ДОКЛАДЫ РОССИЙСКОЙ АКАДЕМИИ НАУК. МАТЕМАТИКА, ИНФОРМАТИКА, ПРОЦЕССЫ УПРАВЛЕНИЯ, 2020, том 491, с. 19–22

МАТЕМАТИКА

УДК 511.212

О ПАРАМЕТРЕ СТОХАСТИЧНОСТИ КВАДРАТИЧНЫХ ВЫЧЕТОВ

© 2020 г. М. Р. Габдуллин[1,*]

Представлено академиком РАН С.В. Конягиным 12.11.2019 г.
Поступило 14.11.2019 г.
После доработки 20.11.2019 г.
Принято к публикации 12.12.2019 г.

Следуя В.И. Арнольду, определим параметр стохатичности $S(U)$ множества $U \subseteq \mathbb{Z}_M$ как сумму квадратов расстояний между соседними элементами множества U. В работе изучается параметр стохастичности множества R_M квадратичных вычетов по модулю M. Мы сравниваем $S(R_M)$ со средним значением $s(k) = s(k, M)$ величины $S(U)$ по всем k-элементным подмножествам $U \subseteq \mathbb{Z}_M$. Доказано, что: а) для множества модулей положительной нижней плотности справедливо неравенство $S(R_M) < s(|R_M|)$; б) для бесконечно многих модулей $S(R_M) > s(|R_M|)$.

Ключевые слова: квадратичные вычеты, параметр стохастичности
DOI: 10.31857/S2686954320020125

Рассмотрим произвольное множество U в кольце вычетов $\mathbb{Z}_n$. Пусть

$$U = \{0 \le u_1 < u_2 < \ldots < u_k < n\}$$

и $u_{k+1} = n + u_1$ (тем самым мы "склеили" $[0, n)$ в окружность). Для исследования случайности распределения точек множества U среди всех вычетов В.И. Арнольд (см. [1, §9]) вводит параметр стохастичности

$$S(U) = \sum_{i=1}^{k} (u_{i+1} - u_i)^2.$$

Несложно видеть, что $S(U)$ минимально, когда точки идут через равные интервалы, и максимально, когда все собираются в одном месте. Поэтому слишком малые или слишком большие значения $S(U)$ свидетельствуют о неслучайном поведении множества U. Имея в виду указанные два экстремальных случая, мы будем говорить, что для точек множества U имеет место отталкивание (или притяжение), если $S(U)$ меньше (соответственно больше) среднего значения параметра стохастичности среди всех k-элементных подмножеств $\mathbb{Z}_n$.

М.З. Гараев, С.В. Конягин и Ю.В. Малыхин [2] обобщают параметр стохастичности. Пусть $q > 0$; положим

$$S_q(U) = \sum_{i=1}^{k} (u_{i+1} - u_i)^q.$$

Обозначим через $N_l(U)$, $l \ge 1$, число лакун длины l во множестве U, т.е. количество таких элементов $x \in \mathbb{Z}_n$, что $x \in U, x+1, \ldots, x+l-1 \notin U$, $x+l \in U$. Тогда

$$S_q(U) = \sum_{l \ge 1} N_l(U) l^q \qquad (1)$$

(и, в частности, $S(U) = \sum_{l \ge 1} N_l(U) l^2$). Авторы доказывают, что если $|U| = k < n$ и $\frac{k}{\sqrt{n}} \to \infty$, то для среднего значения $s_q(k, n)$ величины $S_q(U)$ для множества U из k элементов справедливо равенство

$$s_q(k, n) = \frac{k^2}{n} \sum_{l=1}^{\infty} \left(1 - \frac{k}{n}\right)^{l-1} l^q (1 + o(1)).$$

Отметим, что эта асимптотическая формула согласуется со следующими эвристическими соображениями: вероятность того, что некоторая точка случайного множества из k элементов будет началом лакуны длины l, равна $\left(\frac{k}{n}\right)^2 \left(1 - \frac{k}{n}\right)^{l-1}$, и поэтому в среднем величина $N_l(U)$ должна быть близка к $\frac{k^2}{n}\left(1 - \frac{k}{n}\right)^{l-1}$.

[1] *Математический институт им. В.А. Стеклова Российской академии наук, Москва, Россия*
**E-mail: gabdullin.mikhail@yandex.ru*

Кроме того, авторы отмечают, что в случае $q = 2$ величину $s(k) := S_2(k, M)$ можно выписать явно.

Предложение 1. *Имеем*

$$s(k) = \frac{M(2M - k + 1)}{k + 1}.$$

В работе [2] оцениваются величины $S_q(G)$ в случае, когда $n = p$ – простое число, а множество G является подгруппой $G_t \subset \mathbb{Z}_p^*$ порядка t, т.е. состоит из d-х степеней чисел от 1 до $p - 1$, где $d = \frac{p-1}{t}$. Основным результатом работы [2] является

Теорема А. *Существует константа $c > 0$ такая, что при $q \in (0, 4)$ и $d \le \exp(c\sqrt{\log p})$ справедлива асимптотическая формула*

$$S_q(G_t) = S_q\left(\frac{p-1}{d}\right)(1 + o(1)), \quad p \to \infty.$$

Таким образом, большие мультипликативные подгруппы $\mathbb{Z}_p^*$ с точки зрения поведения величины $S_q(G)$ близки к случайным множествам соответствующего размера.

В настоящей работе изучается параметр стохастичности для множества R_M квадратичных вычетов по модулю M. Мы доказываем отталкивание квадратичных вычетов для множества модулей положительной нижней плотности (здесь и везде далее мы имеем в виду нижнюю асимптотическую плотность, т.е. величину $d(A) = \liminf\limits_{N\to\infty} \frac{|A \cap \{1,\dots,N\}|}{N}$, $A \subseteq \mathbb{N}$), а также их притяжение для бесконечно многих модулей. Перейдем к точным формулировкам. Пусть c_0 и C_0 – абсолютные положительные постоянные, причем c_0 достаточно мало, а C_0 достаточно велико. Обозначим через Ω множество чисел M таких, что $M = Am$, где $m = p_1 \dots p_t$, причем $t \ge 0.4\log\log M$ и $p_1 < p_2 < \dots < p_t$ – различные простые числа, большие $2^{C_0 t}$, а число A бесквадратно, $(A, m) = 1$ и $A \le 2^{c_0 t}$.

Основным результатом данной работы является

Теорема 1. *Существует абсолютная постоянная $c > 0$ такая, что при $M \in \Omega$ имеет место асимптотическая формула*

$$S(R_M) = m2^{t+1}A^2|R_A|^{-1} - A^2|R_A|^{-1}m + E, \qquad (2)$$

где

$$E \ll m2^{3t}A^4 p_1^{-c} + mA^2|R_A|2^{-t} = o(m),$$
$$M \to \infty, \quad M \in \Omega.$$

Кроме того, множество Ω имеет положительную нижнюю плотность.

С другой стороны, для модулей $M \in \Omega$ предложение 1 дает нам

$$s(|R_M|) = m2^{t+1}A^2|R_A|^{-1} - Am + O(A^2|R_A|^{-1}m2^{2t}p_1^{-1}). \qquad (3)$$

Таким образом, главные члены в полученных асимптотических формулах $S(R_M)$ и $s(|R_M|)$ совпадают. Отсюда мы получаем аналог теоремы А.

Следствие 1. *Имеем*

$$S(R_M) = s(|R_M|)(1 + o(1)), \quad M \to \infty, \quad M \in \Omega.$$

Сравнивая вторые члены в (2) и (3), мы улавливаем отталкивание квадратичных вычетов.

Следствие 2. *При всех достаточно больших $M \in \Omega$ с $A \ge 3$ справедливо*

$$S(R_M) < s(|R_M|).$$

Кроме того, для модулей вида $M = Ap$, где p – простое и $(A, p) = 1$, мы можем написать асимптотику с меньшим остаточным членом, что позволяет нам установить притяжение квадратичных вычетов по бесконечно многим модулям.

Теорема 2. *Пусть $M = Ap$, $(A, p) = 1$. Тогда*

$$S(R_M) = 2f_A(0.5)p + O(A^4 p^{1-c}),$$

где f_A – рациональная функция, определяемая числом A.

Коэффициенты рациональной функции f_A можно выписывать явно. Пусть $s_1, \dots, s_{|R_A|}$ – последовательные расстояния между квадратичными вычетами по модулю A, пронумерованные вычетами по модулю $|R_A|$. Тогда

$$f_A(y) = \frac{F(y)}{Q(y)},$$

где $Q(y) = Q_A(y) = 1 + y + \dots + y^{|R_A|-1}$, а $F(y) = F_A(y) = \sum\limits_{k=0}^{|R_A|} \beta_k y^k$ – возвратный многочлен с коэффициентами $\beta_0 = \beta_{|R_A|} = \sum\limits_i s_i^2$ и $\beta_k = 2\sum\limits_{i=1}^{|R_A|} s_i s_{i+k}$ при $0 < k < |R_A|$ (мы считаем, что индексы i чисел s_i вычисляются по модулю $|R_A|$). Отметим, что поведение функции f_A в окрестности точки $y = 1$ является определяющим фактором для притяжения или отталкивания квадратичных вычетов.

Из предложения 1 (или из (3) при $t = 1$) для модулей того же вида находим

$$s(|R_M|) = \left(\frac{4A^2}{|R_A|} - A\right)p + O(A^2|R_A|^{-1}).$$

Численная проверка показывает, что

$$2f_A(0.5) < \frac{4A^2}{|R_A|} - A$$

при всех $3 \le A \le 100$, $A \ne 89$, и

$$2f_A(0.5) > \frac{4A^2}{|R_A|} - A$$

при $A = 89$. Таким образом, из теоремы 2 вытекает следующее утверждение.

Следствие 3. *Имеем*

$$\underline{\lim_{M\to\infty}} \frac{S(R_M)}{s(|R_M|)} < 1 < \overline{\lim_{M\to\infty}} \frac{S(R_M)}{s(|R_M|)}.$$

Из неравенства Коши–Буняковского следует, что

$$\overline{\lim_{M\to\infty}} \frac{S(R_M)}{s(|R_M|)} \ge 0.5.$$

В то же время мы не знаем, конечен ли верхний предел $\overline{\lim_{M\to\infty}} \frac{S(R_M)}{s(|R_M|)}$. Отметим, что в недавней работе Ф. Арьяна [3] доказано, что в случае бесквадратных M справедлива оценка

$$S(R_M) \ll M \cdot 2^{\omega(M)} \log M \prod_{p|M} \left(1 + \frac{1}{\sqrt{p}}\right)\left(1 - \frac{1}{p}\right).$$

Обсудим основные идеи доказательства теоремы 1 (теорема 2 доказывается аналогично, но технически несколько проще). Зафиксируем $\alpha \in \left(0, \frac{1}{10}\right)$ и достаточно малое число $\varepsilon_0 > 0$. Положим $d_1 := \frac{\alpha A}{2|R_A|} 2^t \log p_1$ и $d_2 := \frac{A}{|R_A|} p_1^{\varepsilon_0}$. Мы записываем величину $S(R_M)$ в виде $\sum_{l\ge 1} N_l(R_M) l^2$ (см. (1)) и разбиваем эту сумму на три части. Далее мы находим асимптотику для вклада от малых лакун длины $l \le d_1$ в терминах функции f_A, определяемой числом A, и показываем, что вклад средних (длины $l \in (d_1, d_2]$) и больших (длины $l > d_2$) лакун соответственно асимптотически мал; более точно, мы доказываем, что

$$S(R_M) = m \cdot 2^t f_A(y_t) + O(m \cdot 2^{4t} A^4 p_1^{-c_1}),$$

где $c_1 > 0$ – некоторая абсолютная постоянная и $y_t = 1 - 2^{-t}$. Наконец, мы показываем, что $f_A(1) = 2A^2 |R_A|^{-1}$, $f_A'(1) = A^2 |R_A|^{-1}$ и $f_A''(y) \ll A^2 |R_A|$ при $y \in (y_t, 1)$ в предположении $|R_A| \ll 2^t$. После этого первое утверждение теоремы 1 получается разложением функции f_A в ряд Тейлора в окрестности точки $y = 1$. Наконец, тот факт, что множество Ω имеет положительную нижнюю плотность, доказывается с помощью некоторых комбинаторных рассуждений и методов решета.

Отметим, что для нахождения асимптотики для вклада от малых лакун можно использовать предельное распределение расстояний между квадратичными вычетами, которое было найдено в работе П. Курлберга и З. Рудника [4] для бесквадратных модулей и в работе П. Курлберга [5] для произвольных модулей. Пусть $0 = u_1 < u_2 < \ldots < u_{R_M} < M$ – множество квадратичных вычетов по модулю M. Следующий результат был получен в работе [5].

Теорема B. *При $t \ge 0$ имеем*

$$|R_M|^{-1} \#\{j \in \{1, \ldots, |R_M|\} : u_j - u_{j-1} > tM |R_M|^{-1}\} = e^{-t} + o(1)$$

при $\omega(M) \to \infty$, причем эта оценка равномерна при $t \in [0, t_0]$ для любого фиксированного $t_0 > 0$.

Тем не менее, слагаемое $o(1)$ в правой части помешает нам найти второй член в асимптотике для $S(R_M)$; поэтому мы используем другие соображения (и рассматриваем модули специального вида).

Доказательство теоремы 1 позволяет также получить нижнюю оценку (довольно слабую) на плотность множества Ω; мы не стремились выписать ее явно и оптимизировать.

По-видимому, наш метод не позволяет улавливать притяжение для большого числа модулей. Тем не менее, мы считаем весьма правдоподобным, что притяжение квадратичных вычетов должно иметь место также для множества модулей положительной нижней плотности.

ИСТОЧНИК ФИНАНСИРОВАНИЯ

Исследование выполнено за счет гранта Российского научного фонда (проект 19–11–00001).

СПИСОК ЛИТЕРАТУРЫ

1. *Арнольд В.И.* Группы Эйлера и арифметика геометрических прогрессий. М.: МЦНМО, 2003.
2. *Гараев М.З., Конягин С.В., Малыхин Ю.В.* Асимптотика суммы расстояний между степенными вычетами по простому модулю. Тр. МИАН. 2012. Т. 276. С. 1–13.
3. *Aryan F.* Distribution of squares modulo a composite number // Int. Math. Res. Not. IMRN 2015. V. 23. P. 12405–12431, https://arxiv.org/pdf/1502.05062.pdf.
4. *Kurlberg P., Rudnick Z.* The Distribution of Spacings between Quadratic Residues // Duke Math. J. 1999. V. 100. P. 211–242.
5. *Kurlberg P.* The Distribution of Spacings between Quadratic Residues. II // Israel J. Math. 2000. V. 120. Pt. A. P. 205–224.

ON THE STOCHASTICITY PARAMETER OF QUADRATIC RESIDUES

M. R. Gabdullin

Steklov Mathematical Institute of the Russian Academy of Sciences, Moscow, Russian Federation

Presented by Academician of the RAS S.V. Konyagin

Following V.I. Arnold, we define the stochasticity parameter $S(U)$ of the set $U \subseteq \mathbb{Z}_M$ to be the sum of squares of consecutive distances between elements of U. We study the stochasticity parameter of the set R_M of quadratic residues modulo M. We compare $S(R_M)$ with the average value $s(k) = s(k, M)$ of $S(U)$ over all subsets of $U \subseteq \mathbb{Z}_M$ of size k. We prove that: a) for a set moduli of positive lower density we have $S(R_M) < s(|R_M|)$; b) for infinitely many moduli $S(R_M) > s(|R_M|)$.

Keywords: quadratic residues, the stochasticity parameter