Отчёт по конкурсу «Молодая математика России» за 2020 год
Габдуллина Михаила Рашидовича

0.1 Результаты, полученные в 2020 году

Многие интригующие задачи теории чисел возникают при одновременном рассмотрении аддитивной и мультипликативной структур целых чисел (колец вычетов, полей): к ним можно отнести проблему простых чисел-близнецов, проблемы Гольдбаха, принцип сумм-произведений в его разных формах, теорему Грина-Тао о наличии сколь угодно длинных арифметических прогрессий в простых числах, гипотезу Виноградова о наименьшем квадратичном невычете, а также многие другие нерешенные проблемы и знаменитые теоремы. Имеется также общий принцип, согласно которому множество, имеющее богатую аддитивную структуру (например, содержащее длинные арифметические прогрессии, или имеющее большую аддитивную энергию или малую константу удвоения, и т.п.), должно обладать случайными мультипликативными свойствами, и наоборот — множество, имеющее богатую мультипликативную структуру, должно обладать случайными аддитивными свойствами. В частности, множество $R_m = \{a^2 : a \in \mathbb{Z}_m\}$ квадратичных вычетов, имея ярко выраженную мультипликативную структуру (так, при простом p множество $R_p \setminus \{0\}$ — подгруппа индекса 2 в $\mathbb{Z}_p^*$) должно быть «случайно» с аддитивной точки зрения. В 2020 году мною были получены результаты в двух известных задачах, иллюстрирующих последний (неформальный) принцип.

Первая из этих задач следующая: насколько большим может быть множество $A \subset \mathbb{Z}_m$, если известно, что $(A - A) \cap R_m = \{0\}$? Так как $A - A$ имеет богатую аддитивную структуру, то согласно сказанному выше, оно должно иметь случайные мультипликативные свойства, и потому не должно избегать квадратичных вычетов, если только A не совсем мало. Таким образом, резонно ожидать, что множества A с указанным свойством малы; имеется гипотеза, согласно которой при бесквадратных m справедлива оценка $|A| \ll_\varepsilon m^\varepsilon$. Кроме того, для случая простого $m = p \equiv 1 \pmod 4$ задача имеет следующую интерпретацию на языке теории графов. Определим граф Пэли G_p как граф с множеством вершин $\mathbb{Z}_p$ и множеством ребер $E_p = \{\{x, y\} : x - y \in R_p \setminus \{0\}\}$ (при указанном ограничении на p это неориентированный регулярный граф). Тогда максимальный размер множества $A \subset \mathbb{Z}_p$, разность которого избегает квадратичных вычетов, равен размеру максимальной клики в графе G_p. Графы Пэли обладают рядом случайных свойств; ожидается, что максимальная клика в них имеет логарифмический размер. Тем не менее, для неё неизвестно ничего лучше корневой верхней оценки; для исходной задачи также была известна оценка $m^{1/2+o(1)}$, но и то лишь для почти всех (в смысле асимптотической плотности) бесквадратных модулей. Подобный «корневой барьер» встречается в разных задачах теории чисел, и, как правило, преодолеть его либо очень сложно, либо вовсе невозможно. Тем не менее, в нашей совместной работе с Кевином Фордом нам удалось получить в этой задаче существенное продвижение и доказать следующую теорему.

Теорема 1 *Пусть $\varepsilon(m)$ стремится к нулю сколь угодно медленно. Тогда для почти всех модулей m и всякого множества $A \subset \mathbb{Z}_m$ такого, что $(A-A) \cap R_m = \{0\}$, справедлива оценка*

$$|A| \leqslant m^{1/2-\varepsilon(m)}.$$

Выбирая, скажем, $\varepsilon(m) = \frac{1}{\sqrt{\log m}}$, мы получаем, что для почти всех модулей в этой задаче имеет место оценка $|A| = o(m^{1/2})$.

Вторая задача о квадратичных вычетах, в которой я получил результаты, была поставлена В. И. Арнольдом. Пусть $U = \{0 \leqslant u_1 < u_2 < \ldots u_k < m\}$ — k-элементное подмножество $\mathbb{Z}_m$. Определим параметр стохастичности $S(U)$ множества U как сумму квадратов последовательных расстояний между элементами множества U:

$$S(U) = \sum_{i=1}^{k} s_i^2,$$

где $s_i \in \mathbb{R}^+$ и $s_i = u_{i+1} - u_i$, $i = 1, \ldots, k-1$, $s_k = u_1 + m - u_k$. Зафиксируем $k = |U|$; тогда нетрудно показать, что $S(U)$ минимально, если все s_i равны (или почти равны) между собой, и $S(U)$ максимально, если U является интервалом длины k. Таким образом, слишком малые или слишком большие значения $S(U)$ свидетельствуют о неслучайном поведении множества U; естественно сравнивать $S(U)$ со средним значением параметра стохастичности, взятого по всем подмножествам $\mathbb{Z}_m$ размера k. Обозначим эту величину через $s(k) = s(k, \mathbb{Z}_m)$; на неё можно смотреть как на параметр стохастичности случайного множества размера k. Как уже отмечалось выше, резонно ожидать, что множество квадратичных вычетов R_m имеет случайные аддитивные свойства, и потому $S(R_m)$

должно быть близко к $s(|R_m|)$. Гараев, Малыхин и Конягин показали, что

$$S(R_p) = s(|R_p|)(1 + o(1)), \quad p \to \infty, \tag{1}$$

тем самым подтверждая сказанное для случая простого модуля. В своей работе я рассмотрел эту задачу по составным модулям и получил следующие результаты.

Теорема 2 *Существует множество* $\mathcal{M} \subset \mathbb{N}$ *положительной плотности такое, что*
а) $S(R_m) = s(|R_m|)(1 + o(1))$, $m \in \mathcal{M}$, $m \to \infty$.
б) $S(R_m) < s(|R_m|)$ *при всех* $m \in \mathcal{M}$.

Таким образом, имеет место аналог соотношения (1) для достаточно большого числа модулей m; при этих m множество R_m ведёт себя случайно с точки зрения параметра стохастичности, и при этом можно дополнительно гарантировать, что $S(R_m)$ меньше соответствующего среднего значения. Однако, аналог (1) для всех модулей неверен:

Теорема 3 *Справедливы неравенства*

$$\varliminf_{m\to\infty} \frac{S(R_m)}{s(|R_m|)} < 1 < \varlimsup_{m\to\infty} \frac{S(R_m)}{s(|R_m|)}.$$

Естественно предположить, что имеет место аналог соотношения (1) для почти всех модулей. Кроме того, было бы интересно найти поведение $S(R_m)$ в среднем по модулям $m \leqslant X$. Я планирую рассмотреть эти задачи в ближайшем будущем.

0.2 Опубликованные и поданные в печать работы

1. М. Р. Габдуллин, *Нижние оценки винеровской нормы в* $\mathbb{Z}_p^d$, Матем. заметки, 107:4 (2020), 515–532.

2. М. Р. Габдуллин, *О параметре стохастичности квадратичных вычетов*, Докл. РАН. Мат. информ. проц. упр., 491:1 (2020), 19–22.

3. K. Ford, M. R. Gabdullin, *Sets whose differences avoid squares modulo* m, https://arxiv.org/abs/2007.05774.

4. M. R. Gabdullin, *On the stochasticity parameter of quadratic residues*, https://arxiv.org/abs/2010.04982.

0.3 Участие в конференциях и школах

Участвовал в XX Международной Саратовской зимней школе «Современные проблемы теории функций и их приложения», 28 января – 1 февраля 2020 года, Саратов (без доклада). Был одним из организаторов Международной конференции по аналитической теории чисел, посвященной 75-летию Г. И. Архипова и С. М. Воронина (14-16 декабря 2020 года, онлайн формат).

0.4 Работа в научных центрах и международных группах

Являюсь сотрудником отдела теории чисел Математического института им. В. А. Стеклова РАН, сотрудником Математического центра мирового уровня «Математический институт им. В. А. Стеклова РАН» и сотрудником лаборатории «Многомерная аппроксимация и приложения» при мехмате МГУ.

0.5 Педагогическая деятельность

Прочитан спецкурс “Теория чисел” для магистров МФТИ на базе Математического института им. В.А. Стеклова РАН; см. http://www.mathnet.ru/php/conference.phtml?option_lang=rus&eventID=31&confid=1840 .