R_{\alpha s} V_\alpha; \quad (5)$$

$L_\alpha^2 = -m$ и конец L_α — примитивная точка, лежащая на одном из Δ_k (что будем записывать так: $L_\alpha \in \Delta_k$) и $R_{\alpha j}$ ($j = 1, \dots, s$) выбираются из некоторого фиксированного набора $\{R\}$ неассоциированных справа кватернионов нормы q^k . Рассмотрим равенства (5) при $L_\alpha \in \Delta_k$; пусть при этом $\alpha = 1, 2, \dots, h_{\Delta_k}$; $h_{\Delta_k} = H_0(\Delta_k)$.

Обозначим $T_{\alpha j} = R_{\alpha 1} R_{\alpha 2} \dots R_{\alpha j}$ и сопоставим кватернионам $T_{\alpha j}$ единичные кватернионы $T_{\alpha j} (N(T_{\alpha j}))^{-1/2}$, которые можно изобразить точками на четырехмерной сфере $S\phi_4$: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 1$. Обозначим через $\mathfrak{U}_k = \mathfrak{U}(\Delta_k, \Gamma)$ область на $S\phi_4$, занятую точками Ω , которые переводят вектор $\vec{OO'}$, идущий из начала координат в центр

треугольника Λ_k , в область Γ по формуле $\Omega^{-1}\overrightarrow{OO'}\Omega \subset \Gamma$. Мера этой области, состоящей из двух симметричных связных кусков, как нетрудно вывести, будет

$$\frac{\text{mes } \mathcal{U}_k}{\text{mes } C\phi_1} = \frac{\text{mes } \Gamma}{4\pi m} = u.$$

В равенствах (5) вводим разбиение вторых индексов j на два типа:

I тип: такие индексы j , для которых среди операторов $\Omega_{\alpha j}$ ($\alpha = 1, 2, \dots, h_{\Lambda_k}$) число ν_j первых индексов α под условием $\Omega_{\alpha j} \in \mathcal{U}_k$ подчинено условиям

$$(1 - \varepsilon_5) u h_{\Lambda_k} \leq \nu_j \leq (1 + \varepsilon_5) u h_{\Lambda_k}. \quad (6)$$

II тип: такие индексы j , для коих это не выполняется.

Если индексов II типа меньше $s_0 = \varepsilon_6 s$, соответствующий треугольник Λ_k будем считать «допустимым». Мы будем также считать Λ_k допустимым, если $H_0(\Lambda_k) < \frac{H_0(m)}{\ln m}$ (из работы (3) следует, что это невозможно, так как $H_0(\Lambda_k) > c_0 H_0(m)$, но мы не будем здесь пользоваться этим трудно достижимым результатом).

Оказывается, можно доказать, что все треугольники Λ_k допустимы, что затем приводит к равенству (4). Приведем схему такого доказательства.

Пусть Λ_k не является допустимым. В этом случае при помощи рассуждения, аналогичного рассуждению А. В. Малышева в (7), находим, что среди первых индексов α найдется $h'_{\Lambda_k} > \varepsilon_7 h_{\Lambda_k}$ таких, что при определенных вторых индексах $j_1, \dots, j_{s_1}$, $s_1 \geq s_0/2$, количество r_α операторов $\Omega_{\alpha j} \in \mathcal{U}_k$ удовлетворяет одному из неравенств:

$$r_\alpha < (1 - \varepsilon_8) u s_1 \text{ или } r_\alpha > (1 + \varepsilon_8) u s_1. \quad (7)$$

Это предположение можно привести к противоречию.

Рассмотрим получающиеся таким образом h'_{Λ_k} равенств вида $l + L_x = R_{\alpha_1} R_{\alpha_2} \dots R_{\alpha_s} V_\alpha$ и кватернионы, отвечающие операторам $\Omega_{\alpha j_1}, \Omega_{\alpha j_2}, \dots, \Omega_{\alpha j_{s_1}}$:

$$T_{\alpha j_1} = R_{\alpha_1} \dots R_{\alpha_{j_1}}; \dots; T_{\alpha j_{s_1}} = R_{\alpha_1} \dots R_{\alpha_{j_{s_1}}}. \quad (8)$$

Пусть $M(n)$ — число примитивных кватернионов нормы n из соответствующего набора неассоциированных справа. Методами аддитивной теории чисел (9) можно доказать, что число возможных примитивных $T_{\alpha j_i}$, для которых $\Omega_{\alpha j_i} \in \mathcal{U}_k$, есть

$$\frac{\text{mes } \mathcal{U}_k}{\text{mes } C\phi_1} M(q^{j_i k}) (1 + \theta \varepsilon_9) = u M(q^{j_i k}) (1 + \theta \varepsilon_9). \quad (9)$$

Пусть $T_{\alpha j_1}$ — один из вообще возможных в качестве (8) примитивных кватернионов. При данном $T_{\alpha j_1}$ количество $T_{\alpha j_2}$ таких, что $\Omega_{\alpha j_2} \in \mathcal{U}_k$ будет, как оказывается,

$$M(\bar{Q}_0, q^{(j_2 - j_1)k}) u (1 + \theta \varepsilon_9), \quad (10)$$

где $M(\bar{Q}_0, q^{(j_2 - j_1)k})$ — число примитивных, неассоциированных справа кватернионов, не делящихся слева на заданный $\bar{Q}_0$. При этом $M(\bar{Q}_0, q^{(j_2 - j_1)k}) = M_1(q^{(j_2 - j_1)k})$ не зависит от $\bar{Q}_0$. Далее так же рассуждаем относительно $T_{\alpha j_2}, \dots, T_{\alpha j_{s_1}}$. Произведение $N = M(q^{j_1 k}) M_1(q^{(j_2 - j_1)k}) \dots M_1(q^{(j_{s_1} - j_{s_1-1})k})$ совпадает с полным числом возможных $T_{\alpha j_{s_1}}$ в (8).

Если $\Omega_{\alpha j \beta} \in \mathfrak{U}_k$, то будем говорить, что внутри $T_{\alpha j s_1}$ произошло событие $\mathfrak{U}_k$. Число таких $T_{\alpha j s_1}$, внутри которых событие $\mathfrak{U}_k$ происходит ровно r раз, равно, согласно предыдущему,

$$NC_{s_1}^r u^r (1-u)^{s_1-r} (1+\theta_1 \varepsilon_9) \dots (1+\theta_s \varepsilon_9). \quad (11)$$

Мы видим, что множитель $C_{s_1}^r u^r (1-u)^{s_1-r}$ отвечает теоретико-вероятностной схеме Бернулли для появления события с вероятностью u ровно r раз в s_1 испытаниях. Математическое ожидание числа таких появлений должно быть us_1 . Если число r подчиняется одному из неравенств (7), то число появлений нашего события будет аномально уклоняться от его математического ожидания. Вероятности таких больших уклонений могут быть рассчитаны⁽⁸⁾; они не превосходят $\exp(-\varepsilon_{10}s_1)$, где ε_{10} зависит только от ε_8 . Отсюда число возможных в наших строчках различных $T_{\alpha j \beta}$ не превосходит

$$N \exp(-\varepsilon_{10}s_1 + 2\varepsilon_9 s_1).$$

Число ε_9 выбирается по k (показателю q^k); оно может быть сделано $< 1/4 \varepsilon_{10}$, так что получим оценку $N \exp(-1/2 \varepsilon_{10}s_1)$ для числа различных $T_{\alpha j s_1}$ в наших h'_{Λ_k} строках. Полное число различных множителей $T_{\alpha s} = R_{\alpha 1} \dots R_{\alpha s}$ в них будет $\leq m^{1/2 + \varepsilon_4} \exp(-1/2 \varepsilon_{10}\varepsilon_8 s)$; при подходящем выборе ε_4 оно будет $\leq m^{1/2 - \varepsilon_{11}}$. Но такая ситуация противоречива, как доказано, например, в работе⁽⁹⁾. Это и доказывает, что все Λ_k допустимы. Для всех их индексов II типа будет $< s_0 = \varepsilon_6 s$, а для полного числа всех g треугольников Λ_k число индексов II типа $< g\varepsilon_6 s < 1/2 s$. Значит, найдется хотя бы один индекс μ , который будет I типа для всех Λ_k . Рассмотрим для всех Λ_k ($k = 1, 2, \dots, g$) все преобразования $T_{\alpha \mu}^{-1} L_{\alpha} T_{\alpha \mu} = L'_{\alpha}$. Они дают целые примитивные векторы; все они различны в силу условий, наложенных на L_{α} и $T_{\alpha \mu}$. Число их будет $1/12 H_0(m) + O(m^{\varepsilon})$. Количество тех из них, которые будут отвечать операторам $\Omega_{\alpha \mu}$, переводящим центр Λ_k в Γ , будет, согласно неравенствам (6), лежать между $(1 - \varepsilon_5) u \sum_{k=1}^g H_0(\Lambda_k)$ и

$(1 + \varepsilon_5) u \sum_{k=1}^g H_0(\Lambda_k)$. Концы таких векторов L'_{α} будут лежать в области Γ' , содержащей Γ и расширяющей ее не более чем в $(1 + \varepsilon_1)$ раз; остальные L_{α} будут вне этой области. Рассматривая далее 12 кватернионных единиц $\rho_0 = 1, \rho_1, \dots, \rho_{11}$, не связанных равенствами $\rho_i = -\rho_j$, и заменяя взятый вначале фиксированный набор $\{R\}$ на $\{R\rho_j\}$ ($j = 1, 2, \dots, 11$), получаем еще 11 наборов векторов L'_{α} в количестве $11/12 H_0(m) + O(m^{\varepsilon})$, причем число векторов L'_{α} с концами в Γ' будет заключено между числами $11(1 - \varepsilon_5) u \sum_{k=1}^g H_0(\Lambda_k)$ и

$11(1 + \varepsilon_5) u \sum_{k=1}^g H_0(\Lambda_k)$. Отсюда уже без труда получается (4) и, наконец, (2).

Ленинградский государственный
университет
им. А. А. Жданова

Поступило
5 III 1954

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

- ¹ И. М. Виноградов, Избр. тр., М., 1952, стр. 366. ² С. F. Gauss, Disquisitiones Arithmeticae, Нем. пер., Берлин, 1889. ³ Ю. В. Линник, А. В. Малышев, ДАН, 89, 209 (1953). ⁴ Н. Heilbronn, Quart. J. Math., ser. 5, 293 (1934). ⁵ С. L. Siegel, Acta Arithm., I, 83 (1935). ⁶ Ю. В. Линник, А. В. Малышев, Усп. матем. наук, 8, № 5, 3 (1953). ⁷ А. В. Малышев, ДАН, 93, 771 (1953). ⁸ В. Феллер, Введение в теорию вероятностей и ее приложения, ИЛ, 1952, стр. 147. ⁹ H. D. Kloosterman, Acta Math., 49, 407 (1926).