

**О некоторых работах по аддитивной комбинаторике
в Отделе теории чисел**

С.В. Конягин, М.А. Королёв

(стендовый доклад на конференции «МИАН-90» 13 мая 2024 года)

§1. Теорема Рота для многих переменных.

Пусть $N \geq k \geq 3$ – натуральные числа. Через $\alpha_k(N)$ обозначим максимум отношения $|A|/N$, где максимум берется по всем множествам $A \subset \{1, \dots, N\}$, не содержащим непостоянных арифметических прогрессий длины k . Erdős и Turán предположили, что при фиксированном k справедливо равенство

$$\lim_{N \rightarrow \infty} \alpha_k(N) = 0.$$

Первый прорыв сделал Roth, доказавший гипотезу для $k = 3$. Он установил, что

$$\alpha_3(N) = O(1/\log \log N).$$

Behrend почти 80 лет назад получил нижнюю оценку для $\alpha_3(N)$:

$$\alpha_3(N) \geq \exp(-c\sqrt{\log N}). \quad (1)$$

С тех пор она по существу не улучшалась и, скорее всего, является правильной. Получением оценок сверху занимались многие математики, включая таких выдающихся, как Heath-Brown, Szemerédi, Bourgain. До недавнего времени были известны логарифмические оценки типа

$$\alpha_3(N) \leq (\log N)^{-c+o(1)}.$$

При этом значение величины c неоднократно улучшалось. Но логарифмические оценки были очень далеки от нижней оценки (1).

В работе И.Д. Шкредова [Shk2] (соавтор – Schoen) указан новый рубеж, с которого можно атаковать проблему получения верхних оценок для $\alpha_3(N)$, приближающихся к (1). Величину $\alpha_3(N)$ можно определить как максимум отношения $|A|/N$, где максимум берется по всем множествам $A \subset \{1, \dots, N\}$, не содержащих троек различных чисел x_1, x_2, y таких, что $x_1 + x_2 = 2y$. Аналогично для любого $k \geq 2$ можно определить $\gamma_k(N)$ как максимум отношения $|A|/N$, где максимум берется по всем множествам $A \subset \{1, \dots, N\}$, не содержащих различных чисел $x_1, \dots, x_k, y$ таких, что $x_1 + \dots + x_k = ky$. Таким образом, $\gamma_2(N) = \alpha_3(N)$.

Можно ожидать, что любого $k \geq 2$ и для больших N выполняется неравенство $\alpha_{k+1}(N) \leq \alpha_k(N)$. Тем не менее для любого фиксированного k выполнен аналог неравенства (1) с заменой α_3 на γ_k . При этом величина $c > 0$ зависит от k .

В [Shk2] авторы устанавливают оценку субстепенного типа, приближающуюся к нижней оценке типа (1) для $\gamma_k(N)$. Они показали, что

$$\gamma_5(N) \leq \exp(-c(\log N / \log \log N)^{1/6}) \quad (N \geq 3).$$

Трудная многолетняя работа по улучшению верхних оценок величины $\alpha_3(N)$ привела к успеху: Kelly и Mea установили субстепенную оценку! Наилучший известный докладчику результат

$$\alpha_3(N) \leq \exp(-c(\log N)^{1/9})$$

получили Bloom и Sisask.

§2. Удвоение и энергия выпуклых множеств.

Пусть A, B — подмножества абелевой группы. Мы можем определить их сумму и разность:

$$A \pm B = \{a \pm b : a \in A, b \in B\}.$$

При наличии дополнительной структуры абелевой группы можно определять и другие операции. Так, если она является кольцом, то можно определить и произведение множеств AB . В данной секции нас будет интересоваться AA , где $A \subset \mathbb{R}$, $0 < |A| < \infty$. Легко получить оценки

$$2|A| - 1 \leq |A + A| \leq |A|(|A| + 1)/2. \quad (2)$$

Оба неравенства точные, причем левое достигается в том и только том случае, когда A образует арифметическую прогрессию.

Для конечного множества A определим его энергию

$$E(A) = |\{(a_1, a_2, a_3, a_4) \in A : a_1 + a_2 = a_3 + a_4\}|.$$

Легко видеть, что

$$2|A|^2 - |A| \leq E(A) \leq |A|^3.$$

Оценки справедливы для любой абелевой группы. Для подмножеств $A \subset \mathbb{R}$ верхнюю оценку можно уточнить, но порядок $|A|^3$ является правильным.

Нетрудно показать, что $|A + A|$ и $E(A)$ связаны соотношением

$$|A + A| \geq |A|^4 / E(A).$$

Таким образом, нетривиальная верхняя оценка для $E(A)$ влечет нетривиальную верхнюю оценку для $|A + A|$.

Множество $A = \{a_1 < \dots < a_N\}$ называется выпуклым, если $a_{i+1} - a_i > a_i - a_{i-1}$, $i = 2, \dots, N - 1$. Такие множества очень непохожи на арифметические прогрессии, так что естественно предположить, что для выпуклых множеств A энергия намного меньше $|A|^3$ и, следовательно, $|A + A|$ намного больше $|A|$. Так оно и оказалось. Гараев и докладчик независимо показали, что для выпуклого множества A , справедливо неравенство

$$E(A) \leq C|A|^{5/2}.$$

Следовательно,

$$|A + A| \geq c|A|^{3/2} \quad (c > 0). \quad (3)$$

Неравенство (3) довольно простое, его можно доказывать различными способами. Но улучшить его очень трудно, для этого требуются новые идеи. Такое улучшение сделали Schoen и Шкредов [Shk3]. Они доказали, что

$$|A + A| \geq c|A|^{14/9}(\log^{-2/3} |A|) \quad (|A| \geq 2).$$

Работа [Shk3] характерна для И. Д. Шкредова. Он рассматривает задачи, в которых имеется естественная оценка, которую трудно улучшить. И часто находит путь для улучшения! Такие работы И. Д. Шкредова обычно вызывают возрождение или рост интереса коллег к этим задачам.

Конечно, задачи об оценках энергии или мощности удвоения выпуклого множества относятся к аддитивной комбинаторике. В то же время они связаны с задачами об оценке тригонометрических сумм и норм тригонометрических полиномов. Не удивительно, что постановка задач возникла из работ Анатолия Алексеевича Карацубы и Сергея Викторовича Бочкарева.

§3. Проблема сумм и произведений в полях простого порядка.

Напомним, что Erdős и Szemerédi поставили ставшую знаменитой проблему о суммах и произведениях. Пусть $A \subset \mathbb{R}$ — конечное множество и $\varepsilon > 0$. Тогда имеет место неравенство

$$\max(|A + A|, |AA|) \geq C(\varepsilon)|A|^{2-\varepsilon}.$$

Проблема остается далекой от своего решения. В ряде работ получены оценки вида

$$\max(|A + A|, |AA|) \geq c(\gamma)|A|^{1+\gamma} \quad (4)$$

для различных значений γ . В настоящее время (4) доказано для некоторого $\gamma > 1/3$.

Проблема становится еще более трудной, если рассматривать подмножества A поля $\mathbb{F}_p$, где p — простое число. Отметим, что сама постановка задачи требует определенной коррекции. Если $|A|$ близко к p , то мощности множеств $A+A$ и AA не могут быть значительно больше $|A|$. Поэтому вопрос должен ставиться в предположении, что $|A|$ намного меньше p . В течение нескольких десятилетий был найден ряд различных доказательств неравенств вида (4) для множеств $A \subset \mathbb{R}$, но ни одно из них не переносилось на подмножества поля $\mathbb{F}_p$. Прорыв совершили Bourgain, Katz, Tao. Они доказали, что для любого $\varepsilon \in (0, 1/2)$ существуют $\gamma > 0$ и $c(\varepsilon) > 0$ такие, что для любого множества $A \subset \mathbb{F}_p$, удовлетворяющего условию

$$p^\varepsilon \leq |A| \leq p^{1-\varepsilon},$$

выполнено (4) с заменой $c(\gamma)$ на $c(\varepsilon)$.

Эта работа стала началом нового плодотворного направления теории чисел, развиваемого Bourgain'ом и другими математиками. За эти работы Bourgain был удостоен Shaw Prize.

Bourgain, Глибичук, Конягин, используя метод С.А. Степанова, доказали соответствующий результат о суммах и произведениях без предположения $p^\varepsilon \leq |A|$. В частности, существуют абсолютные положительные константы γ и c такие, что для множества $A \subset \mathbb{F}_p$, $|A| < \sqrt{p}$, выполнено неравенство (4) с $c(\gamma) = c$. Доказательство полностью эффективно, так что оно в принципе позволяет найти явное значение константы γ . Мы этого не пытались делать, так как это значение получилось бы слишком малым.

Используя ряд интересных соображений, М. Z. Garaev показал, что в качестве γ можно взять любое положительное число, меньшее $1/14$. Развивая идеи Гараева, авторы ряда работ понемногу улучшали численное значение γ . Bourgain очень ценил эту деятельность и говорил, что любое улучшение величины γ будет значимым результатом.

И вдруг произошло нечто совершенно непредвиденное: значение γ было увеличено сразу в два раза! Это сделали O.Roche–Newton, M. Rudnev и И.Д. Шкредов [Shk4]. Они показали, что можно взять $\gamma = 1/5$. Ясно, что такое значительное продвижение потребовало принципиально новых идей.

Многие результаты аддитивной комбинаторики получены с использованием теоремы Семереди–Троттера об оценке числа инцидентности конечных систем точек и прямых на плоскости. При этом правильная оценка в зависимости от количества точек и количества прямых хорошо известна. Беда лишь в том, что она известна для плоскости над полем $\mathbb{R}$. Для конечных полей понимания ситуации нет, а известные оценки для числа инцидентности, скорее всего, являются слабыми и намного хуже правильных.

М. Руднев нашел хорошие верхние оценки на количество инцидентности точек и двумерных плоскостей в трехмерном пространстве при наличии определенных предположений на точки и плоскости. Преимущество такого подхода состоит в том, что результаты справедливы не только в действительном пространстве, но и в пространствах над конечными полями. Эти оценки оказались очень эффективны для приложений к задачам аддитивной комбинаторики. В частности, они позволили получить вышеуказанные оценки в проблеме сумм–произведений в $\mathbb{F}_p$. И.Д. Шкредов с соавторами использовал инцидентность точек и плоскостей в ряде других задач аддитивной комбинаторики.

§4. Проблема Зарембы.

В 1972 году Zarembka высказал ставшую знаменитой гипотезу о том, что для любого натурального числа $q > 1$ найдется натуральное число $a < q$, взаимно простое с q , такое, что неполные частные в разложении числа a/q ограничены абсолютной константой (возможно, не превосходят 5). Проблема связана с построением сетки Коробова размера q на квадрате $[0, 1) \times [0, 1)$, то есть множества вида

$$\left\{ \left(\left\{ \frac{j}{q} \right\}, \left\{ \frac{aj}{q} \right\} \right), j = 0, 1, \dots, q-1 \right\},$$

где $\{u\}$ обозначает дробную часть числа u , с минимальным по порядку дискрепансом (среди всех множеств мощности q , а не только сеток Коробова). Явное указание множеств с малым дискрепансом важно для построения эффективных квадратурных формул.

Еще до публикации проблемы Н.М. Коробов показал, что для любого натурального числа $q > 1$ найдется натуральное число $a < q$, взаимно простое с q , такое, что неполные частные в разложении числа a/q ограничены числом $C \log q$. Более полувека этот результат не улучшался, в том числе и при предположении простоты числа q .

Недавно проблема была сдвинута с «мертвой точки». Н.Г. Мошечевин, В. Murphy и И.Д. Шкредов [Shk5] доказали, что для любого свобод-

ного от квадратов натурального числа $q > 2$ найдется натуральное число $a < q$, взаимно простое с q , такое, что неполные частные в разложении числа a/q ограничены числом $C \log q / \log \log q$. В той же работе авторы получили аналогичный результат и для некоторых других классов чисел q .

Список литературы

- [Shk2] T. Schaien, I.D. Shkredov, "*Roth's theorem in many variables*", Israel J. Math, 2014, v. 199, i. 1, 287–308.
- [Shk3] I.D. Shkredov, T. Schaien, "*On sumsets of convex sets*", Comb. Prob. Comput., 2011, v. 20, 793–798.
- [Shk4] O.Roche–Newton, M. Rudnev, and I.D. Shkredov, "*New sum–product type estimates over finite fields*", Adv. Math, 2016, v. 203, 589–605.
- [Shk5] N. G. Moschevitin, B. Murphy, and I.D. Shkredov, "*On Korobov bound concerning Zaremba's conjecture*", arXiv:2212.14646v1.