2006 г. ноябрь — декабрь *т. 61, вып. 6 (372)*
УСПЕХИ МАТЕМАТИЧЕСКИХ НАУК

УДК 511.218+511.336

Теорема Семереди и задачи об арифметических прогрессиях

И. Д. Шкредов

Знаменитая теорема Семереди об арифметических прогрессиях утверждает, что любое подмножество целых чисел положительной асимптотической плотности содержит арифметические прогрессии любой длины. Из этой замечательной теоремы выросла новая большая область комбинаторной теории чисел. Обсуждению этой тематики и посвящен настоящий обзор.

Библиография: 132 названия.

Содержание

§ 1. Введение

Пусть k и d – натуральные числа. Арифметической прогрессией длины k с разностью d называется множество $n, n+d, n+2d, \dots, n+(k-1)d$, где n – целое число. В 1927 году Б. Л. Ван дер Варден доказал свою знаменитую теорему об арифметических прогрессиях (см. [1]), которую А. Я. Хинчин назвал жемчужиной теории чисел (см. [2]).

Работа выполнена при поддержке Российского фонда фундаментальных исследований (грант № 06-01-00383), гранта Президента РФ № 1726.2006.1 и INTAS (грант № 03-51-5070).

Теорема 1 (Ван дер Варден). *Пусть h и k – натуральные числа. Для любого разбиения целых чисел на h подмножеств $C_1, \dots, C_h$ одно из подмножеств содержит арифметическую прогрессию длины k.*

Несмотря на кажущуюся простоту и естественность теорема Ван дер Вардена сыграла значительную роль в развитии двух разделов математики – аддитивной комбинаторики и комбинаторной эргодической теории. В нашем обзоре еще пойдет речь об этих разделах, отметим сейчас лишь только то, что обе указанные области математики связаны между собой теснейшим образом и находятся на стыке таких наук, как аддитивная и аналитическая теория чисел, теория графов и теория динамических систем. Сама по себе теорема Ван дер Вардена является одним из фундаментальных результатов теории Рамсея (см. [3], [4]). Действительно, если в теореме 1 разбиение множества целых чисел на h подмножеств $C_1, \dots, C_h$ трактовать как раскраску $\mathbb{Z}$ в h различных цветов, то теорема Ван дер Вардена утверждает, что в множестве целых чисел найдется *монохроматическая* арифметическая прогрессия, т.е. прогрессия, все элементы которой раскрашены в один и тот же цвет.

Настоящий обзор посвящен обсуждению всего многообразия результатов, так или иначе связанных с теоремой Ван дер Вардена и ее обобщениями.

Прежде чем обсуждать эти обобщения, переформулируем теорему 1.

Теорема 2. *Пусть h и k – натуральные числа. Существует такое число $N(h,k)$, что для любого натурального $N \geqslant N(h,k)$ и любого разбиения множества $1, \dots, N$ на h подмножеств одно из подмножеств содержит арифметическую прогрессию длины k.*

В теореме 2, в отличие от теоремы 1, все множества конечны. По этой причине теорему 2 называют *конечной* версией теоремы 1. Легко показать, что эти результаты эквивалентны (см. ниже).

Пожалуй, самый простой вопрос, который может возникнуть в связи с теоремой Ван дер Вардена, это вопрос о том, как быстро стремится к бесконечности величина $N(h,k)$. К сожалению, оригинальное доказательство Ван дер Вардена дает очень слабые оценки на $N(h,k)$, даже когда $h = 2$. Сформулируем имеющийся здесь результат более точно.

Мы определим последовательность функций (иерархия Аккермана), $f_i \colon \mathbb{N} \to \mathbb{N}$. Пусть $f_1(n) = n+1$ и для всех $i \geqslant 2$ выполнено $f_{i+1}(n) = (\underbrace{f_i \circ \dots \circ f_i}_{n})(1)$. Тогда, например $f_2(n) = 2n$, $f_3(n) = 2^n$, а $f_4(n)$ – башня из n двоек. *Функцией Аккермана* называется функция $A(n) = f_n(n)$, $n \in \mathbb{N}$. Ясно, что $A(n)$ стремится к бесконечности быстрее любой фиксированной функции $f_i(n)$. Кроме того, функция $A(n)$ не является примитивно-рекурсивной (грубо говоря, $A(n)$ не может быть выражена через конечное число композиций обычных функциональных операций, более подробно см. [5]). Из оригинального доказательства теоремы Ван дер Вардена вытекает оценка величины $N(2,k)$ вида $N(2,k) \leqslant A(k)$ для всех $k \geqslant 2$.

В 1987 году С. Шелах, получил первую примитивно-рекурсивную оценку для $N(2,k)$ (см. [6]). Пусть $S(1) = 2$ и для всех $n \geqslant 2$ выполнено $S(n) = f_4(S(n-1))$. Тогда при $k \geqslant 2$ справедливо неравенство $N(2,k) \leqslant S(Ck)$, где C – некоторая абсолютная константа.

Другое обобщение, связанное с теоремой 1, было высказано в 1936 году П. Эрдёшем и П. Тураном.

Пусть A – произвольное подмножество целых чисел. *Верхней плотностью Банаха* (или просто *верхней плотностью*) множества A называется величина

$$D^*(A) = \limsup_{N\to\infty} \frac{|A \cap [1, 2, \dots, N]|}{N}.$$

Эрдёш и Туран предположили, что любое множество целых чисел положительной верхней плотности содержит арифметическую прогрессию любой длины. Ясно, что из этой гипотезы вытекает теорема Ван дер Вардена. Действительно, верхняя плотность Банаха обладает полуаддитивным свойством

$$D^*\Big(\bigcup_{i=1}^{m} A_i\Big) \leqslant \sum_{i=1}^{m} D^*(A_i),$$

где $A_i \subseteq \mathbb{Z}$, $i = 1, \dots, m$, – произвольные множества. Следовательно, если $\mathbb{Z}$ разбито на h подмножеств, то одно из этих подмножеств имеет верхнюю плотность не меньшую, чем $1/h > 0$. Сформулируем гипотезу Эрдёша и Турана более точно.

Гипотеза 1 (Эрдёш, Туран). *Пусть $A \subseteq \mathbb{Z}$ – произвольное множество. Пусть также $D^*(A) > 0$. Тогда для любого натурального $k \geqslant 3$ множество A содержит арифметическую прогрессию длины k.*

Из гипотезы 1 вытекает, что любое множество положительной плотности содержит бесконечно много арифметических прогрессий длины k.

Гипотеза Эрдёша и Турана имеет еще одну, эквивалентную, формулировку. Обозначим, для удобства, множество $\{1, 2, \dots, N\}$ через $[N]$.

Гипотеза 1′ (Эрдёш, Туран). *Пусть $k \geqslant 3$ – натуральное число, а $0 < \delta \leqslant 1$ – произвольное действительное число. Существует натуральное $N(k, \delta)$ такое, что для всех $N \geqslant N(k, \delta)$ произвольное множество $A \subseteq [N]$, $|A| \geqslant \delta N$, содержит арифметическую прогрессию длины k.*

Для полноты изложения мы приведем здесь доказательство эквивалентности гипотез 1 и 1′. Примерно такое же рассуждение устанавливает эквивалентность теорем 1 и 2.

Очевидно, что из гипотезы 1′ вытекает гипотеза 1. Докажем обратную импликацию. Предположим, что для некоторого натурального $k \geqslant 3$ и некоторого $\delta \in (0, 1]$ гипотеза 1′ не верна. Иными словами, для любого натурального N существует множество $A \subseteq [N]$, $|A| \geqslant \delta N$, такое, что A не содержит арифметических прогрессий длины k. Пусть $N_1 = 1$, $b_1 = 0$ и для $i \geqslant 2$ выполнено

$$N_i := b_{i-1} + N_{i-1}, \qquad b_i := b_{i-1} + N_{i-1} + N_i + 1. \tag{1}$$

Получаем такую возрастающую последовательность натуральных чисел $1 = N_1 < N_2 < N_3 < \cdots$ и такую последовательность множеств $A_1, A_2, A_3, \dots$, что для любого i выполнено $A_i \subseteq [N_i]$, $|A_i| \geqslant \delta N_i$ и ни одно A_i не содержит арифметических прогрессий длины k. Пусть $\widetilde{A}_i = A_i + b_i$. Ясно, что множества $\widetilde{A}_i$ не пересекаются и не содержат арифметических прогрессий длины k.

Пусть $A = \bigsqcup_i \widetilde{A}_i$. Применяя формулу (1), получаем, что A также не содержит арифметических прогрессий длины k. Имеем $b_i \leqslant 3N_i$ для всех $i \geqslant 1$. Далее,

$$\frac{|A \cap [b_i + N_i]|}{b_i + N_i} \geqslant \frac{|\widetilde{A}_i \cap [b_i, b_i + N_i]|}{4N_i} \geqslant \frac{\delta N_i}{4N_i} = \frac{\delta}{4}\,. \tag{2}$$

Из формулы (2) вытекает, что верхняя плотность множества A не меньше, чем $\delta/4 > 0$. Получаем противоречие с гипотезой 1.

Гипотеза Эрдёша и Турана оказалась чрезвычайно трудной. Самый простой случай $k = 3$ был доказан К. Ф. Ротом лишь в 1953 году (см. [7]). Следует сказать, что случай прогрессий длины три – особый, поскольку в этой ситуации можно применить более или менее известную технику, связанную с круговым методом.

Переформулируем гипотезу Эрдёша–Турана еще раз.

Пусть N – натуральное число. Положим

$$a_k(N) = \frac{1}{N}\max\{|A| : A \subseteq [N],\\ A \text{ не содержит арифметических прогрессий длины } k\}.$$

Сделаем одно замечание относительно функции $a_k(N)$. Пусть $k \geqslant 3$ – натуральное число, N, M – произвольные натуральные числа и A – некоторое подмножество $[N + M]$ без арифметических прогрессий длины k. Тогда множества $A_1 = A \cap [1, \dots, N]$ и $A_2 = A \cap [N + 1, \dots, N + M]$ также не содержат арифметических прогрессий длины k. Получаем очевидное неравенство $a_k(N + M)(N + M) \leqslant a_k(N)N + a_k(M)M$, из которого вытекает существование предела $\lim_{N\to\infty} a_k(N)$. Гипотеза Эрдёша–Турана означает, что для всех $k \geqslant 3$ выполнено

$$a_k(N) \to 0 \quad \text{при} \quad N \to \infty. \tag{3}$$

К. Ф. Рот доказал следующую теорему.

Теорема 3 (Рот). *Пусть N – натуральное число, $N \geqslant 3$. Тогда*

$$a_3(N) \ll \frac{1}{\log\log N}\,.$$

Таким образом, Рот получил больше, чем требовала гипотеза Эрдёша–Турана для $k = 3$. Его теорема представляет собой количественную оценку скорости стремления к нулю величины $a_3(N)$. Мы приведем доказательство теоремы 3 в § 2.

Результат Рота был затем улучшен Е. Семереди в [8] и Д. Р. Хиф-Брауном в [9]. Независимо друг от друга оба этих автора получили следующую оценку для $a_3(N)$.

Теорема 4 (Семереди, Хиф-Браун). *Пусть N – натуральное число, $N \geqslant 3$. Тогда*

$$a_3(N) \ll \frac{1}{(\log N)^c}\,,$$

где константу c можно взять равной $1/20$.

Наилучший, на сегодняшний день, результат об оценке сверху величины $a_3(N)$ принадлежит Ж. Бургейну [10] (см. также его статью [11] о подмножествах $\mathbb{R}^k$, не содержащих арифметических прогрессий).

ТЕОРЕМА 5 (Бургейн). *Пусть N – натуральное число, $N \geqslant 3$. Тогда*

$$a_3(N) \ll \sqrt{\frac{\log\log N}{\log N}}\,. \tag{4}$$

Теоремы Рота, Семереди, Хиф-Брауна и Бургейна относятся к оценке величины $a_3(N)$ (см. также интересную статью [12], в которой гипотеза Эрдёша–Турана для $k = 3$ доказывается методами теории графов). Как было отмечено выше, вопрос гипотезы 3, когда $k = 3$, гораздо более простой, чем случай $k \geqslant 4$. Если $k \geqslant 4$, то обычные аналитические методы перестают работать. Лишь в 1969 году Семереди доказал гипотезу Эрдёша–Турана для случая $k = 4$ (см. [13]), а затем, в 1975 году им было получено полное решение этой проблемы для всех $k \geqslant 4$ (см. [14]). Сформулируем этот замечательный результат.

ТЕОРЕМА 6 (Семереди). *Пусть A – произвольное подмножество натурального ряда и $D^*(A) > 0$. Тогда для любого натурального $k \geqslant 3$ множество A содержит арифметическую прогрессию длины k.*

В своем доказательстве Семереди использует трудные комбинаторные аргументы. Основу его доказательства составляет так называемая лемма регулярности, которая является, на сегодняшний день, важнейшим инструментом исследования графов. Более подробно доказательство Семереди будет обсуждаться в § 4.

Альтернативное доказательство теоремы 6 было предложено Х. Фюрстенбергом в [15] (более простое доказательство изложено в [16]). Его подход использует методы эргодической теории. Фюрстенберг показал, что теорема Семереди эквивалентна утверждению о кратной возвращаемости для почти всех точек в произвольной динамической системе.

ТЕОРЕМА 7 (Фюрстенберг). *Пусть X – некоторое множество и $\mathscr{B}$ – сигма-алгебра измеримых множеств на X и μ – конечная мера на X, $\mu(X) > 0$. Пусть также T – сохраняющее меру μ отображение X в себя и E – произвольное измеримое подмножество X, $\mu(E) > 0$. Тогда найдется натуральное $n > 0$ такое, что*

$$\mu(E \cap T^{-n}E \cap T^{-2n}E \cap \cdots \cap T^{-(k-1)n}E) > 0.$$

Теорема Фюрстенберга будет обсуждаться в § 5.

Следует отметить, что, используя свой метод, Фюрстенберг и его ученики получили множество глубоких обобщений теоремы Семереди (см., например, [17]–[21]), которые комбинаторными методами доказать пока не удалось.

Мы приведем здесь лишь один результат из статьи [19].

ТЕОРЕМА 8 (Бергельсон, Лейбман). *Пусть X – некоторое множество и $\mathscr{B}$ – сигма-алгебра измеримых множеств на X и μ – конечная мера на X,*

$\mu(X) > 0$. Пусть $k \geqslant 2$, $T_1, \dots, T_k$ – обратимые сохраняющие меру μ коммутирующие отображения X в себя и $p_1(n), \dots, p_k(n)$ – многочлены с рациональными коэффициентами, принимающие целые значения для целых значений n. Пусть также $p_i(0) = 0$, $i = 1, \dots, k$. Тогда для любого измеримого множества E с $\mu E > 0$ выполнено

$$\liminf_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \mu(T_1^{-p_1(n)} E \cap T_2^{-p_2(n)} E \cap \dots \cap T_k^{-p_k(n)} E) > 0.$$

Как показывает теорема 8, линейные функции $n, 2n, 3n, \dots, (k-1)n$ из теоремы 7 могут быть заменены на произвольные целые полиномы $p_1(n), p_2(n), \dots, p_k(n)$ с условием $p_i(0) = 0$, $i = 1, \dots, k$.

К сожалению, методы Семереди дают очень слабые верхние оценки для $a_k(N)$. Эргодический подход вообще не дает никаких оценок. Только в 2001 году В. Т. Гауэрс [22] получил первый эффективный результат о скорости стремления к нулю величины $a_k(N)$ для $k \geqslant 4$. Более слабую оценку для $a_4(N)$ см. в [23].

Теорема 9 (Гауэрс). *Для всех натуральных $N \geqslant 3$ и $k \geqslant 4$ справедливо неравенство*

$$a_k(N) \ll 1/(\log\log N)^{c_k},$$

где константа $c_k = 2^{-2^{k+9}}$.

Следствие 1. *Пусть k, N – натуральные числа, и пусть множество $[N]$ раскрашено не более чем в $(\log\log N)^{c_k}$ цветов. Тогда в $[N]$ найдется монохроматическая арифметическая прогрессия длины k.*

Хотя при доказательстве теорем Семереди, Фюрстенберга и Гауэрса используются разные методы, все они имеют много общего. В каждом из этих подходов доказательство представляет собой итеративную процедуру, а ключевая идея состоит в дихотомии между структурой и случайностью. Говоря точнее, на каждом шаге итеративной процедуры (алгоритма, доказывающего теорему) происходит проверка интересующего нас объекта X (множества или динамической системы) на обладание "случайными" свойствами. Итеративная процедура устроена так, что если X обладает случайными свойствами (например, если система X является слабо-перемешивающей динамической системой или множество X имеет "маленькие" коэффициенты Фурье), то установить наличие арифметических прогрессий в X относительно легко. Если же у X отсутствуют случайные свойства, то это означает, что у некоторой части X (подмножества или факторсистемы) есть некоторые "структурные свойства". Применяя наши рассуждения к этой части X, мы либо докажем требуемый результат, найдя в объекте X подобъект, обладающий случайными свойствами, либо будем на каждом шаге итеративной процедуры выделять все более и более "структурированный" подобъект X, так что в конце концов наличие интересующих нас конфигураций в этом подобъекте станет совершенно очевидным.

Результат Гауэрса является значительным шагом к доказательству другой знаменитой гипотезы Эрдёша и Турана об арифметических прогрессиях.

Гипотеза 2 (Эрдёш, Туран). *Пусть* $A = \{n_1 < n_2 < \cdots\}$ – *бесконечная последовательность натуральных чисел такая, что*

$$\sum_{i=1}^{\infty} \frac{1}{n_i} = \infty.$$

Тогда A *содержит арифметическую прогрессию любой длины.*

Легко показать (и это будет сделано в § 5), что гипотеза 2 эквивалентна тому, что для всех натуральных $k \geqslant 3$ ряд $\sum_{l=1}^{\infty} a_k(4^l)$ сходится. Следовательно, для доказательства гипотезы 2 достаточно для всех $k \geqslant 3$ и для некоторого $\varepsilon > 0$ получить оценку $a_k(N) \ll 1/(\log N)^{1+\varepsilon}$.

Доказательство теоремы 9 содержит в себе много новых и красивых идей. Методы из работы Гауэрса развивались различными авторами (см., например, [24]–[33]). Самым ярким из полученных в этих статьях результатом является, несомненно, теорема Б. Грина и Т. Тао о прогрессиях в простых числах.

Теорема 10 (Грин, Тао). *Для всех натуральных* $k \geqslant 3$ *множество простых чисел содержит арифметическую прогрессию длины* k.

На самом деле Грин и Тао доказали еще более сильный результат.

Пусть A – произвольное подмножество множества простых чисел $\mathscr{P}$, и пусть $\pi(N)$ – число простых чисел, не превосходящих N. Верхней плотностью A относительно $\mathscr{P}$ называется величина $\limsup_{N\to\infty} |A \cap [N]|/\pi(N)$.

Теорема 11 (Грин, Тао). *Пусть* $A \subseteq \mathscr{P}$ – *произвольное множество положительной верхней плотности относительно* $\mathscr{P}$, *и пусть* $k \geqslant 3$. *Тогда* A *содержит арифметическую прогрессию длины* k.

Теорему 11 для $k = 3$ доказал Грин в [34]. Он доказал даже более сильный результат. Пусть log означает логарифм по основанию 2. Обозначим $\log_{[1]} = \log N$ и для $l \geqslant 2$ положим $\log_{[l]} N = \log(\log_{[l-1]} N)$. Таким образом, $\log_{[l]} N$ есть результат взятия логарифма от числа N l раз подряд.

Теорема 12 (Грин). *Пусть* N – *достаточно большое натуральное число и* A – *произвольное подмножество* $\mathscr{P} \cap [N]$ *такое, что*

$$|A| \gg \frac{N\sqrt{\log_{[5]} N}}{\log N\sqrt{\log_{[4]} N}}.$$

Тогда A *содержит арифметическую прогрессию длины три.*

Выведем одно простое следствие теоремы 11 (см. [24]). Как известно (см., например, [35]), множество A_1 простых чисел, дающих в остатке один по модулю четыре, имеет положительную верхнюю плотность относительно $\mathscr{P}$. Кроме того, любой элемент A_1 может быть представлен в виде суммы двух квадратов (см., например, [36; с. 82–83]). Применяя теорему 11 к множеству A_1, получаем, что найдется арифметическая прогрессия произвольной длины, все элементы которой являются суммами двух квадратов.

В заключение заметим, что из гипотезы 2 вытекают обе теоремы 10 и 11.

Опишем вкратце структуру настоящего обзора. В § 2 мы рассмотрим простейший случай $k = 3$ гипотезы 1′ и докажем теорему Рота 13. В § 3 мы приведем результаты Ф. А. Беренда, Р. Ранкина и других авторов о нижних оценках величины $a_k(N)$. Следующий § 4 посвящен теореме Семереди и простым следствиям из этой теоремы и лемме регулярности. В § 5 мы обсудим идеи, лежащие в основе доказательства результата Гауэрса для случая $k = 4$, а также свойства норм Гауэрса, которые используются при доказательстве общей теоремы 9. Так как доказательство теоремы 9 очень трудное, то в нашем изложении мы будем следовать более простой статье [23], в которой получена более слабая, чем в теореме 9, оценка величины $a_4(N)$. В § 6 мы приведем схему доказательства Фюрстенберга теоремы Семереди и дадим небольшой обзор результатов, полученных методами эргодической комбинаторной теории чисел. В следующем параграфе мы рассмотрим простейшее двумерное обобщение теоремы 6. Параграф § 8 посвящен результату Грина–Тао 10 о прогрессиях в простых числах. В § 9 обсуждаются дальнейшие обобщения теоремы Рота, а также теоремы Шура (см. [37]). Основные результаты этого раздела комбинаторной теории чисел получены К. Ф. Ротом [38], Р. Радо [39]–[41], а также П. Франклом, Р. Грэхемом и В. Рёдлом [42]. В § 10 мы приведем две теоремы Е. Крута о критических множествах без арифметических прогрессий, несколько результатов об арифметических прогрессиях в суммах и одну теорему о радугах. Наконец, в заключении обсуждаются несколько нерешенных задач, связанных с теоремой Семереди и арифметическими прогрессиями.

Мы завершим введение доказательством теоремы Ван дер Вардена (см. [43]).

Пусть k, r – натуральные числа, $k \geqslant 1$, $r \geqslant 0$. Обозначим символом $[a, r, k]$ арифметическую прогрессию $a, a + r, \dots, a + (k - 1)r$. Пусть $\mathbf{c}\colon [N] \to [m]$ – некоторая раскраска отрезка натурального ряда $1, \dots, N$ в m цветов.

Определение 1. *Веером радиуса k, степени d и с начальной точкой a* называется набор арифметических прогрессий $([a, r_1, k], \dots, [a, r_d, k])$, каждая из которых принадлежит $[N]$. Любая прогрессия вида $[a + r_i, r_i, k - 1]$, $1 \leqslant i \leqslant d$, называется *спицей* веера.

Веер $([a, r_1, k], \dots, [a, r_d, k])$ называется *полихроматическим*, если найдется $d + 1$ различных цветов $c_0, c_1, \dots, c_d$ таких, что начальная точка a окрашена в цвет c_0 и все элементы i-й спицы веера раскрашены в цвет c_i, $i = 1, \dots, d$.

Доказательство теоремы 2. Доказательство проводится индукцией по длине арифметической прогрессии k. Если $k = 1$, то теорема Ван дер Вардена, очевидно, выполняется, поэтому пусть $k \geqslant 2$. Будем считать, что для $k - 1$ теорема доказана. Иными словами, для всех натуральных m существует $N(m, k - 1)$ такое, что в любой раскраске $[N(m, k - 1)]$ найдется монохроматическая арифметическая прогрессия длины $k - 1$.

Пользуясь нашим индуктивным предположением, мы докажем утверждение, состоящее в том, что для всех $d \geqslant 0$ существует натуральное число $N_f(m, k-1, d)$ такое, что в любой раскраске $[N(m, k-1, d)]$ найдется либо монохроматическая арифметическая прогрессия длины k, либо полихроматический веер радиуса k и степени d. Назовем это утверждение N_f и будем доказывать его индукцией по d. Если $d = 0$, то утверждение N_f очевидно. Заметим, что для существования полихроматического веера степени d нужен по крайней мере

$d+1$ цвет. Следовательно, если мы докажем наше утверждение для $d=m$, то тем самым и теорема Ван дер Вардена будет доказана.

Предположим, что справедливость N_f установлена для $d-1$, $d>1$. Пусть $N=N_f(m,k-1,d):=4kN_1N_2$, где $N_1=N_f(m,k-1,d-1)$ и $N_2=N(m^dN_1^d, k-1)$. Заметим, что существование чисел N_1 и N_2 следует из наших индуктивных предположений. Пусть $\mathbf{c}$ – произвольная раскраска в m цветов множества $[N]$. Для любого b из $[N_2]$ множество $\{bkN_1+1, bkN_1+2,\dots,bkN_1+N_1\}$ является арифметической прогрессией длины N_1, принадлежащей отрезку натурального ряда $[N]$. По индуктивной гипотезе множество $\{bkN_1+1, bkN_1+2,\dots, bkN_1+N_1\}$ содержит либо монохроматическую арифметическую прогрессию длины k, либо полихроматический веер радиуса k и степени $d-1$. Если мы нашли монохроматическую прогрессию длины k, то мы доказали теорему Ван дер Вардена, поэтому будем считать, что для всех $b\in[N_2]$ найдется полихроматический веер радиуса k и степени $d-1$. Другими словами, для всякого $b\in[N_2]$ существуют $a(b),r_1(b),\dots,r_{d-1}(b)\in\{1,\dots,N_1\}$ и различные цвета $c_0(b),c_1(b),\dots,c_{d-1}(b)\in[m]$ такие, что $\mathbf{c}(bkN_1+a(b))=c_0(b)$ и для всех $j=1,\dots,k-1$, $i=1,\dots,d-1$ выполнено $\mathbf{c}(bkN_1+a(b)+jr_i(b))=c_i(b)$. Отображение $b\to(a(b),r_1(b),\dots,r_{d-1}(b),c_0(b),c_1(b),\dots,c_{d-1}(b))$ задает раскраску $[N_2]$ в $m^dN_1^d$ цветов. Можно считать, что эти цвета нумерованы числами от 1 до $m^dN_1^d$. По определению числа N_2 существует монохроматическая арифметическая прогрессия $[b,s,k-1]$ длины $k-1$, принадлежащая $[N_2]$. Пусть эта прогрессия раскрашена в цвет $(a,r_1,\dots,r_{d-1},c_0,c_1,\dots,c_{d-1})$. Без ограничения общности можно считать, что $s>0$, так как в противном случае мы можем рассмотреть вместо $[b,s,k-1]$ арифметическую прогрессию $b,b-s,\dots,b-(k-2)s$.

Пусть $b_0=(b-s)kN_1+a$. Так как $N=4kN_1N_2$, то $b\in[N]$. Рассмотрим веер радиуса k, степени d и с начальной точкой b_0

$$([b_0,skN_1,k],[b_0,skN_1+r_1,k],\dots,[b_0,skN_1+r_{d-1},k]). \tag{5}$$

Докажем, что веер (5) полихроматический. Рассмотрим первую спицу веера. Для всех $j=1,\dots,k-1$ выполнено

$$\mathbf{c}(b_0+jskN_1)=\mathbf{c}((b+(j-1)s)kN_1+a)=c_0(b+(j-1)s)=c_0.$$

Следовательно, первая спица веера является монохроматической. Остальные спицы веера также монохроматические. Действительно, для всех $j=1,\dots,k-1$, $t=1,\dots,d-1$ выполнено

$$\mathbf{c}(b_0+j(skN_1+r_t))=\mathbf{c}((b+(j-1)s)kN_1+a+jr_t)=c_t(b+(j-1)s)=c_t.$$

Если некоторая спица веера раскрашена в тот же цвет, что и начальная точка b_0, то мы нашли монохроматическую арифметическую прогрессию длины k. Если же цвет b_0 не совпадает с цветом ни одной спицы веера, то мы получили полихроматический веер радиуса k и степени d. Иными словами, мы доказали утверждение N_f, а вместе с ним и теорему Ван дер Вардена.

§ 2. Теорема Рота

В настоящем параграфе мы докажем теорему Рота 3. Сформулируем эту замечательную теорему еще раз.

Теорема 13 (Рот). *Пусть $\delta > 0$ – действительное число и N – натуральное число, $N \gg \exp\exp(\delta^{-1})$. Пусть также A – произвольное подмножество $[N]$, $|A| = \delta N$. Тогда A содержит арифметическую прогрессию длины три.*

Прежде чем доказывать теорему 13, мы дадим несколько определений, а после этого приведем схему доказательства.

Пусть комплексная функция f определена на множестве целых чисел. Пусть также E – произвольное подмножество $\mathbb{Z}$. Будем писать $f\colon E \to \mathbb{C}$, если вне E функция f равна нулю.

Пусть функция f принимает конечное число ненулевых значений. Преобразование Фурье функции f задается формулой

$$\widehat{f}(x) = \sum_n f(n) e^{-2\pi i n x}, \qquad x \in \mathbb{S}^1. \tag{6}$$

(Числа $\widehat{f}(x)$ называются также коэффициентами Фурье функции f.) Будем писать $\int$ вместо $\int_0^1$ и $\sum_n$ вместо $\sum_{n\in\mathbb{Z}}$. Справедливы формулы

$$\int |\widehat{f}(x)|^2\, dx = \sum_n |f(n)|^2, \tag{7}$$

$$\int \widehat{f}(x)\overline{\widehat{g}(x)}\, dx = \sum_n f(n)\overline{g(n)}. \tag{8}$$

Определение 2. Пусть $\alpha \in (0,1)$ – действительное число, N – натуральное число. Функция $f\colon [N] \to \mathbb{C}$ называется *α-равномерной*, если

$$\|\widehat{f}\|_\infty \leqslant \alpha N. \tag{9}$$

Пусть $A \subseteq [N]$. Обозначим через $\chi_{[N]}$ характеристическую функцию множества $[N]$. Функция $f = A - \delta\chi_{[N]}$ называется *балансовой* функцией A. Множество A называется *α-равномерным*, если его балансовая функция α-равномерна. Заметим, что $\sum_n f(n) = 0$.

Простейшими примерами α-равномерных множеств являются так называемые случайные множества. Остановимся на этих множествах чуть подробнее. Пусть $\delta > 0$ – произвольное число. Пусть Ω – пространство последовательностей длины N, состоящих из нулей и единиц, а $\mathscr{F}$ – сигма-алгебра всех подмножеств Ω. Если последовательность $\omega \in \Omega$ имеет k единиц и $N-k$ нулей, то припишем этой последовательности вероятность $\delta^k(1-\delta)^{N-k}$. Мы задали вероятностное пространство $(\Omega, \mathscr{F}, \mathsf{P})$. Каждой точке $\omega = (\omega_1, \dots, \omega_N)$ множества Ω сопоставим множество $A(\omega) = \{i : \omega_i = 1\}$. Случайные множества – это множества $A(\omega)$ для "типичных" последовательностей ω. Например, легко показать, что математическое ожидание мощности множества $A(\omega)$ равно δN. Исходя из этого факта говорят, что мощность случайного множества в заданной выше вероятностной модели равна δN. Аналогично, можно найти математическое ожидание числа арифметических прогрессий в случайном множестве. Оно оказывается по порядку равным величине $\delta^3 N^2$. Пользуясь

оценками больших уклонений для последовательности независимых одинаково распределенных случайных величин, можно также показать, что все ненулевые коэффициенты Фурье случайного множества не превосходят $N^{1/2+\varepsilon}$, где $\varepsilon > 0$ (более подробно см., например, [44]). Следовательно, случайные множества представляют собой пример α-равномерных множеств, когда $\alpha > N^{-1/2+\varepsilon}$. Можно сказать, что в некотором смысле "почти все" подмножества $[N]$ мощности δN являются α-равномерными. Тем не менее легко привести примеры множеств из $[N]$ мощности δN, не являющихся α-равномерными. Например, можно взять любую арифметическую прогрессию в $[N]$ длины δN.

Обсудим основные идеи, лежащие в доказательстве теоремы Рота. Предположим, что множество $A \subseteq [N]$, $|A| = \delta N$, не содержит арифметических прогрессий длины три. Доказательство теоремы Рота представляет собой алгоритм. На первом шаге этого алгоритма возможны две ситуации: либо множество A является α-равномерным с некоторым α, зависящим только от δ (в доказательстве берется $\alpha = 2^{-5}\delta^2$), либо не является.

Если множество A есть α-равномерное множество, то легко показать, что A содержит очень много арифметических прогрессий длины три. Более точно, количество арифметических прогрессий длины три в множестве A равно, по порядку, $\delta^3 N^2$. Заметим, что случайные множества содержат как раз это число арифметических прогрессий. В A также есть так называемые тривиальные, или вырожденные, прогрессии, т.е. прогрессии с нулевой разностью. Ясно, что число таких прогрессий не больше, чем мощность множества A. По условию число N не меньше, чем $\exp\exp(\delta^{-1})$. Отсюда делается вывод, что если A является α-равномерным, то число арифметических прогрессий в множестве A больше, чем $|A| = \delta N$. Следовательно, A содержит по крайней мере одну не тривиальную прогрессию (на самом деле таких прогрессий в A будет много). Получаем противоречие с предположением об отсутствии в A арифметических прогрессий длины три.

Пусть теперь множество A не является α-равномерным. Можно показать, что α-равномерность множества A эквивалентна равномерной распределенности A в длинных арифметических прогрессиях. Говоря точнее, мощность пересечения α-равномерного множества A мощности δN с любой достаточно длинной прогрессией P примерно равна $\delta|P|$. Точный смысл слов "достаточно длинный" будет ясен из доказательства теоремы Рота. Следовательно, если множество A не является α-равномерным, то найдется прогрессия P такая, что $|A \cap P| = (\delta + \theta)|P|$, где $|\theta| > 0$. Более аккуратные рассуждения позволяют доказать, что прогрессию P можно выбрать так, чтобы величина θ была положительна и выражалась явным образом в терминах плотности δ.

После этого мы рассматриваем новое множество $A' = A \cap P$ и применяем к нему наш алгоритм. Заметим, что так как $A' \subseteq A$, то множество A' не содержит арифметических прогрессий длины три. Кроме того, плотность A' в P не меньше, чем $\delta + \theta$, где $\theta > 0$. Следовательно, на каждом шаге алгоритма плотность получающихся множеств увеличивается на положительную величину. С другой стороны, плотность всегда не превосходит единицы. Это означает, что через конечное число шагов наш алгоритм остановится. Следовательно, на каком-то шаге алгоритма мы получим арифметическую прогрессию $\widetilde{P}$ и α-равномерное множество $\widetilde{A}$, принадлежащее$A \cap \widetilde{P}$. Как было сказано выше,

в этом случае множество $\widetilde{A}$ содержит арифметическую прогрессию длины три. Значит, множество A также содержит арифметическую прогрессию. Опять получаем противоречие с предположением об отсутствии в A арифметических прогрессий длины три.

Мы привели схему доказательства теоремы Рота. Приступим к самому доказательству.

Предложение 1. *Пусть δ – действительное число, M – натуральное число, P – арифметическая прогрессия длины M и A – некоторое подмножество P, $|A| = \delta M$, без арифметических прогрессий длины три. Пусть также*

$$M \geqslant 2^{25}\pi^2\delta^{-4}. \tag{10}$$

Тогда существует прогрессия $P' \subseteq P$ такая, что

1) $|A \cap P'| \geqslant (\delta + 2^{-9}\delta^2)|P'|$,
2) $|P'| \geqslant 2^{-15}\delta^2\sqrt{M}$.

Покажем, как из предложения 1 вытекает теорема Рота.

Как было сказано выше, доказательство теоремы Рота представляет собой алгоритм. Проведем первый шаг этого алгоритма. Предположим, что множество $A \subseteq [N]$ не содержит арифметических прогрессий длины три. Пусть $P_0 = [N]$, $A_0 = A$, $\delta_0 = \delta$. Имеем $N \geqslant 2^{25}\pi^2\delta^{-4}$. Применяя предложение 1, получаем прогрессию $P_1 \subseteq [N]$, для которой выполнено $|A_0 \cap P_1| \geqslant (\delta_0 + 2^{-9}\delta_0^2)|P_1|$ и $|P_1| \geqslant 2^{-15}\delta_0^2\sqrt{|P_0|}$. После этого положим $A_1 = A_0 \cap P_1$.

Пусть на i-м шаге алгоритма, $i \geqslant 1$, мы построили прогрессию P_i и множество $A_i \subseteq P_i$ без арифметических прогрессий длины три такие, что

$$|A_{i-1} \cap P_i| \geqslant (\delta_{i-1} + 2^{-9}\delta_{i-1}^2)|P_i|, \qquad |P_i| \geqslant 2^{-15}\delta_{i-1}^2\sqrt{|P_{i-1}|}\,. \tag{11}$$

Заметим, что на каждом шаге алгоритма плотность множеств A_i в прогрессиях P_i увеличивается на величину $2^{-9}\delta_{i-1}^2$. На первом шаге алгоритма плотность A_0 в P_0 равна δ. Если

$$N_i := |P_i| \geqslant 2^{25}\pi^2\delta^{-4} \geqslant 2^{25}\pi^2\delta_i^{-4}, \tag{12}$$

то мы можем провести $(i+1)$-й шаг алгоритма.

Оценим максимальное число шагов алгоритма. Пусть $\varepsilon(t) = 2^{-9}t^2$. Пусть также $k_1 = \lceil \delta_0/\varepsilon(\delta_0)\rceil$, $k_2 = \lceil \delta_{k_1}/\varepsilon(\delta_{k_1})\rceil, \dots, k_s = \lceil \delta_{k_{s-1}}/\varepsilon(\delta_{k_{s-1}})\rceil, \dots$. Применяя первое неравенство (11), получаем $\delta_{k_1} \geqslant 2\delta$, $\delta_{k_2} \geqslant 2^2\delta, \dots, \delta_{k_s} \geqslant 2^s\delta, \dots$. Отсюда следует, что не более чем через

$$k_1 + k_2 + \dots < 200\left(\frac{1}{\delta} + \frac{1}{2\delta} + \frac{1}{2^2\delta} + \dots\right) = \frac{400}{\delta} = K$$

шагов плотность δ_K станет больше 1. Полученное противоречие еще не доказывает теорему Рота, поскольку мы не проверили выполнение условия (12) на каждом шаге нашего алгоритма. Имеем $N \gg \exp\exp(\delta^{-1})$. Применяя второе неравенство (11), получаем

$$N_K \geqslant (2^{-15}\delta_K^2)^K N^{1/2^K} \geqslant (2^{-15}\delta^2)^K N^{1/2^K} = 2^{-6000/\delta}\delta^{800/\delta}N^{1/2^K} \geqslant 2^{25}\pi^2\delta^{-4}.$$

Так как $N_i \geqslant N_K$ для всех $i \leqslant K$, то неравенство (12) выполняется на каждом шаге алгоритма. Теорема 13 доказана.

Доказательство предложения 1. Пусть $P = \{b, b+d, \dots, b+(|P|-1)d\}$. Без ограничения общности можно считать, что $b = d = 1$. Действительно, в противном случае рассмотрим прогрессию $\widetilde{P} = \{n : n = (p-b)/d,\ p \in P\}$ и множество $\widetilde{A} = \{n : n = (a-b)/d,\ a \in A\}$. Тогда $\widetilde{A} \subseteq \widetilde{P}$ и $\widetilde{A}$ не содержит арифметических прогрессий длины три.

Итак, пусть $P = \{1, \dots, M\}$.

Случай 1. *Множество A является α-равномерным.* Предположим, что A является α-равномерным подмножеством P, $\alpha = 2^{-5}\delta^2$. Количество арифметических прогрессий в A равно

$$\sigma = \int \widehat{A}^2(x)\widehat{A}(-2x)\,dx. \tag{13}$$

Имеем

$$\begin{aligned}\sigma &= \delta^3 \int \widehat{P}^2(x)\widehat{P}(-2x)\,dx + \delta^2 \int \widehat{P}^2(x)(\widehat{A} - \delta\widehat{P})(-2x)\,dx \\ &\quad + \delta \int \widehat{P}(x)(\widehat{A} - \delta\widehat{P})(x)\widehat{A}(-2x)\,dx + \int (\widehat{A} - \delta\widehat{P})(x)\widehat{A}(x)\widehat{A}(-2x)\,dx \\ &= \sigma^* + \sigma_1 + \sigma_2 + \sigma_3\,. \end{aligned} \tag{14}$$

Каждое слагаемое σ_1, σ_2, σ_3 не превосходит по модулю величины $\alpha\delta M^2$. Оценим, например, σ_3. Пользуясь α-равномерностью множества A, равенством (7) и неравенством Коши–Буняковского, находим

$$\begin{aligned}|\sigma_3| &\leqslant \|\widehat{A} - \delta\widehat{P}\|_\infty \int |\widehat{A}(x)|\,|\widehat{A}(-2x)|\,dx \\ &\leqslant \alpha M \left(\int |\widehat{A}(x)|^2\,dx\right)^{1/2} \left(\int |\widehat{A}(-2x)|^2\,dx\right)^{1/2} = \alpha\delta M^2.\end{aligned}$$

Аналогично оцениваются σ_1, σ_2. Отсюда

$$\sigma = \delta^3 \int \widehat{P}^2(x)\widehat{P}(-2x)\,dx + 3\alpha\delta M^2\theta_1, \tag{15}$$

где $|\theta_1| \leqslant 1$. Величина $\displaystyle\int \widehat{P}^2(x)\widehat{P}(-2x)\,dx$ есть число арифметических прогрессий в $[M]$. Это число равно $(M-2)+(M-4)+\dots+(M-\lfloor M/2\rfloor) \geqslant M^2/8$. Так как $\alpha = 2^{-5}\delta^2$, то $\sigma \geqslant \delta^3 M^2/8 - 3\delta^3 M^2/32 = \delta^3 M^2/32$. Количество тривиальных арифметических прогрессий в A равно δM. По условию $M \geqslant 2^{25}\pi^2\delta^{-4}$. Отсюда $\delta^3 M^2/32 > \delta M$. Последнее неравенство означает, что множество A содержит нетривиальную арифметическую прогрессию длины три. Противоречие с условием предложения 1.

Случай 2. *Множество A не является α-равномерным.* Пусть теперь A не является α-равномерным подмножеством P с $\alpha = 2^{-5}\delta^2$. Пусть f – балансовая функция множества A. Так как A не α-равномерно, то найдется $x_0 \in \mathbb{S}^1$ такое, что $|\widehat{f}(x_0)| \geqslant \alpha M$. Пусть $M_1 = \sqrt{M}$. По теореме Дирихле существует натуральное $q \leqslant M_1$ такое, что $\|qx_0\| \leqslant 1/M_1$, где $\|\cdot\|$ означает расстояние до ближайшего целого. Другими словами, $x_0 = p/q + \theta/(qM_1)$, где $|\theta| \leqslant 1$. Пусть

$P_j = \{n \in [M] \mid n \equiv j \pmod q\}$, $j = 1, \dots, q$. Имеем $|P_j| = \lfloor (M-j)/q \rfloor + 1$ и $P_j = j + kq$, $k = 0, 1, \dots, \lfloor (M-j)/q \rfloor$. Пусть $\widetilde{P}_j = 0, 1, \dots, \lfloor (M-j)/q \rfloor$.

Пусть $t = \lceil (\pi 2^5)/(\alpha M_1) \cdot M/q \rceil > 1$. Имеем $t < M/q$. Несложно показать, что всякая прогрессия $\widetilde{P}_j$ может быть разбита на t прогрессий $\widetilde{P}_j^l$, длины которых отличаются не более чем на 1. Имеем

$$\begin{aligned}
\alpha M \leqslant |\widehat{f}(x_0)| &= \left| \sum_n f(n) e^{-2\pi i n x_0} \right| \\
&= \left| \sum_{j=1}^{q} \sum_{l=1}^{t} \sum_{k \in \widetilde{P}_j^l} f(j+kq) e^{-2\pi i (j+kq)\left(\frac{p}{q} + \frac{\theta}{qM_1}\right)} \right| \\
&= \left| \sum_{j=1}^{q} e^{-2\pi i j \left(\frac{p}{q} + \frac{\theta}{qM_1}\right)} \sum_{l=1}^{t} \sum_{k \in \widetilde{P}_j^l} f(j+kq) e^{-2\pi i \frac{k\theta}{M_1}} \right| \\
&\leqslant \sum_{j=1}^{q} \sum_{l=1}^{t} \left| \sum_{k \in \widetilde{P}_j^l} f(j+kq) e^{-2\pi i \frac{k\theta}{M_1}} \right|. \qquad (16)
\end{aligned}$$

Пусть $\widetilde{P}_j^l = [c, c+1, \dots, c+r]$, $r = |\widetilde{P}_j^l|$. Тогда

$$\sum_{k \in \widetilde{P}_j^l} f(j+kq) e^{-2\pi i \frac{k\theta}{M_1}} = e^{-2\pi i \frac{c\theta}{M_1}} \left(\sum_{k \in \widetilde{P}_j^l} f(j+kq) + 2\pi\theta' \frac{r^2}{M_1} \right). \qquad (17)$$

Так как длины прогрессий $\widetilde{P}_j^l$ отличаются не более чем на 1, то для любого l выполнено $r = |\widetilde{P}_j^l| \leqslant 4M/(tq)$. Применяя последнее неравенство и (16), (17), находим

$$\sum_{j=1}^{q} \sum_{l=1}^{t} \left| \sum_{k \in \widetilde{P}_j^l} f(j+kq) \right| \geqslant \frac{\alpha M}{2}. \qquad (18)$$

Имеем

$$\sum_{j=1}^{q} \sum_{l=1}^{t} \sum_{k \in \widetilde{P}_j^l} f(j+kq) = 0. \qquad (19)$$

Из неравенства (18) и равенства (19) вытекает существование такой прогрессии $\widetilde{P}_{j_0}^{l_0}$, что

$$\sum_{k \in \widetilde{P}_{j_0}^{l_0}} f(j+kq) \geqslant \frac{\alpha M}{4qt}. \qquad (20)$$

Пусть $P' = \{n : n = j + kq,\ k \in \widetilde{P}_{j_0}^{l_0}\}$. Имеем $|P'| = |\widetilde{P}_{j_0}^{l_0}| \geqslant M/(4qt)$. Так как $t = \lceil \pi 2^5/(\alpha M_1) \cdot M/q \rceil$, то $|P'| \geqslant 2^{-10} \alpha M_1 = 2^{-15} \delta^2 \sqrt{M}$ и пункт 1) предложения 1 выполнен. Докажем теперь пункт 2). Применяя неравенство (20), получаем

$$2^{-9} \delta^2 |P'| = \frac{\alpha |P'|}{16} \leqslant \frac{\alpha M}{4qt} \leqslant \sum_{n \in P'} f(n) = |A \cap P'| - \delta |P'|. \qquad (21)$$

Предложение 1 доказано.

Недавно в работе [25] Б. Грин несколько усилил теорему Рота. Он доказал, что любое достаточно плотное подмножество $[N]$ содержит арифметическую прогрессию длины три, разность которой представляется в виде x^2+y^2, где x, y – некоторые натуральные числа.

ТЕОРЕМА 14 (Грин). *Пусть N – натуральное число. Существует положительная эффективная константа $c>0$ такая, что всякое множество $A\subseteq[N]$, $|A|\gg N/(\log\log N)^c$, содержит арифметическую прогрессию длины три, разность которой представима в виде x^2+y^2.*

§ 3. Нижние оценки величины $a_k(N)$

В предыдущем параграфе мы доказали теорему Рота о верхней оценке величины $a_3(N)$. Сейчас мы приведем несколько результатов о *нижних* границах для $a_k(N)$, $k\geqslant 3$ – натуральное.

В 1946 году Ф. А. Беренд в статье [45], развивая метод из работ Р. Салема и Д. Спенсера [46], [47], получил следующую нижнюю оценку величины $a_3(N)$ (см. также [48]).

ТЕОРЕМА 15 (Беренд). *Пусть $\varepsilon>0$ – любое действительное число. Тогда существует $N_\varepsilon\in\mathbb{N}$ такое, что для любого натурального N, $N\geqslant N_\varepsilon$, выполнено*

$$a_3(N)\geqslant \exp\bigl(-(1+\varepsilon)C\sqrt{\ln N}\,\bigr),$$

где C – некоторая положительная абсолютная константа.

ДОКАЗАТЕЛЬСТВО. Пусть N_ε – натуральное число такое, что для всех $N\geqslant N_\varepsilon$, $N\in\mathbb{N}$, выполнено $\ln(4\ln N)/\sqrt{\ln N}<\varepsilon$. Пусть также m и n – натуральные параметры, и пусть $\Lambda=\{0,1,\dots,m-1\}^n$. Рассмотрим n-мерную сферу $S_t=\{\mathbf{x}\in\Lambda : x_1^2+\dots+x_n^2=t\}$, где $0\leqslant t\leqslant n(m-1)^2$. Ясно, что любая сфера S_t не содержит арифметических прогрессий длины три, в том смысле, что равенство $\mathbf{x}+\mathbf{y}=2\mathbf{z}$ для $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}\in S_t$ возможно, только если $\mathbf{x}=\mathbf{y}=\mathbf{z}$.

Заметим, что число всех сфер не превосходит nm^2. Так как любая точка множества Λ принадлежит некоторой сфере, то по принципу Дирихле существует такое $t_0\in\mathbb{N}$, что мощность S_{t_0} не меньше, чем $m^n/(nm^2)=m^{n-2}/n$.

Итак, мы нашли достаточно плотное множество S_{t_0} из Λ, не содержащее арифметических прогрессий длины три. Построим по S_{t_0} множество $A\subseteq\mathbb{N}$, также не содержащее арифметических прогрессий. Для этого рассмотрим отображение $\varphi\colon\Lambda\to\mathbb{Z}$, задаваемое формулой $\varphi(\mathbf{x})=\sum_{i=1}^n x_i(2m)^{i-1}$. Пусть $A=\varphi(S_{t_0})$. Так как равенство $\varphi(\mathbf{x})+\varphi(\mathbf{y})=2\varphi(\mathbf{z})$ выполнено тогда и только тогда, когда $\mathbf{x}+\mathbf{y}=2\mathbf{z}$, то множество A не содержит арифметических прогрессий длины три. Заметим, что при этом множество A лежит в отрезке натурального ряда $\{1,2,\dots,(2m)^n\}$.

Выберем параметры m и n. Пусть $n=\lceil\sqrt{2\log N}\,\rceil$, а m удовлетворяет условиям $(2(m-1))^n\leqslant N<(2m)^n$. Имеем

$$\begin{aligned}|A|=|S_{t_0}|&\geqslant\frac{m^{n-2}}{n}\geqslant N\frac{N^{-2/n}}{2^n n}\geqslant N\exp\left(-\left(2\sqrt{2\ln 2}+\frac{\ln(4\ln N)}{\sqrt{\ln N}}\right)\sqrt{\ln N}\right)\\&\geqslant N\exp\bigl(-\bigl(2\sqrt{2\ln 2}+\varepsilon\bigr)\sqrt{\ln N}\bigr).\end{aligned}\tag{22}$$

Так как $a_3(N) \geqslant |A|/N$, то мы получили утверждение теоремы 15.

Несмотря на свою простоту, результат Ф. А. Беренда, полученный им в 1946 году, на сегодняшний день остается наилучшим.

Р. Ранкин в [49] обобщил теорему Беренда на случай всех $k \geqslant 3$.

Теорема 16 (Ранкин). *Пусть $\varepsilon > 0$ – любое действительное число и $k \geqslant 3$ – натуральное. Тогда для всех достаточно больших N выполнено*

$$a_k(N) \geqslant \exp(-(1+\varepsilon)C_k(\ln N)^{1/(k-1)}),$$

где C_k – некоторая положительная абсолютная константа, зависящая только от k.

В своей работе Ранкин, развивая основную идею теоремы 15, строит целую последовательность сфер S_t. При этом он использует асимптотическую формулу из статьи [50] для числа решений уравнения $x_1^2 + \cdots + x_n^2 = t$, $0 \leqslant x_i \leqslant m-1$, $i = 1, \ldots, n$.

Первый пример бесконечной последовательности натуральных чисел, которая не содержит арифметических прогрессий длины три, был предложен П. Эрдёшем и П. Тураном в [51] (см. также [52]). Эта последовательность состоит из чисел, в троичном разложении которых отсутствует цифра два:

$$0, 1, 3, 4, 9, 10, 12, 13, 27, \ldots . \tag{23}$$

К сожалению, эта последовательность имеет очень маленькую плотность. В отрезке натурального ряда от 1 до N содержится примерно $N^{\log 2/\log 3}$ элементов этой последовательности. Ранкин в [49] предложил способ построения бесконечного подмножества натуральных чисел, плотность которого та же, что и в теореме 16 (см. также [52]). Мы ограничимся, для простоты, случаем $k = 3$.

Предложение 2. *Пусть $\varepsilon > 0$ – любое действительное число. Тогда существует бесконечное множество $A^* \subseteq \mathbb{N}$ такое, что для всех достаточно больших M выполнено*

$$\frac{|A^* \cap [M]|}{M} \geqslant \exp\bigl(-(1+\varepsilon)C\sqrt{\ln M}\,\bigr), \tag{24}$$

где C – константа из теоремы 15.

Доказательство. Пусть N_ε то же, что и в теореме Беренда 15. Пусть также s – натуральное число такое, что $3^{s-2} < N \leqslant 3^{s-1}$. Рассмотрим непересекающиеся полуинтервалы $[2\cdot 3^{t-1}, 3^t)$, $t \geqslant s$. По теореме Беренда для любого $t \geqslant s$ существует множество A_t, принадлежащее $[2\cdot 3^{t-1}, 3^t)$, не содержащее арифметических прогрессий длины три и имеющее мощность

$$|A_t| \geqslant 3^{t-1}\exp(-(1+\varepsilon)C(\ln 3^{t-1})^{1/2})\,. \tag{25}$$

Пусть $A^* = \bigsqcup_{t=s}^{\infty} A_t$. Тогда A^* – бесконечное множество. Легко убедиться, что A^* не содержит арифметических прогрессий длины три. Пусть $M \in \mathbb{N}$ достаточно большое, $M \geqslant 3^s$. Положим $p = [\ln M/\ln 3]$. Имеем

$$\frac{|A^* \cap [M]|}{M} \geqslant \frac{|A_p|}{M} \geqslant \frac{1}{9}\exp(-(1+\varepsilon)C(\ln M)^{1/2}) \geqslant \exp(-(1+2\varepsilon)C(\ln M)^{1/2}). \tag{26}$$

Предложение 2 доказано.

§ 4. Теорема Семереди

В этом параграфе мы обсудим некоторые идеи, лежащие в доказательстве теоремы Семереди. По мнению автора сердцем доказательства является так называемая *лемма регулярности*, которая утверждает, грубо говоря, что любой граф на n вершинах и с cn^2 ребрами ($0 < c \leqslant 1$ – абсолютная константа) может быть разбит на небольшое число подграфов, обладающих "случайными" свойствами. Нет никакой возможности привести здесь доказательство леммы регулярности, ни, тем более, теоремы 6. Мы ограничимся лишь формулировкой указанной леммы и покажем, как из леммы регулярности вытекает оценка $a_3(n) = o(1)$. Таким образом, мы рассматриваем лишь простейший случай теоремы Семереди $k = 3$.

Сформулируем лемму регулярности.

Пусть $G = (V, E)$ – конечный неориентированный граф без петель и кратных ребер, и пусть $A, B \subseteq V$ – два непустых непересекающихся подмножества V. Пусть $e(A, B)$ – число ребер (a, b) графа G, где $a \in A$ и $b \in B$. *Реберной плотностью* пары (A, B) называется отношение

$$d(A, B) := \frac{e(A, B)}{|A|\,|B|}\,.$$

Определение 3. Пара (A, B) называется *ε-равномерной*, если для всех $A' \subseteq A$, $B' \subseteq B$, для которых $|A'| > \varepsilon|A|$, $|B'| > \varepsilon|B|$, выполнено

$$|d(A', B') - d(A, B)| < \varepsilon.$$

Приведем пример ε-равномерных пар. Пусть A и B – два непересекающихся множества, и пусть $0 < p \leqslant 1$. *Двудольным случайным графом* называется граф $G_p = (V, E)$, где $V = A \sqcup B$ и ребро (a, b), $a \in A$, $b \in B$, принадлежит E с вероятностью p. Таким образом в G_p нет ребер, идущих из A в A или из B в B. Ясно, что для G_p почти наверное выполнено $d(A, B) = p$ и при фиксированном $\varepsilon > 0$ пара (A, B) почти наверное является ε-равномерной.

Определение 4. Разбиение множества вершин V графа G на множества $C_0, C_1, \ldots, C_k$ называется ε-равномерным, если

1) $|C_0| < \varepsilon|V|$;
2) $|C_1| = |C_2| = \cdots = |C_k|$;
3) все, кроме, может быть, $\varepsilon\binom{k}{2}$ пар (C_i, C_j), $1 \leqslant i < j \leqslant k$, являются ε-равномерными.

Лемма 1 (лемма регулярности Семереди). *Пусть $0 < \varepsilon \leqslant 1$ – действительное число и l – натуральное число. Тогда найдутся два натуральных числа $n_0(\varepsilon, l)$ и $k_0(\varepsilon, l)$ такие, что для всякого графа G с не менее чем $n_0(\varepsilon, l)$ вершинами найдется ε-равномерное разбиение вершин G на k классов, причем $l < k < k_0(\varepsilon, l)$.*

Классы C_i называются *группами* или *кластерами*. Лемма регулярности утверждает, грубо говоря, что множество вершин всякого достаточно большого графа может быть разбито на не очень большое число кластеров C_i, $i = 1, \ldots, k$, и "исключительное" множество C_0 так, что "почти все" пары (C_i, C_j) ведут себя

как двудольные случайные графы. Число l в лемме регулярности нужно для того, чтобы мощность кластеров $|C_i|$, $i = 1, \dots, k$, была достаточно малой. Это бывает необходимым, чтобы утверждать, например, что число ребер между кластерами значительно больше, чем число ребер с началом и концом в одном и том же кластере C_i. Следует отметить, что оценки Семереди для чисел $n_0(\varepsilon, l)$ и $k_0(\varepsilon, l)$ чрезвычайно слабые (по этому поводу см. статью [53]).

Доказательство леммы регулярности может быть найдено в [14] и в [54] (см. также хороший обзор [55]).

Сделаем еще одно замечание. Пусть $\varepsilon > 0$ и число ребер в графе $G = (V, E)$ равно $\varepsilon'|V|^2$, где ε' – достаточно малое число, зависящее от ε (например, $\varepsilon' = \varepsilon^3/100$). В этом случае утверждение леммы регулярности становится тривиальным, поскольку любое разбиение множества V на k кластеров, для которого выполнено 1) и 2), будет обладать также и свойством 3). Таким образом, лемма регулярности применима лишь для достаточно плотных графов, например, для которых выполнено $|E| > c|V|^2$, где $c > 0$ – абсолютная константа. Тем не менее существуют работы, где лемма регулярности перенесена на случай графов с малым числом ребер (см., например, [56]).

Покажем, как, пользуясь леммой регулярности, получить оценку $a_3(n) = o(1)$ (см. [12]). В своем доказательстве мы следуем обзору [57].

Теорема 17 (Ружа–Семереди). *$a_3(n) = o(1)$ при $n \to \infty$.*

Доказательство. Пусть $0 < \delta \leqslant 1$ – фиксированное число и множество $A \subseteq [n]$, $|A| = \delta n$, не содержит арифметических прогрессий длины три. Пусть также X, Y, Z – три непересекающихся копии отрезка $[1, 3n]$. Рассмотрим множество S всех троек $(x, y, z) \in X \times Y \times Z$ таких, что

$$y - x = z - y = \frac{z - x}{2} \in A. \tag{27}$$

Построим по множеству A граф $G = (V, E)$. Пусть $V = X \sqcup Y \sqcup Z$, $|V| = 9n$. Пусть также пара вершин множества V соединена ребром тогда и только тогда, когда найдется тройка из S, содержащая эту пару. Ясно, что $|E| \geqslant 3|A|n$. Тройка $(x, y, z) \in X \times Y \times Z$ в графе G называется *треугольником*, если все вершины x, y, z соединены ребрами. Если тройка (x, y, z) принадлежит S, то назовем такой треугольник *простым*.

Легко видеть, что если граф G содержит треугольник, не являющийся простым, то множество A содержит арифметическую прогрессию длины три. Действительно, пусть (x, y, z) – треугольник, не являющийся простым. Пусть, например, в этом треугольнике выполнено $y - x \neq z - y$. Положим $a := y - x$, $b := z - y$. Тогда $a \in A$, $b \in B$ и $(a + b)/2 = (z - x)/2 \in A$. Следовательно, множество A содержит арифметическую прогрессию длины три.

Таким образом, для доказательства теоремы достаточно показать, что G содержит треугольник, не являющийся простым. Пусть $m = 9n = |V|$, и пусть $\beta = |E|/\binom{m}{2}$. Так как $|E| \geqslant 3|A|n = 3\delta n^2$, то β – положительное число, не зависящее от n. Пусть $\varepsilon = \beta/15$, и пусть $l = [\varepsilon^{-1}] + 1$. Применяя лемму регулярности с параметрами ε и l к графу G, получаем разбиение множества V на кластеры $C_1, \dots, C_k$ и C_0, для которых выполнены неравенства 1)–3). Имеем $|C_0| < \varepsilon|V|$. Отсюда число ребер в G с концом в C_0 не больше, чем εm^2.

Из свойств 1) и 2) вытекает неравенство $m/(2k) \leqslant |C_i| \leqslant m/k$, $i = 1, \dots, k$. Следовательно, число ребер с началом и концом в одном и том же кластере не превосходит величины $k\binom{m/k}{2}$. Кроме того, по свойству 3) существует не более $\varepsilon\binom{k}{2}$ пар (C_i, C_j), $1 \leqslant i < j \leqslant k$, не являющихся ε-равномерными. Значит, число ребер, не содержащихся в ε-равномерных парах (C_i, C_j) с $d(C_i, C_j) \geqslant \beta/6$, не больше, чем

$$\varepsilon m^2 + k\binom{m/k}{2} + \varepsilon\binom{k}{2}\left(\frac{m}{k}\right)^2 + \frac{\beta}{6}\binom{k}{2}\left(\frac{m}{k}\right)^2 < \frac{\beta}{3}\binom{m}{2}. \tag{28}$$

После удаления этих ребер мы получим граф G' и три *различных* кластера C_p, C_q и C_r, содержащихся в G', причем каждая пара этих кластеров является ε-равномерной с реберной плотностью не меньше, чем $\beta/6$.

Докажем, что в кластере C_r найдется x, содержащийся по крайней мере в $(\beta/10)^3|C_p|\,|C_q|$ треугольниках.

Так как $d(C_p, C_r), d(C_q, C_r) \geqslant \beta/6$, то найдется не менее $(1-2\varepsilon)|C_r|$ вершин x из C_r, соединенных по крайней мере с $(\beta/6-\varepsilon)|C_i|$ вершинами кластера C_i, где $i = p$ или $i = q$. Пусть N_x^i – вершины из C_i, $i = p, q$, соединенные с x. Имеем $\beta/6 - \varepsilon = \beta/10 > \varepsilon$. Из определения ε-равномерности вытекает, что найдется не менее $(\beta/10)^3|C_p|\,|C_q|$ ребер, соединяющие вершины из N_x^p и N_x^q. Ясно, что каждому такому ребру соответствует треугольник, содержащий x.

Завершая доказательство теоремы, заметим, что существует не более трех простых треугольников, имеющих две общих вершины. Следовательно, существует не более $3|C_p| = 3|C_q|$ простых треугольников, содержащих x. Кроме того, из неравенства $|C_i| \geqslant m/(2k)$, $i = 1, \dots, k$, при достаточно большом m и фиксированном k вытекает оценка

$$\left(\frac{\beta}{10}\right)^3 |C_p|\,|C_q| > 3|C_p|. \tag{29}$$

Поэтому G содержит треугольник, не являющийся простым. Значит, множество A содержит арифметическую прогрессию длины три и теорема 17 доказана.

Недавно в работах [58]–[60] были получены аналоги леммы регулярности для гиперграфов и показано, как из этих аналогов вытекает оценка $a_k(n) = o(1)$ для всех $k \geqslant 3$.

Сформулируем небольшое усиление теоремы Семереди, принадлежащее П. Варнавидесу [61].

ТЕОРЕМА 18 (Варнавидес). *Пусть $k \geqslant 3$ – натуральное число и $\delta > 0$ – вещественное число. Пусть также N – достаточно большое число, а $A \subseteq [N]$ – некоторое множество такое, что*

$$|A| \geqslant \delta N. \tag{30}$$

Тогда для некоторой положительной постоянной $c(k,\delta)>0$, зависящей только от k и δ, выполнено

$$\frac{1}{N^2}\sum_{x,r\in[N]} A(x)A(x+r)\cdots A(x+(k-1)r) \geqslant c(k,\delta). \tag{31}$$

Замечание 1. Пусть $\rho\in(0,1]$ – вещественное число. Обозначим через $N_k(\rho)$ минимальное натуральное число такое, что для всех натуральных $m\geqslant N_k(\rho)$ в произвольном множестве $T\subseteq[m]$ со свойством $|T|\geqslant \rho m$ найдется арифметическая прогрессия длины k. Как будет следовать из доказательства теоремы 18, константу $c(k,\delta)$ можно взять равной $\delta^2/(16N_k(\delta/2)^3)$.

Доказательство. Пусть $N>2N_k(\rho/2)$. Пусть также $K=N_k(\rho/2)$. Обозначим через P_d, $d\geqslant 1$, семейство арифметических прогрессий длины K и шагом d, содержащихся в $[N]$. Ясно, что для всех $d\geqslant 1$ выполнено $|P_d|\leqslant N$. Пусть $P=\bigsqcup_{d\geqslant 1}P_d$.

Прогрессия $p\in P$ называется *хорошей*, если $|A\cap p|\geqslant \delta/2\cdot K$. Пусть G – множество всех хороших прогрессий. Докажем, что $|G|\geqslant \delta^2N^2/(32K)$. Рассмотрим случай, когда

$$d<\frac{\delta N}{8K}. \tag{32}$$

Заметим, что любой $x\in[Kd,N-Kd]$ принадлежит в точности K прогрессиям из P_d. Применяя неравенство (32), находим

$$\begin{aligned}\sigma&=\sum_{p\in P_d}|A\cap p|=\sum_{x\in[N]}A(x)\sum_{p\in P_d}p(x)\geqslant\sum_{x\in[Kd,N-Kd]}A(x)\sum_{p\in P_d}p(x)\\&=K|A\cap[Kd,N-Kd]|\geqslant K(|A|-2Kd)=K(\delta N-2Kd)\geqslant 3\delta KN/4.\end{aligned}\tag{33}$$

С другой стороны,

$$3\delta KN/4\leqslant\sigma\leqslant\sum_{p\in(P_d\cap G)}|A\cap p|+\sum_{p\in(P_d\setminus G)}|A\cap p|\leqslant|P_d\cap G|K+\delta KN/2. \tag{34}$$

Следовательно, для всех $1\leqslant d<\delta N/(8K)$ справедливо неравенство $|P_d\cap G|\geqslant \delta N/4$. Отсюда $|G|\geqslant\delta^2N^2/(32K)$.

По определению для каждой прогрессии из G найдутся $x,r\in[N]$ такие, что $A(x)A(x+r)\cdots A(x+(k-1)r)>0$. К сожалению, для различных прогрессий из G числа $x,r\in[N]$ могут совпасть. Оценим число прогрессий $p\in P$, содержащих фиксированную прогрессию $x_0,x_0+r_0,\ldots,x_0+(k-1)r_0$. Ясно, что существует не более $K-2$ таких прогрессий из P_{r_0}. Кроме того, если прогрессия $p\in P_d$, $d\neq r_0$, содержит $x_0,x_0+r_0,\ldots,x_0+(k-1)r_0$, то d делит r_0. Пусть $d=r_0/t$, $t>1$. Так как прогрессия $p\in P_d$ содержит $x_0,x_0+r_0,\ldots,x_0+(k-1)r_0$, то $Kd>2r_0=2td$ и, следовательно, $t<K/2$. Поэтому число прогрессий $p\in P$, содержащих прогрессию $x_0,x_0+r_0,\ldots,x_0+(k-1)r_0$, не превосходит $K-2+(K-2)K/2\leqslant K^2/2$.

Имеем $2|G|/(K^2N^2)\geqslant\delta^2/(16K^3)$. Отсюда получаем, что константу $c(k,\delta)$ в неравенстве (31) можно взять равной $\delta^2/(16K^3)=\delta^2/(16N_k(\delta/2)^3)$. Теорема 18 доказана.

В работе [62] Э. Крут рассмотрел вопрос о количестве арифметических прогрессий по модулю N и немного усилил теорему 18.

ТЕОРЕМА 19 (Крут). *Пусть $k \geqslant 3$ – натуральное число и $\delta > 0$ – вещественное число. Пусть также N – достаточно большое число, а $A \subseteq \mathbb{Z}_N$ – некоторое множество такое, что*

$$|A| \geqslant \delta N. \tag{35}$$

Тогда для некоторой положительной постоянной $c(k,\delta) > 0$, зависящей только от k и δ, выполнено

$$\frac{1}{N^2} \sum_{x,r \in \mathbb{Z}_N} A(x)A(x+r)\cdots A(x+(k-1)r) \geqslant c(k,\delta). \tag{36}$$

При этом константу $c(k,\delta)$ можно взять равной $\delta/(16N_k(\delta/2)^2)$.

Пусть $k \geqslant 3$ – натуральное число и $\delta > 0$ – вещественное число. Пусть также N – достаточно большое натуральное число, а $A \subseteq \mathbb{Z}_N$ – некоторое множество такое, что $|A| \geqslant \delta N$. В связи с теоремами 18 и 19 возникает следующий вопрос. Сколько арифметических прогрессий длины k содержит множество A при достаточно большом N? Обозначим число арифметических прогрессий длины k в A, деленное на N^2, через $\mu_k(A)$. Применяя оценку теоремы 5 и оценки теорем 18, 19, находим, что $\mu_3(A) \geqslant \exp(C\delta^{-2}\log(1/\delta))$, где $C > 0$ – некоторая абсолютная константа. Для произвольного $k \geqslant 4$ из теорем 18, 19 и теоремы 9 вытекает, что $\mu_k(A) \gg \exp(-\exp(\delta^{-c_k}))$, $c_k > 0$ – абсолютная константа из теоремы 9. В работе [62] Крут, применяя результат Беренда [45] и Ранкина [49], получил *нижние* оценки величины $\mu_k(A)$.

ТЕОРЕМА 20 (Крут). *Пусть $k \geqslant 3$ – натуральное число и $\delta \in (0,1)$ – вещественное число. Пусть также N – достаточно большое натуральное число. Тогда существует множество $A \subseteq \mathbb{Z}_N$ такое, что $|A| \geqslant \delta N$ и количество арифметических прогрессий длины k в A не больше, чем $N^2 \exp\left(-\left(\frac{1}{2C_k}\log\frac{1}{4\delta}\right)^{k-1}\right)$, где C_k – абсолютная константа из теоремы 16.*

Иными словами, теорема 20 дает оценку величины $\mu_k(A)$ снизу: $\mu_k(A) \geqslant \exp\left(-\left(\frac{1}{2C_k}\log\frac{1}{4\delta}\right)^{k-1}\right)$.

ДОКАЗАТЕЛЬСТВО. Пусть $L_k(x) = \exp(2C_k(\log x)^{1/(k-1)})$, где C_k – абсолютная константа из теоремы 16. Найдем x из неравенств $4L_k(x) < 1/\delta \leqslant 4L_k(x+1)$. Пусть $N > 4x$. Применим теорему 16 с $\varepsilon = 1$. По этой теореме существует множество $S \subseteq [x]$, $|S| \leqslant xL_k(x)^{-1}$, без арифметических прогрессий длины k. Пусть

$$A = \{s + 2mx : s \in S, : 0 \leqslant m \leqslant M = [N/(4x)]\}.$$

Тогда $A \subseteq [N/2] \subseteq \mathbb{Z}_N$. Заметим, что

$$\frac{|A|}{N} = \frac{|S|(M+1)}{N} > \frac{|S|}{4x} > \frac{1}{4L_k(x)} > \delta.$$

Таким образом, плотность A в $\mathbb{Z}_N$ не меньше, чем δ. Предположим, что числа $a_1,\dots,a_k \in A$ образуют арифметическую прогрессию длины k. Так как $A \subseteq [N/2]$, то числа $a_1,\dots,a_k$ составляют арифметическую прогрессию длины k в $\mathbb{Z}_N$ тогда и только тогда, когда $a_1,\dots,a_k$ образуют арифметическую прогрессию длины k в $[N]$. Из свойств множества A вытекает, что $a_i = s+2m_ix$, $i=1,\dots,k$, где $s \in S$ и $m_1,\dots,m_k$ составляют арифметическую прогрессию в $[M]$. Поэтому множество A содержит не более $|S|M^2$ арифметических прогрессий длины k. Имеем

$$|S|M^2 \leqslant \frac{xN^2}{4x^2} \leqslant \frac{N^2}{x+1} \leqslant \frac{N^2}{\exp\left(\left(\dfrac{1}{2C_k}\log\dfrac{1}{4\delta}\right)^{k-1}\right)}.$$

Теорема 20 доказана.

§ 5. Оценки Гауэрса величины $a_k(N)$

В этом параграфе мы обсудим верхние оценки величины $a_k(N)$ (см. теорему 9), полученные в работе В. Т. Гауэрса [22]. Доказательство теоремы 9 очень сложное, поэтому мы ограничимся лишь обсуждением главных идей, лежащих в основе метода Гауэрса.

В своей замечательной работе Гауэрс дал определение α-равномерных функций степени d. Мы обсудим комбинаторный смысл α-равномерных функций степени d несколько позже, а сейчас дадим строгие определения.

Пусть $d \geqslant 0$ – натуральное число и $\{0,1\}^d = \{\omega = (\omega_1,\dots,\omega_d) : \omega_j \in \{0,1\}, j=1,\dots,d\}$ – обычный d-мерный куб. Для $\omega \in \{0,1\}^d$ пусть $|\omega|$ равно $\omega_1 + \dots + \omega_d$. Если $h = (h_1,\dots,h_d) \in \mathbb{Z}_N^d$, то $\omega \cdot h := \omega_1h_1 + \dots + \omega_dh_d$. Пусть также $\mathscr{C}$ означает оператор комплексного сопряжения. Если n – натуральное число, то $\mathscr{C}^n$ означает применение оператора комплексного сопряжения n раз.

Определение 5. Пусть даны 2^d комплексных функций $(f_\omega)_{\omega\in\{0,1\}^d}$, определенных на $\mathbb{Z}_N$. *Скалярным произведением Гауэрса* функций $(f_\omega)_{\omega\in\{0,1\}^d}$ называется величина

$$\langle (f_\omega)_{\omega\in\{0,1\}^d}\rangle_{U^d} := \frac{1}{N^{d+1}} \sum_{x\in\mathbb{Z}_N,\ h\in\mathbb{Z}_N^d} \prod_{\omega\in\{0,1\}^d} \mathscr{C}^{|\omega|} f_\omega(x+\omega\cdot h). \tag{37}$$

Мы получим некоторые свойства скалярного произведения Гауэрса.

Пусть $d \geqslant 1$. Предположим вначале, что функции $(f_\omega)_{\omega\in\{0,1\}^d}$ не зависят от последней цифры ω_d, иными словами, $f_\omega = f_{\omega_1,\dots,\omega_{d-1}}$. Тогда формула (37) может быть переписана следующим образом:

$$\langle (f_\omega)_{\omega\in\{0,1\}^d}\rangle_{U^d} = \frac{1}{N^{d+1}} \sum_{x\in\mathbb{Z}_N,\ h'\in\mathbb{Z}_N^{d-1},\ h_d\in Z_N} \times \prod_{\omega'\in\{0,1\}^{d-1}} \mathscr{C}^{|\omega'|}(f_{\omega'}(x+\omega'\cdot h')\overline{f_{\omega'}(x+h_d+\omega'\cdot h')}),$$

где $\omega' = (\omega_1, \dots, \omega_{d-1})$ и $h' = (h_1, \dots, h_{d-1})$. Отсюда

$$\langle (f_\omega)_{\omega\in\{0,1\}^d}\rangle_{U^d} = \frac{1}{N^{d+1}} \sum_{h'\in\mathbb{Z}_N^{d-1}} \Bigg| \sum_{y\in\mathbb{Z}_N} \prod_{\omega'\in\{0,1\}^{d-1}} \mathscr{C}^{|\omega'|} f_{\omega'}(y+\omega'\cdot h') \Bigg|^2. \tag{38}$$

Следовательно, для $d \geqslant 1$ и любой функции $f\colon \mathbb{Z}_N \to \mathbb{C}$ скалярное произведение Гауэрса обладает свойством неотрицательности

$$\langle (f)_{\omega\in\{0,1\}^d}\rangle_{U^d} \geqslant 0. \tag{39}$$

Неравенство (39) позволяет определить *равномерную норму Гауэрса* (или просто норму Гауэрса) функции $f\colon \mathbb{Z}_N \to \mathbb{C}$ по формуле

$$\|f\|_{U^d} := \langle (f)_{\omega\in\{0,1\}^d}\rangle_{U^d}^{1/2^d} = \left(\frac{1}{N^{d+1}} \sum_{x\in\mathbb{Z}_N,\ h\in\mathbb{Z}_N^d} \prod_{\omega\in\{0,1\}^d} \mathscr{C}^{|\omega|} f_\omega(x+\omega\cdot h) \right)^{1/2^d}. \tag{40}$$

Как мы увидим в дальнейшем, формула (40) определяет норму лишь для $d \geqslant 2$. Для $d = 1$ норма Гауэрса на самом деле является полунормой.

Если функции $(f_\omega)_{\omega\in\{0,1\}^d}$ зависят от последней цифры ω_d, то сумма (37) должна быть переписана следующим образом:

$$\begin{aligned}\langle (f_\omega)_{\omega\in\{0,1\}^d}\rangle_{U^d} = \frac{1}{N^{d+1}} \sum_{h'\in\mathbb{Z}_N^{d-1}} \left(\sum_{y\in\mathbb{Z}_N} \prod_{\omega'\in\{0,1\}^{d-1}} \mathscr{C}^{|\omega'|} f_{\omega',0}(y+\omega'\cdot h') \right) \\ \times \left(\overline{\sum_{y\in\mathbb{Z}_N} \prod_{\omega'\in\{0,1\}^{d-1}} \mathscr{C}^{|\omega'|} f_{\omega',1}(y+\omega'\cdot h')} \right).\end{aligned}$$

Применяя неравенство Коши–Буняковского и формулу (38), получаем

$$|\langle (f_\omega)_{\omega\in\{0,1\}^d}\rangle_{U^d}| \leqslant \langle (f_{\omega',0})_{\omega\in\{0,1\}^d}\rangle_{U^d}^{1/2} \cdot \langle (f_{\omega',1})_{\omega\in\{0,1\}^d}\rangle_{U^d}^{1/2}.$$

Применяя теперьнеравенство Коши–Буняковского и формулу (38) для каждой цифры $\omega \in \{0,1\}^d$, находим

$$|\langle (f_\omega)_{\omega\in\{0,1\}^d}\rangle_{U^d}| \leqslant \prod_{\omega\in\{0,1\}^d} \|f_\omega\|_{U^d}. \tag{41}$$

Неравенство (41) называется неравенством *Коши–Буняковского–Гауэрса*. Пользуясь неравенством (41), полилинейностью скалярного произведения (37) и формулой бинома Ньютона, легко получаем

$$|\langle (f+g)_{\omega\in\{0,1\}^d}\rangle_{U^d}| \leqslant (\|f\|_{U^d} + \|g\|_{U^d})^{2^d}, \tag{42}$$

откуда следует неравенство треугольника для нормы Гауэрса

$$\|f+g\|_{U^d} \leqslant \|f\|_{U^d} + \|g\|_{U^d}, \qquad d \geqslant 1. \tag{43}$$

Как было сказано ранее, для $d = 1$ норма Гауэрса не является нормой. Действительно, $\|f\|_{U^1} = \frac{1}{N}\big|\sum_{x\in\mathbb{Z}_N} f(x)\big|$ и $\|f\|_{U^1}$ равна нулю для всех функций,

для которых $\sum_{x\in\mathbb{Z}_N} f(x) = 0$. Напротив, для $d \geqslant 2$ норма Гауэрса есть норма. Докажем это.

Пусть $\widehat{f}(r) = \sum_{x\in\mathbb{Z}_N} f(x)e^{-2\pi ixr/N}$ – r-й коэффициент Фурье функции f. Тогда справедлива формула обращения $f(x) = 1/N \cdot \sum_{r\in\mathbb{Z}_N} \widehat{f}(r)e^{2\pi ixr/N}$, из которой вытекает равенство

$$\|f\|_{U^2} = \left(\sum_{r\in\mathbb{Z}_N} |\widehat{f}(r)|^4\right)^{1/4}. \tag{44}$$

Отсюда получаем, что $\|f\|_{U^2} = 0$ тогда и только тогда, когда $\widehat{f} \equiv 0$ или, что то же самое, $f \equiv 0$. Итак, мы доказали, что $\|f\|_{U^2}$ – норма.

Покажем, что $\|f\|_{U^d}$ является нормой для всех $d \geqslant 2$. Пусть ν_{const} обозначает функцию, тождественно равную единице. Имеем $\|\nu_{\mathrm{const}}\|_{U^d} = 1$. Пусть $f\colon \mathbb{Z}_N \to \mathbb{C}$ – некоторая функция. Рассмотрим набор функций $(f_\omega)_{\omega\in\{0,1\}^d}$, где $f_\omega := \nu_{\mathrm{const}}$, если $\omega_d = 1$, и $f_\omega := f$, если $\omega_d = 0$. Применяя неравенство (41) к набору $(f_\omega)_{\omega\in\{0,1\}^d}$, получаем

$$\|f\|_{U^{d-1}} \leqslant \|f\|_{U^d} \tag{45}$$

для всех $d \geqslant 2$. Неравенство (45) называется *неравенством монотонности* нормы Гауэрса. Из (45) вытекает, что если для $d \geqslant 2$ выражение $\|f\|_{U^d}$ равно нулю, то норма $\|f\|_{U^2}$ функции f равна нулю и, следовательно, $f \equiv 0$.

Дальнейшие свойства норм Гауэрса могут быть найдены в недавней работе [32] (см. также [63]).

Пользуясь понятием нормы $\|\cdot\|_{U^d}$, Гауэрс дал определение α-равномерных функций степени d.

Определение 6. Пусть $d \geqslant 2$ – натуральное число и $\alpha \in [0,1]$ – вещественное число. Функция $f\colon \mathbb{Z}_N \to \mathbb{C}$ называется *α-равномерной степени d*, если

$$\|f\|_d \leqslant \alpha.$$

В § 2 мы дали другое определение α-равномерных функций (см. определение 2). Легко показать, что обычное понятие α-равномерности из § 2 совпадает с определением 6 при $d = 2$ (см. [23], [22]). Мы видим, таким образом, что подход Гауэрса значительно обобщает классическое определение 2.

Пусть $f = A - \delta$ – балансовая функция множества A. Множество A называется α-равномерным степени d, если его балансовая функция является α-равномерной степени d.

Обсудим комбинаторный смысл понятия α-равномерных множеств степени d.

Пусть $d \geqslant 0$ и $a_0, a_1, \ldots, a_d \in \mathbb{Z}_N$ – некоторые вычеты. Тогда *d-мерным кубом* называются 2^d точек из $\mathbb{Z}_N$ вида $a_0 + \varepsilon_1 a_1 + \cdots + \varepsilon_d a_d$, где $\varepsilon_i \in \{0,1\}$. Пусть $A \subseteq \mathbb{Z}_N$ – некоторое множество. A содержит d-мерный куб, если A содержит все точки этого куба. Используя неравенство Коши–Буняковского, легко показать, что любое множество $A \subseteq \mathbb{Z}_N$ мощности δN всегда содержит не менее $\delta^{2^d} N^{d+1}$ d-мерных кубов, причем равенство достигается на "случайных подмножествах" $\mathbb{Z}_N$, имеющих плотность δ. С другой стороны, справедлив следующий результат.

Теорема 21 (комбинаторный смысл α-равномерных множеств степени d). *Пусть $d \geqslant 2$ и $A \subseteq \mathbb{Z}_N$, $|A| = \delta N$, – α-равномерное множество степени d. Тогда A содержит не более $(\delta + \alpha)^{2^d} N^{d+1}$ кубов.*

Доказательство. Имеем $A = \delta + f$. Применяя неравенство треугольника для нормы Гауэрса (43), получаем $\|A\|_d \leqslant \|\delta\|_d + \|f\|_d$. Ясно, что $\|\delta\|_d = \delta$ и $N^{d+1}\|A\|_d^{2^d}$ есть число d-мерных кубов в A. Так как множество A является α-равномерным степени d, то, по определению, $\|f\|_d \leqslant \alpha$. Отсюда $\|A\|_d \leqslant \delta + \alpha$ и мы получаем требуемый результат.

Теорема 21 показывает, что при маленьких значениях параметра α α-равномерные множества степени d содержат d-мерных кубов примерно столько, сколько содержат кубов случайные множества. В этом смысле α-равномерные множества являются близкими к случайным. Более того, во многих ситуациях α-равномерные множества ведут себя как случайные множества. Так, в первой части своих рассуждений Гауэрс показал, что α-равномерные и случайные множества содержат примерно одинаковое количество арифметических прогрессий.

Теорема 22. *Пусть $k \geqslant 3$ и $A \subseteq \mathbb{Z}_N$, $|A| = \delta N$, – α-равномерное множество степени $k-1$. Тогда*

$$\sum_{r \in \mathbb{Z}_N} |(A + r) \cap (A + 2r) \cap \cdots \cap (A + kr) - \delta^k N^2| \leqslant 2^k \alpha^{1/2^{k-1}} N^k.$$

Из теоремы 22 Гауэрс выводит следствие.

Следствие 2. *Пусть $k \geqslant 3$ и $A \subseteq \mathbb{Z}_N$, $|A| = \delta N$, – α-равномерное множество степени $k-1$. Пусть также $\alpha \leqslant (\delta/2)^{2k}$ и $N \geqslant 32k^2\delta^{-k}$. Тогда множество A содержит арифметическую прогрессию длины k.*

Следствие 2 завершает первую часть доказательства Гауэрса. Так как дальнейшие рассуждения очень сложны, то мы ограничимся, для простоты, случаем $k = 4$ и будем следовать при этом более простой статье [23]. В этой статье Гауэрс доказал более слабую оценку

$$a_4(N) \ll 1/(\log\log\log N)^c, \tag{46}$$

где c – некоторая константа.

Изложим план доказательства. Пусть $A \subseteq \mathbb{Z}_N$, $|A| = \delta N$, – некоторое множество. Если множество A является α-равномерным множеством с достаточно малым α и при этом число N достаточно большое, $N \geqslant 32k^2\delta^{-k}$, то по следствию 2 множество A содержит прогрессию и мы получаем требуемый результат. Таким образом, мы можем предполагать, что исходное множество A не является α-равномерным с некоторым $\alpha = \alpha_0$. Во второй части своей работы Гауэрс доказывает, что для любого не α_0-равномерного множества найдется арифметическая прогрессия P размера не меньше N^β такая, что $|A \cap P| \geqslant (\delta + \varepsilon)|P|$, где β и ε зависят только от δ и α_0. После этого он применяет те же самые аргументы к новому множеству $A' = A \cap P$, плотность которого в P не меньше, чем $\delta + \varepsilon$. И так далее. После некоторого числа итераций мы либо найдем α_0-равномерное подмножество A, либо плотность A в некоторой прогрессии станет

достаточно близкой к единице. Если у A есть α_0-равномерное подмножество, то по следствию 2 это подмножество и, следовательно, множество A содержит арифметическую прогрессию. Если же плотность A в некоторой прогрессии больше, чем $3/4$, то существование арифметической прогрессии длины четыре в множестве A становится очевидным. Рассуждая, как при доказательстве теоремы Рота и оценивая число итераций в терминах β и ε, получаем неравенство (46).

Договоримся об обозначениях. Пусть в дальнейшем величины α_i означают параметры, зависящие от α_0 полиномиальным образом. В работе [22] все параметры α_i выражены в терминах α_0, нам же будет удобнее не выписывать их в явном виде.

Доказательство Гауэрса существенным образом опирается на замечательную теорему Г. А. Фреймана [64] (см. также [65], [66] и [67]). Пусть $D \geqslant 1$ – натуральное число и $E, F \subseteq \mathbb{Z}^D$ – некоторые множества. Суммой по Минковскому множеств $E+F$ называется множество $E+F = \{e+f : e \in E,\ f \in F\}$. Аналогичным образом определяется разность двух множеств. Если мощность $E+E$ не слишком превосходит $|E|$ (например, если для некоторой константы $C > 1$ выполнено $|E+E| \leqslant C|E|$), то множество E называется множеством с маленькой суммой. Теорема Фреймана описывает структуру всех таких множеств. Ясно, что любая арифметическая прогрессия является множеством с маленькой суммой. Легко видеть, что множество вида $P_1 + \cdots + P_s$, где P_i – арифметические прогрессии, также есть множество с маленькой суммой. Такие множества называются *d-мерными арифметическими прогрессиями*. Кроме того, любые большие подмножества $P_1 + \cdots + P_s$ будут множествами с маленькой суммой. Теорема Фреймана утверждает, что других примеров множеств с маленькой суммой не существует. Приведем точную формулировку.

Теорема 23 (Фрейман). *Пусть $C > 0$ – некоторое число, $D \geqslant 1$ и $A \subseteq \mathbb{Z}^D$ – некоторое множество. Пусть также $|A+A| \leqslant C|A|$. Тогда найдутся числа d и K, зависящие только от C и D, и d-мерная арифметическая прогрессия Q такие, что $|Q| \leqslant K|A|$ и $A \subseteq Q$.*

Для разности $A - A$ теорема Фреймана также остается верной.

Вернемся к определению 6. Как было показано в теореме 21, множество $A \subseteq \mathbb{Z}_N$, $|A| = \delta N$, является α-равномерным степени d тогда и только тогда, когда оно содержит примерно $\delta^{2^d} N^{d+1}$ d-мерных кубов. Существует другая характеризация α-равномерных множеств. Мы знаем, что если $d = 2$, то множество A является α-равномерным степени два тогда и только тогда, когда оно имеет маленькие коэффициенты Фурье. Оказывается, что A будет α-равномерным степени три тогда и только тогда, когда "почти все" множества вида $A \cap (A+k)$, $k \in \mathbb{Z}_N$, имеют маленькие (в терминах α) коэффициенты Фурье. В этом обзоре мы не можем долго останавливаться на характеризации α-равномерных множеств в терминах коэффициентов Фурье их подмножеств, а лишь укажем, что такая характеризация существует для всех степеней $d \geqslant 2$ (см. [22]). Сформулируем точный результат для случая, когда $d = 2$. Пусть $f\colon \mathbb{Z}_N \to \mathbb{Z}_N$ – некоторая функция, и пусть $k \in \mathbb{Z}_N$ – произвольный вычет. *Разностной функцией* $\Delta(f;k)\colon \mathbb{Z}_N \to \mathbb{Z}_N$ называется функция $\Delta(f;k)(s) = f(s)\overline{f(s-k)}$.

Утверждение 1. *Пусть $A \subseteq \mathbb{Z}_N$, $|A| = \delta N$, – не α_0-равномерное множество степени 3. Пусть B – множество тех k, для которых найдется $r = r(k)$ такое, что $|\Delta(f;k)\hat{}(r)| \geqslant \alpha_1 N$. Тогда $|B| \geqslant \alpha_2 N$.*

Из определения множества B вытекает, что на B корректно определена функция $\varphi\colon B \to \mathbb{Z}_N$ такая, что для всех k из B выполнено $|\Delta(f;k)\hat{}(\varphi(k))| \geqslant \alpha_1 N$. Следующее предложение показывает, что функция φ обладает некоторым свойством, похожим на линейность.

Предложение 3. *Существует не менее $\alpha_3 N^3$ четверок $(a,b,c,d) \in B^4$ таких, что $a+b=c+d$ и $\varphi(a)+\varphi(b)=\varphi(c)+\varphi(d)$.*

Рассмотрим график $\Gamma \subseteq \mathbb{Z}^2$ функции φ, т.е. множество $\Gamma = \{(b,\varphi(b)) : b \in B\}$. По предложению 3 у Γ существует не менее $\alpha_3 N^3$ четверок $(x,y,z,w) \in \Gamma$ таких, что $x+y=z+w$. Такие четверки называются *аддитивными*. Гауэрс показал, что множества, имеющие много аддитивных четверок, обладают весьма специальными свойствами.

Предложение 4. *Пусть $c_0 > 0$, и пусть $M \subseteq \mathbb{Z}^D$ – некоторое множество мощности m, имеющее не менее $c_0 m^3$ аддитивных четверок. Тогда найдутся постоянные c и C, зависящие только от c_0, и множество $M' \subseteq M$, $|M'| \geqslant cm$, такие, что $|M' - M'| \leqslant Cm$.*

Соединяя предложение 4 и теорему Фреймана 23, Гауэрс получает следующий результат.

Предложение 5. *Пусть $B \subseteq \mathbb{Z}_N$ – множество мощности βN, и пусть график функции $\varphi\colon B \to \mathbb{Z}_N$ имеет не менее $c'N^3$ аддитивных четверок. Тогда найдутся постоянные γ и η, зависящие только от β и c', арифметическая прогрессия $P \subseteq \mathbb{Z}_N$, $|P| \geqslant N^\gamma$, и числа λ и μ такие, что*

$$\sum_{k\in P} |\Delta(f;k)\hat{}(\lambda k+\mu)|^2 \geqslant \eta |P| N^2. \tag{47}$$

Мы проведем очень грубые рассуждения, поясняющие доказательство предложения 5. Применим предложение 4 к графику Γ. Тогда у Γ найдется подмножество Γ' с маленькой разностью. Из теоремы Фреймана вытекает, что найдется не очень большая d-мерная арифметическая прогрессия Q, содержащая Γ'. С другой стороны, каждая d-мерная арифметическая прогрессия может быть разбита на некоторое число прогрессий вида $Q_1 \times Q_2$, где Q_1, Q_2 являются одномерными арифметическими прогрессиями в $\mathbb{Z}$. Следовательно, существует прогрессия вида $Q_1 \times Q_2$, которая пересекает Γ' по достаточно большому множеству. Но это и означает, что на Q_1 значения функции φ очень часто совпадают со значениями некоторой *линейной* функции. Эти рассуждения позволяют получить неравенство (47). Применяя принцип Дирихле, можно показать, что прогрессии Q_1, Q_2 имеют длину не меньше, чем $|Q|^{1/d}$. Отсюда вытекает неравенство $|P| \geqslant N^\gamma$.

Затем Гауэрс доказывает следующее предложение.

Предложение 6. *Пусть выполнены условия предложения 5. Тогда найдутся многочлены второй степени $\psi_0, \psi_1, \dots, \psi_{N-1}$ такие, что*

$$\sum_s \Big| \sum_{x\in P+s} f(x) e^{2\pi i \psi_s(x)/N} \Big| \geqslant \frac{\eta |P| N}{\sqrt{2}}\,. \tag{48}$$

После этого Гауэрс применяет оценки Вейля для тригонометрических сумм от многочленов второй степени и выводит следствие предложения 6.

Предложение 7. *Пусть выполнены условия предложения 5. Тогда найдутся $\zeta > 0$, $m \leqslant |P|^\zeta$ и прогрессии P_{sj}, $s \in [N]$, $j \in [m]$, такие, что для любого $s \in [N]$ прогрессии $P_{s1}, \dots, P_{sm}$ разбивают $P + s$ и*

$$\sum_s \sum_{j=1}^m \Big| \sum_{x\in P_{sj}} f(x) \Big| \geqslant \frac{\eta |P| N}{2\sqrt{2}}\,. \tag{49}$$

Так как f – балансовая функция множества A, то $\sum_s \sum_{j=1}^m \sum_{x\in P_{sj}} f(x) = 0$ и из неравенства (49) легко вытекает, что найдется прогрессия P_{sj}, для которой выполнено

$$\sum_{x\in P_{sj}} f(x) \geqslant \frac{\beta |P|}{4m\sqrt{2}} \geqslant \frac{\beta |P_{sj}|}{4\sqrt{2}}\,.$$

Таким образом, мы нашли арифметическую прогрессию P', для которой $|A \cap P'| \geqslant (\delta + \varepsilon)|P'|$, где ε зависит только от δ и α_0. Как было сказано выше, проделав ту же самую процедуру несколько раз, мы в конце концов найдем арифметическую прогрессию в A.

Простым следствием теоремы 9 является предложение о раскраске множества $[N]$ в два цвета.

Следствие 3. *Пусть k, N – натуральные числа и $N \geqslant 2^{2^{2^{2^{k+9}}}}$. Пусть также множество $[N]$ раскрашено в два цвета. Тогда в $[N]$ найдется монохроматическая арифметическая прогрессия длины k.*

Итак, как может убедиться читатель, доказательство Гауэрса теоремы 9 существенным образом опирается на теорему Фреймана. Еще одно приложение теоремы 23 принадлежит С. Л. Чои [68]. Он соединил теорему Семереди и теорему Фреймана и получил следующий результат.

Теорема 24 (Чои). *Пусть A – произвольное подмножество $\mathbb{Z}$, $C > 0$ – положительная константа и $k \geqslant 3$ – натуральное число. Пусть также $|A + A| \leqslant C|A|$. Тогда найдется константа $\alpha = \alpha(C, k)$ такая, что множество A содержит $\alpha |A|^2$ арифметических прогрессий длины k.*

Мы завершаем этот параграф некоторыми замечаниями о гипотезе Эрдёша и Турана 2.

Гипотеза 3 (Эрдёш, Туран). *Пусть $A = \{n_1 < n_2 < \cdots\}$ – бесконечная последовательность натуральных чисел таких, что*

$$\sum_{i=1}^\infty \frac{1}{n_i} = \infty. \tag{50}$$

Тогда A содержит арифметическую прогрессию любой длины.

Существует тесная связь между оценками величины $a_k(N)$ и гипотезой 3.

Утверждение 2. *Гипотеза 3 справедлива тогда и только тогда, когда для всех $k \geqslant 3$ выполнено*

$$\sum_{l=1}^{\infty} a_k(4^l) < \infty. \tag{51}$$

Доказательство. Для доказательства утверждения нам потребуется простая лемма об $a_k(N)$.

Лемма 2. *Пусть $k \geqslant 3$ – натуральное число. Пусть также x, y – натуральные числа, $x \leqslant y$. Тогда*

$$a_k(y) \leqslant \frac{x}{y}\left(\left\lfloor \frac{y}{x} \right\rfloor + 1\right) a_k(x) \leqslant 3a_k(x). \tag{52}$$

Доказательство. Пусть $M \subseteq [y]$ – максимальное множество без арифметических прогрессий длины k. Рассмотрим непересекающиеся отрезки $\Delta_1 = [1, x]$, $\Delta_2 = [x+1, 2x], \ldots, \Delta_s = [(s-1)x+1, sx]$, где $s = \lfloor y/x \rfloor + 1$. Ясно, что $[y]$ лежит в объединении этих отрезков. Так как M не содержит арифметических прогрессий длины k, то для всякого $j = 1, \ldots, s$ выполнено $|M \cap \Delta_j| \leqslant x a_k(x)$. Отсюда

$$a_k(y)y = |M| = \sum_{j=1}^{s} |M \cap \Delta_j| \leqslant \sum_{j=1}^{s} x a_k(x) = x\left(\left\lfloor \frac{y}{x} \right\rfloor + 1\right) a_k(x). \tag{53}$$

Замечание 2. В лемме 2 было установлено простейшее неравенство для функции $a_k(N)$. Дальнейшие результаты, касающиеся $a_k(N)$, могут быть найдены в статье К. Ф. Рота [7], а также недавней статье Э. Крута [62].

Приступим теперь к доказательству утверждения 2.

Достаточность. Пусть для всех $k \geqslant 3$ ряд $\sum_{l=1}^{\infty} a_k(4^l)$ сходится. Предположим, что гипотеза Эрдёша и Турана неверна. Иными словами, для некоторого $k_0 \geqslant 3$ найдется бесконечная последовательность натуральных чисел $A = \{n_1 < n_2 < \cdots\}$, не содержащая арифметических прогрессий длины k_0, такая, что ряд (50) расходится. Пусть $N = 16$. Разобьем натуральный ряд $\mathbb{N}$ на подмножества $C_0 = [1, N)$, $C_1 = [N, 4N)$, $C_2 = [4N, 4^2N), \ldots$, $C_l = [4^{l-1}N, 4^lN), \ldots$. Так как A не содержит арифметических прогрессий длины k_0, то для любого $l = 0, 1, 2, \ldots$ выполнено $|A \cap C_l| \leqslant 4^{l-1}N \cdot a_{k_0}(4^{l-1}N)$. Имеем

$$\sum_{i=1}^{\infty} \frac{1}{n_i} = \sum_{l=0}^{\infty} \sum_{n_i \in C_l} \frac{1}{n_i} \leqslant 4 \sum_{l=0}^{\infty} \frac{|A \cap C_l|}{4^{l-1}N} \leqslant 4 \sum_{l=0}^{\infty} a_{k_0}(4^{l+1}) = 4 \sum_{l=1}^{\infty} a_{k_0}(4^l) < \infty\,. \tag{54}$$

Неравенство (54) противоречит неравенству (50). Достаточность доказана.

Необходимость. Пусть для некоторого $k_0 \geqslant 3$ ряд $\sum_{l=1}^{\infty} a_{k_0}(4^l)$ расходится. Как и при доказательстве эквивалентности гипотез 1 и 1′, построим две последовательности натуральных чисел. Пусть $N_1 = 1$, $b_1 = 1$ и для $l \geqslant 2$ выполнено

$$N_l := b_{l-1} + N_{l-1}, \qquad b_l := b_{l-1} + N_{l-1} + N_l + 1. \tag{55}$$

Получаем возрастающую последовательность натуральных чисел $1 = N_1 < N_2 < N_3 < \cdots$. Для всякого $l = 1, 2, \ldots$ найдется множество $A_l \subseteq [N_l]$, не содержащее арифметических прогрессий длины k_0, такое, что $|A_l| = a_{k_0}(N_l)N_l$. Пусть $\widetilde{A}_l = A_l + b_l$. Ясно, что множества $\widetilde{A}_l$ не пересекаются и не содержат арифметических прогрессий длины k_0. Пусть $A = \bigsqcup_i \widetilde{A}_i$, $A = \{n_1 < n_2 < \cdots\}$. Применяя формулу (55), получаем, что A также не содержит арифметических прогрессий длины k_0. Имеем $b_l \leqslant 3N_l$ для всех $l \geqslant 1$. Аналогично, $N_{l+1} \leqslant 4N_l$ для $l \geqslant 1$. Отсюда $N_l \leqslant 4^l$, $l \geqslant 1$. Применяя лемму 1, находим

$$\sum_{i=1}^{\infty} \frac{1}{n_i} = \sum_{l=1}^{\infty} \sum_{n_i \in [b_l, b_l+N_l]} \frac{1}{n_i} \geqslant \sum_{l=1}^{\infty} \frac{a_{k_0}(N_l)N_l}{b_l + N_l} \geqslant \frac{1}{4} \sum_{l=1}^{\infty} a_{k_0}(N_l) \geqslant \frac{1}{12} \sum_{l=1}^{\infty} a_{k_0}(4^l). \tag{56}$$

Из формулы (56) вытекает, что ряд $\sum_{i=1}^{\infty} 1/n_i$ расходится. Применяя гипотезу Эрдёша–Турана, получаем, что множество A содержит арифметическую прогрессию длины k_0. Противоречие. Утверждение 2 доказано.

§ 6. Эргодический подход к теореме Семереди

Пусть X – некоторое множество с сигма-алгеброй множеств $\mathscr{B}$. Пусть также T – измеримое, сохраняющее меру μ отображение X в себя. Всюду ниже будем считать, что $\mu(X) = 1$. Четверка $(X, \mathscr{B}, \mu, T)$ называется *динамической системой с инвариантной мерой*. Хорошо известная **теорема А. Пуанкаре о возвращении** [69] утверждает, что для всякого измеримого множества $E \subseteq X$, $\mu(E) > 0$, существует натуральное $n > 0$ такое, что $\mu(E \cap T^{-n}E) > 0$.

В работе [15](см. также [17], [16]) Х. Фюрстенберг обобщил теорему Пуанкаре на случай нескольких степеней отображения T.

Теорема 25 (Фюрстенберг). *Пусть X – пространство с сигма-алгеброй измеримых множеств $\mathscr{B}$ и μ – мера на X. Пусть T – отображение X в себя, сохраняющее меру μ, и $k \geqslant 3$. Тогда для любого измеримого множества E с $\mu(E) > 0$ существует натуральное $n > 0$ такое, что*

$$\mu(E \cap T^{-n}E \cap T^{-2n}E \cap \cdots \cap T^{-(k-1)n}E) > 0.$$

В этом параграфе мы покажем, что теорема 25 эквивалентна теореме Семереди и, следовательно, Фюрстенбергом получено альтернативное доказательство гипотезы Эрдёша–Турана 1, использующее методы эргодической теории. Сформулируем теорему Семереди еще раз.

Теорема 26 (Семереди). *Пусть A – произвольное подмножество натурального ряда и $D^*(A) > 0$. Тогда для любого натурального $k \geqslant 3$ множество A содержит арифметическую прогрессию длины k.*

Легко показать (см. [17] или [16]), что теорема 25 вытекает из теоремы 26. Действительно, пусть N – достаточно большое натуральное число, которое будет выбрано ниже. Для любого $x \in X$ рассмотрим множество $\Lambda(x) = \{l \in [N] : T^l x \in E\}$. Имеем

$$\int_X |\Lambda(x)|\, d\mu = N\mu(E). \tag{57}$$

Пусть $M = \{x \in X : |\Lambda(x)| \geqslant N\mu(E)/2\}$. Из неравенства (57) вытекает, что $\mu(M) \geqslant \mu(E)/2$. Как было показано во введении, гипотеза 1 (другими словами, теорема 26) эквивалентна гипотезе 1′. Пусть $N = N(k, \mu(E)/2)$. Тогда для любого $x \in M$ множество $\Lambda(x)$ содержит арифметическую прогрессию длины k. Обозначим эту прогрессию через $\{a(x) + b(x)m\}_{m=0}^{k-1}$. Любой точке x из M мы сопоставили пару чисел $(a(x), b(x))$. Так как для всякого $x \in X$ выполнено $(a(x), b(x)) \in [N]^2$, то существует множество $M' \subseteq M$ со свойством $\mu(M') \geqslant \varepsilon/(2N^2)$, всем точкам которого соответствует одна и та же пара (a, b). Тогда $\mu\bigl(\bigcap_{m=0}^{k-1} T^{-(a+bm)}E\bigr) \geqslant \mu(M') > 0$. Отображение T сохраняет меру μ, следовательно,

$$\mu\biggl(\bigcap_{m=0}^{k-1} T^{-(a+bm)}E\biggr) = \mu\biggl(T^{-a}\bigcap_{m=0}^{k-1} T^{-(bm)}E\biggr) = \mu\biggl(\bigcap_{m=0}^{k-1} T^{-(bm)}E\biggr) > 0,$$

что и требовалось.

Итак, мы показали, что теорема 25 вытекает из теоремы 26. На самом же деле теорема 25 и теорема 26 равносильны. Для доказательства их равносильности Фюрстенберг установил следующий красивый результат, который называется *принципом соответствия Фюрстенберга* (см. [15]).

Теорема 27 (Фюрстенберг). *Пусть A – произвольное подмножество натурального ряда с $D^*(A) > 0$. Тогда существуют динамическая система с инвариантной мерой $(X, \mathscr{B}, \mu, T)$ и измеримое множество E, $\mu(E) = D^*(A)$, такие, что для всех натуральных $k \geqslant 3$ и всех натуральных положительных $m_1, m_2, \ldots, m_{k-1}$ выполнено*

$$D^*(A \cap (A + m_1) \cap \cdots \cap (A + m_{k-1})) \geqslant \mu(E \cap T^{-m_1}E \cap \cdots \cap T^{-m_{k-1}}E). \quad (58)$$

Теорема 27 указывает на тесную связь между эргодической теорией и комбинаторными задачами об арифметических прогрессиях.

Утверждение 3 (Фюрстенберг). *Из теорем 25 и 27 вытекает теорема 26.*

Доказательство. Пусть k – натуральное число, $k \geqslant 3$. Пусть также множество $A \subseteq \mathbb{N}$ не содержит арифметических прогрессий длины k и имеет положительную верхнюю плотность. По теореме 27 существуют динамическая система $(X, \mathscr{B}, \mu, T)$ и измеримое множество E положительной меры такие, что для всех натуральных $m_1, m_2, \ldots, m_{k-1}$, выполнено неравенство (58). С другой стороны, по теореме 25 существует натуральное $n > 0$ такое, что

$$\mu(E \cap T^{-n}E \cap T^{-2n}E \cap \cdots \cap T^{-(k-1)n}E) > 0. \quad (59)$$

Положим $m_1 = n$, $m_2 = 2n, \ldots$, $m_{k-1} = (k-1)n$. Из (58) и (59) вытекает неравенство $D^*(A \cap (A + n) \cap \cdots \cap (A + (k-1)n)) > 0$. Это противоречит тому, что A не содержит арифметических прогрессий длины k. Утверждение 3 доказано.

В этом обзоре мы не будем доказывать теорему 27 в полном объеме. Заинтересованный читатель может найти подробное доказательство принципа соответствия в статье [15] или книге [17]. Тем не менее мы попытаемся показать

схематически, каким образом по произвольному подмножеству натурального ряда A с $D^*(A) > 0$ в теореме 27 строится динамическая система с требуемыми свойствами.

Итак, пусть множество $A \subseteq \mathbb{N}$ имеет положительную верхнюю плотность Банаха. Пусть $\Omega = \{0,1\}^{\mathbb{N}}$ – пространство бесконечных в одну сторону последовательностей из нулей и единиц. Пусть отображение T пространства Ω в себя задается формулой $(T\omega)_i = \omega_{i+1}$. Таким образом, отображение T представляет собой сдвиг влево. Пусть также $\omega' \in \Omega$ – бесконечная последовательность такая, что $\omega'_i = 1$ тогда и только тогда, когда $i \in A$. Возьмем произвольную метрику на пространстве Ω и рассмотрим замыкание X орбиты точки ω' под действием отображения T. Иными словами, пусть $X = \overline{\{T^i\omega'\}_{i=0}^{\infty}}$. Ясно, что X является T-инвариантным множеством. Пусть $C_0 = \{\omega \in \Omega : \omega_0 = 1\}$ – элементарный цилиндр, и пусть $E = C_0 \cap X$. Из определения точки ω' вытекает, что A содержит арифметическую прогрессию длины k тогда и только тогда, когда для некоторого натурального $n \geqslant 1$ множество $\bigcap_{m=0}^{k-1} T^{-mn}E$ непусто (заметим, что $\bigcap_{m=0}^{k-1} T^{-mn}E$ открыто).

Мы не будем доказывать неравенство (58), а лишь построим вероятностную инвариантную относительно T меру на X так, чтобы $\mu(E) = D^*(A) > 0$. Так как $D^*(A) > 0$, то существует возрастающая последовательность натуральных чисел n_k такая, что $\lim_{k\to\infty} |A \cap [n_k]|/n_k = D^*(A)$. Пусть $\mu_k := 1/n_k \cdot \sum_{i=0}^{n_k-1} \delta_{T^i\omega'}$, где δ_x означает меру Дирака на X : $\delta_x(M) = 1$ тогда и только тогда, когда $x \in M$. Ясно, что для каждого k мера μ_k является вероятностной мерой на X. Кроме того, для любого множества $M \subseteq X$ выполнено

$$\left|\mu_k(T^{-1}M) - \mu_k(M)\right| \leqslant \frac{2}{n_k}. \tag{60}$$

Пусть μ – $*$-слабый предел вероятностных мер μ_k (см. определение $*$-слабого предела, например, в [70]). Тогда из неравенства (60) вытекает, что μ является T-инвариантной вероятностной мерой на X. Кроме того,

$$\mu(E) = \lim_{k\to\infty} \mu_k(E) = \lim_{k\to\infty} \frac{|A \cap [n_k]|}{n_k} = D^*(A) > 0,$$

что и требовалось.

Используя эргодический подход, Х. Фюрстенберг, Я. Кацнельсон, Д. Орнштейн и другие получили множество обобщений теоремы Семереди. В настоящем обзоре мы не сможем охватить все имеющиеся здесь результаты и ограничимся лишь некоторыми из них. В работе [18] Фюрстенберг и Кацнельсон перенесли теорему 25 на случай нескольких *коммутирующих* отображений.

Теорема 28 (Фюрстенберг, Кацнельсон). *Пусть X – пространство с сигма-алгеброй измеримых множеств $\mathscr{B}$ и μ – мера на X. Пусть $k \geqslant 2$ и $T_1, \dots, T_k$ – сохраняющие меру μ коммутирующие отображения X в себя. Тогда для любого измеримого множества E с $\mu(E) > 0$ существует натуральное $n > 0$ такое, что*

$$\mu(E \cap T_1^{-n}E \cap T_2^{-n}E \cap \dots \cap T_k^{-n}E) > 0.$$

В § 7 мы получим количественный вариант теоремы 28 для случая *двух* коммутирующих отображений. Следует сказать, что недавно в работе [21] теорема 28 была доказана для произвольных разрешимых групп.

Отметим также замечательную теорему В. Бергельсона и А. Лейбмана [19] (см. также [71]), уже упоминавшуюся во введении.

ТЕОРЕМА 29 (Бергельсон, Лейбман). *Пусть X – некоторое множество и $\mathscr{B}$ – сигма-алгебра измеримых множеств на X и μ – конечная мера на X, $\mu(X) > 0$. Пусть $k \geqslant 2$, $T_1, \dots, T_k$ – обратимые сохраняющие меру μ коммутирующие отображения X в себя и $p_1(n), \dots, p_k(n)$ – многочлены с рациональными коэффициентами, принимающие целые значения для целых значений n. Пусть также $p_i(0) = 0$, $i = 1, \dots, k$. Тогда для любого измеримого множества E с $\mu(E) > 0$ выполнено*

$$\liminf_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} \mu(T_1^{-p_1(n)} E \cap T_2^{-p_2(n)} E \cap \dots \cap T_k^{-p_k(n)} E) > 0.$$

А. Шаркози в работах [72], [73] получил количественный вариант теоремы 29 для случая $k = 2$, $T_2 = T_1^2$ и $p_1(n) = n$, $p_2(n) = n^2$ (см. также [74] и [25]). Наилучший на сегодняшний день результат по этой тематике принадлежит Я. Пинцу, В. Стигеру и Е. Семереди (см. [75]).

ТЕОРЕМА 30 (Пинц, Стигер, Семереди). *Пусть A – произвольное подмножество $[N]$ и*

$$|A| \gg \frac{N}{(\log N)^{c \log\log\log\log N}},$$

где $c > 0$ – некоторая абсолютная константа. Тогда A содержит два элемента a, a' такие, что $a' - a$ есть полный квадрат.

Используя эргодическую технику, Фюрстенберг и Кацнельсон [20] передоказали известную теорему Холса–Джуита [76], обобщающую теорему Ван дер Вардена 1. Чтобы сформулировать теорему Холса–Джуита, нам потребуется несколько определений.

Пусть

$$C_t^n := \{x_1 x_2 \dots x_n : x_i \in \{0, 1, \dots, t-1\}\}$$

есть множество всех слов длины n, составленных из букв $0, 1, \dots, t-1$.

ОПРЕДЕЛЕНИЕ 7. *Комбинаторной прямой* в C_t^n называется набор из t слов $X_1, \dots, X_t \in C_t^n$, где $X_i = x_{i1} \dots x_{in}$, таких, что для некоторого непустого множества $J \subseteq \{1, \dots, n\}$ выполнено $x_{sj} = s$, если $j \in J$, и для всех $j \notin J$ найдется буква $c_j \in \{0, 1, \dots, t-1\}$, для которой выполнено $x_{1j} = \dots = x_{tj} = c_j$.

ПРИМЕР. Пусть $t = 3$, $n = 5$. Тогда слова 01012, 11112, 21212 образуют комбинаторную прямую в C_3^5.

ТЕОРЕМА 31 (Холс, Джуит). *Пусть t, r – натуральные числа. Тогда существует натуральное число $N = N(t, r)$ такое, что для всех $n \geqslant N$ и для любой раскраски C_t^n в r цветов найдется монохроматическая комбинаторная прямая.*

Ясно, что из теоремы 31 вытекает теорема Ван дер Вардена 2 (и, следовательно, теорема Ван дер Вардена 1). Действительно, в системе исчисления по основанию t множество C_t^n можно интерпретировать как числа от 0 до $t^n - 1$. При этом комбинаторная прямая в C_t^n будет соответствовать арифметической прогрессии длины t в множестве $\{0, 1, \dots, t^n - 1\}$.

Как было сказано ранее, теорема 25 послужила отправной точкой нового раздела эргодической теории – комбинаторной эргодической теории. В настоящем обзоре мы не в состоянии даже перечислить все имеющиеся в данной области результаты. Мы можем лишь указать заинтересованному читателю на замечательную книгу [17] и монографию [77]. Отметим также, что в недавних работах [78]–[86] получены количественные варианты теоремы Пуанкаре, а в работе [87] – теоремы 27.

Как отмечалось выше, существует тесная связь между оригинальным доказательством теоремы Семереди, доказательством Фюрстенберга и Гауэрса. Мы хотим закончить этот параграф обсуждением основных идей, лежащих в основе метода Фюрстенберга.

В первой, предварительной, части своего доказательства Фюрстенберг устанавливает справедливость теоремы 25 для двух специальных классов динамических систем: слабо-перемешивающих и компактных динамических систем. Дадим строгие определения этих классов.

Динамическая система называется *слабо-перемешивающей*, если для любых двух множеств $A, B \in \mathscr{B}$ выполнено

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \Big(\mu(A \cap T^{-n}B) - \mu(A)\mu(B) \Big)^2 = 0.$$

С любой динамической системой $(X, \mathscr{B}, \mu, T)$ можно связать унитарный оператор U в $L_2(X, \mathscr{B}, \mu)$, действующий по правилу $(Uf)(x) = f(Tx)$ для любой функции $f\colon X \to \mathbb{C}$. Функция, тождественно равная единице, всегда является собственным вектором этого оператора. Динамическая система называется компактной, если U имеет дискретный спектр. Дадим другое определение. Система называется компактной, если для любой функции $f \in L_2(X, \mathscr{B}, \mu)$ замыкание в $L_2(X, \mathscr{B}, \mu)$ орбиты $\{U^n f\}_{n=0}^{\infty}$ является компактом. Можно показать, что динамическая система не может быть одновременно слабо-перемешивающей и компактной (более подробно см. [17]).

Как было сказано ранее, для динамических систем из названных классов справедлива теорема 25. Тем не менее причины, по которым эта теорема выполняется, – совершенно разные. Слабо-перемешивающие динамические системы обладают сильными случайными свойствами, что позволяет доказать для этих систем утверждение более сильное, чем теорема 25.

Теорема 32 (Фюрстенберг). *Пусть $(X, \mathscr{B}, \mu, T)$ – слабо-перемешивающая динамическая система, и пусть $A_0, A_1, \dots, A_k \in \mathscr{B}$, $k \geqslant 1$, – произвольные измеримые множества. Тогда*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \big(\mu(A_0 \cap T^{-n}A_1 \cap T^{-2n}A_2 \cap \dots \cap T^{-kn}A_k) - \mu(A_0)\mu(A_1)\dots\mu(A_k) \big)^2 = 0.$$

С другой стороны, совершенно ясно, что теорема 25 верна для периодических отображений T, т.е. для отображений, для которых найдется $p \in \mathbb{N}$ такое, что T^p является тождественным отображением. Очень широким обобщением периодических систем являются компактные динамические системы. Рассмотрим следующий пример. Пусть X есть единичная окружность $\mathbb{S}^1$, μ – мера Лебега на X и $\mathscr{B}$ – сигма-алгебра измеримых по Лебегу множеств. Пусть отображение T_α есть поворот окружности $\mathbb{S}^1$, задаваемый формулой $T_\alpha x = x + \alpha \pmod 1$, где α – любое, не обязательно рациональное, действительное число. Тогда динамическая система $(X, \mathscr{B}, \mu, T_\alpha)$ будет компактной. Ясно, что для иррационального α отображение T_α не будет периодическим, но также ясно, что T_α будет "почти периодическим", в том смысле, например, что для любого интервала I и любого $\varepsilon > 0$ найдется число n такое, что $\mu(T^n I \triangle I) < \varepsilon$. Пользуясь "почти периодическими" свойствами компактных динамических систем, Фюрстенберг доказал для них теорему 25. Заметим, что для таких систем более сильная теорема 32 не верна (см. [16]). Все дело в том, что компактные системы не обладают хорошими случайными свойствами.

На втором этапе своего доказательства Фюрстенберг дает характеризацию слабо-перемешивающих динамических систем с помощью факторов. Пусть $\mathscr{B}_1 \subseteq \mathscr{B}$ – под-сигма-алгебра сигма-алгебры $\mathscr{B}$. Пусть также отображение T измеримо относительно этой сигма-алгебры, иными словами, для любого множества $A \in \mathscr{B}_1$ выполнено $T^{-1}A \in \mathscr{B}_1$. Тогда динамическая система $(X, \mathscr{B}_1, \mu, T)$ называется *фактором* динамической системы $(X, \mathscr{B}, \mu, T)$. Если система $(X, \mathscr{B}_1, \mu, T)$ является компактной, то мы говорим, что фактор $(X, \mathscr{B}_1, \mu, T)$ – компактный. Фактор называется *нетривиальным*, если он содержит множества, мера которых не равна нулю или единице.

Теорема 33 (Фюрстенберг). *Динамическая система $(X, \mathscr{B}, \mu, T)$ является слабо-перемешивающей тогда и только тогда, когда у нее нет нетривиальных компактных факторов.*

Из теоремы 33 вытекает, что у любой динамической системы $(X, \mathscr{B}, \mu, T)$ существует нетривиальный фактор, для которого справедлива теорема 25. Действительно,если $(X, \mathscr{B}, \mu, T)$ является слабо-перемешивающей динамической системой, то для нее справедлива теорема 32. Если же $(X, \mathscr{B}, \mu, T)$ не слабо-перемешивающая система, то по теореме 33 у нее существует нетривиальный компактный фактор. Но так как найденный фактор является компактным, то мы получаем, что для него справедлива теорема 25.

Рассмотрим семейство $\mathscr{M}$ нетривиальных факторов исходной динамической системы $(X, \mathscr{B}, \mu, T)$, для которых справедлива теорема 25 (на самом деле в своем доказательстве Фюрстенберг рассматривает немного другое семейство факторов). Как мы только что показали, семейство $\mathscr{M}$ непусто. Фюрстенберг доказал два факта о семействе $\mathscr{M}$. Первый состоит в том, что у $\mathscr{M}$ есть максимальный элемент, а второй – этот максимальный элемент совпадает с $(X, \mathscr{B}, \mu, T)$. Ясно, что из этих двух фактов следует теорема 25.

Доказательство утверждения о существовании максимального элемента у $\mathscr{M}$ относительно просто и использует лемму Цорна. Доказательство того, что максимальный элемент семейства $\mathscr{M}$ совпадает с исходной динамической системой,

– сложно и занимает по объему почти половину статьи [16]. Мы можем лишь вкратце изложить имеющиеся здесь идеи.

Во-первых, Фюрстенберг обобщает понятия слабо-перемешивающих и компактных динамических систем на факторы системы $(X, \mathscr{B}, \mu, T)$. Пусть $\mathscr{B}_1 \subseteq \mathscr{B}_2$ – две сигма-алгебры. Фюрстенберг дает определение компактности (а также слабого перемешивания) фактора $(X, \mathscr{B}_2, \mu, T)$ относительно фактора $(X, \mathscr{B}_1, \mu, T)$ и доказывает утверждение о поднятии: если для "меньшего" фактора была выполнена теорема 25, то она выполнена и для "большего". Во-вторых, Фюрстенберг устанавливает, что если фактор $(X, \mathscr{B}_1, \mu, T)$ начальной системы $(X, \mathscr{B}, \mu, T)$ не является слабо-перемешивающим, то найдется фактор $(X, \mathscr{B}_1', \mu, T)$, $\mathscr{B}_1 \subsetneq \mathscr{B}_1'$, такой, что $(X, \mathscr{B}_1', \mu, T)$ компактен относительно $(X, \mathscr{B}_1, \mu, T)$.

Предположим, что *максимальный* фактор $F_0 = (X, \mathscr{B}_0, \mu, T)$ из семейства $\mathscr{M}$ не совпадает с $F = (X, \mathscr{B}, \mu, T)$. Если F_0 является относительно слабо-перемешивающим, то $F \in \mathscr{M}$ и мы получили противоречие с максимальностью F_0. Если же F_0 не является относительно слабо-перемешивающим, то найдется фактор F_0', больший F_0 и компактный относительно F_0. Значит, $F_0' \in \mathscr{M}$ и мы опять получили противоречие с максимальностью F_0. Это рассуждение завершает доказательство Фюрстенберга.

Необходимо отметить, что рассуждения Фюрстенберга не дают никаких верхних оценок величины $N(k, \delta)$. Как мы видели, в своем доказательстве Фюрстенберг существенно использует лемму Цорна. Тем не менее недавно появилось новое доказательство теоремы Семереди (см. [43]) методами эргодической теории и дающее количественные (правда, очень слабые) оценки $N(k, \delta)$.

§ 7. Двумерные обобщения теоремы Семереди

Рассмотрим двумерную решетку $[1, N]^2$ с базисом $\{(1, 0), (0, 1)\}$. Пусть

$$L(N) = \frac{1}{N^2} \max\big\{|A| : A \subseteq [N]^2 \\ \text{и } A \text{ не содержит троек вида } (k, m), (k + d, m), (k, m + d),\ d > 0\big\}. \tag{61}$$

Тройку из (61) мы будем называть *уголком*. В работе [88] М. Атаи и Е. Семереди доказали, что величина $L(N)$ стремится к нулю, когда N стремится к бесконечности. Говоря точнее, они получили следующий результат.

Теорема 34. *Пусть $0 < \delta \leqslant 1$ – действительное число, N – натуральное число и $S = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ – единичный квадрат. Тогда любое множество $A \subseteq [N]^2$, $|A| \geqslant \delta N^2$, содержит аффинный образ S, т.е. множество $aS + b$, где $a \in \mathbb{N}$ и $b \in \mathbb{N}^2$.*

Затем теорема 34 была передоказана Х. Фюстенбергом в [17] (более подробно см. § 5).

Ясно, что задача про уголки является двумерным обобщением задачи о множествах без арифметических прогрессий длины три. Точнее, из равенства $\lim_{N\to\infty} L(N) = 0$ вытекает $\lim_{N\to\infty} a_3(N) = 0$.

Действительно, пусть $\lim_{N\to\infty} L(N) = 0$, но $\lim_{N\to\infty} a_3(N) = a > 0$ (то, что $\lim_{N\to\infty} a_3(N)$ существует, было доказано во введении). Последнее равенство означает, что для всех достаточно больших N найдется множество $A_N \subseteq [N]$ без прогрессий длины три, мощности не меньше, чем $aN/2$. Рассмотрим квадрат $Q_N = \{1,\dots,2N\}^2$ и множество $\widetilde{A}_N = \bigsqcup_{i=1}^{N}\big((A_N + i)\times\{i\}\big) \subseteq Q_N$. Двумерное множество $\widetilde{A}_N$ представляет собой объединение N трансляций множества A_N в направлении правого верхнего угла квадрата Q_N. Нетрудно убедиться, что если $\widetilde{A}_N$ содержит уголок, то A_N содержит арифметическую прогрессию длины три, что неверно. Кроме того, мощность $\widetilde{A}_N$ равна $|A_N|N \geqslant aN^2/2$. Отсюда вытекает, что $\limsup_{N\to\infty} L(N) > 0$. Противоречие с равенством $\lim_{N\to\infty} L(N) = 0$.

В. Т. Гауэрс (см. [22]) поставил вопрос о скорости сходимости $L(N)$ к 0. В работе [89] В. Ву, развивая подход из статей [90], [91], предложил следующее решение этого вопроса. Пусть $\log_{[1]} = \log N$ и для $l \geqslant 2$ положим $\log_{[l]} N = \log(\log_{[l-1]} N)$. Таким образом $\log_{[l]} N$ есть результат взятия логарифма от числа N l раз подряд. Далее, пусть k – наибольшее натуральное число такое, что $\log_{[k]} N \geqslant 2$. Тогда положим $\log_* N = k$. Ву доказал, что

$$L(N) \leqslant \frac{100}{(\log_* N)^{1/4}}\,.$$

В работах [28], [29] был получен следующий результат.

Теорема 35 [28], [29]. *Пусть $\delta > 0$, $N \gg \exp\exp\exp(\delta^{-C})$, $C > 0$ – некоторая эффективная константа и $A \subseteq \{1,\dots,N\}^2$ – произвольное подмножество мощности не меньше, чем δN^2. Тогда A содержит тройку вида (k,m), $(k+d,m)$, $(k,m+d)$, где $d > 0$.*

Затем эта теорема была улучшена (см. [30], [31]).

Теорема 36 [30], [31]. *Пусть $\delta > 0$, $N \gg \exp\exp(\delta^{-c})$, $c > 0$ – некоторая абсолютная константа и $A \subseteq \{1,\dots,N\}^2$ – произвольное подмножество мощности не меньше, чем δN^2. Тогда A содержит тройку вида (k,m), $(k+d,m)$, $(k,m+d)$, где $d > 0$.*

Таким образом, получена оценка величины $L(N)$ сверху:

$$L(N) \ll \frac{1}{(\log\log N)^{C_1}}\,,$$

где $C_1 = 1/c$.

Вопрос о верхних оценках для функции $L(N)$ в группах $\mathbb{Z}_p^n$, где p – простое число, был рассмотрен в [92]. В таких группах *уголком* называется тройка вида (k,m), $(k+d,m)$, $(k,m+d)$ с $d \neq 0$. В настоящем обзоре мы ограничимся, для простоты изложения, случаем $p = 2$.

Теорема 37 (Грин). *Пусть $\delta > 0$, N и n – натуральные, $N = 2^n$, $N \gg \exp\exp(\delta^{-c'})$, $c' > 0$ – некоторая абсолютная константа и $A \subseteq \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ – произвольное подмножество мощности не меньше, чем δN^2. Тогда A содержит тройку вида (k,m), $(k+d,m)$, $(k,m+d)$, где $d \neq 0$.*

Доказательства теорем 35 и 36 довольно сложны из-за большого количества технических деталей. В этом обзоре мы ограничимся изложением более простой теоремы 37. При этом основные идеи доказательства теорем 35 и 36 сохранятся, а технические сложности сведутся к минимуму.

Мы излагаем доказательство по [92]. Прежде чем доказывать теорему 37, дадим несколько определений.

Пусть $x, y \in \mathbb{Z}_2^n$. Пусть также скалярное произведение $x \cdot y$ задается формулой

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n.$$

Пусть $f\colon \mathbb{Z}_2^n \to \mathbb{C}$ – некоторая функция. Обозначим через $\widehat{f}(x)$ коэффициент Фурье функции f:

$$\widehat{f}(\xi) = \sum_{x \in \mathbb{Z}_2^n} f(x) e(-(x \cdot \xi)),$$

где $e(x) = e^{2\pi i x}$.

Мы будем использовать несколько несложных фактов о преобразовании Фурье:

$$\sum_{x \in \mathbb{Z}_2^n} |f(x)|^2 = \frac{1}{N} \sum_{\xi \in \mathbb{Z}_2^n} |\widehat{f}(\xi)|^2, \tag{62}$$

$$\sum_{x \in \mathbb{Z}_2^n} f(s)\overline{g(s)} = \frac{1}{N} \sum_{\xi \in \mathbb{Z}_2^n} \widehat{f}(\xi)\overline{\widehat{g}(\xi)}, \tag{63}$$

$$\sum_{x \in \mathbb{Z}_2^n} |(f * g)(x)|^2 := \sum_{x \in \mathbb{Z}_2^n} \left| \sum_{y \in \mathbb{Z}_2^n} f(y)\overline{g(y-x)} \right|^2 = \frac{1}{N} \sum_{\xi \in \mathbb{Z}_2^n} |\widehat{f}(\xi)|^2 |\widehat{g}(\xi)|^2 . \tag{64}$$

Определение 8. Пусть$A \subseteq \mathbb{Z}_2^n$ и $\alpha \in (0,1)$ – некоторый параметр. Множество A называется *α-равномерным*, если

$$\max_{\xi \neq 0} |\widehat{A}(\xi)| \leqslant \alpha N. \tag{65}$$

Следующая лемма позволяет лучше понять определение α-равномерных множеств.

Лемма 3. *Пусть $\tau, \kappa \in (0,1)$ – два параметра, а $S_1, \ldots, S_k \subseteq \mathbb{Z}_2^n$ – некоторые множества. Будем писать $\varepsilon(k) = \kappa 2^k \tau^{-k/2}$. Предположим, что $|S_i| = \sigma_i N$ и каждое S_i является $\varepsilon(k-1)$-равномерным. Тогда существует по крайней мере $(1 - 2^k\tau)N^k$ векторов $(x_1, \ldots, x_k) \in (\mathbb{Z}_2^n)^k$ таких, что*

$$\left| \sum_y S_1(x_1 + y) S_2(x_2 + y) \cdots S_k(x_k + y) - \sigma_1 \cdots \sigma_k N \right| \leqslant \varepsilon(k) N. \tag{66}$$

Доказательство. Доказательство леммы будет проходить по индукции. Случай $k = 1$ тривиален. Пусть $u = (x_1, \ldots, x_{k-1})$ – фиксированный вектор. Будем писать $F_u(y) = S_1(x_1 + y) S_2(x_2 + y) \cdots S_{k-1}(x_{k-1} + y)$. Тогда

$$\sum_y S_1(x_1 + y) S_2(x_2 + y) \cdots S_k(x_k + y) = (F_u * S_k)(-x_k) = (F_u * S_k)(x_k). \tag{67}$$

Пользуясь формулами (64), (62) и $\varepsilon(k-1)$-равномерностью множества S_k, получаем

$$\sum_{x_k}\Big((F_u * S_k)(x_k) - \sigma_k \sum_y F_u(y)\Big)^2 = N^{-1}\sum_{\xi\neq 0}|\widehat{F}_u(\xi)|^2|\widehat{S}_k(\xi)|^2 \leqslant \varepsilon(k-1)^2N^3\,. \tag{68}$$

По индукции существует по крайней мере $(1-2^{k-1}\tau)N^{k-1}$ значений u таких, что

$$\Big|\sum_y F_u(y) - \sigma_1\cdots\sigma_{k-1}N\Big| \leqslant \varepsilon(k-1)\tau N. \tag{69}$$

Используя (68), получаем, что для этих u выполнено

$$\sum_{x_k}((F_u * S_k)(x_k) - \sigma_1\cdots\sigma_k N)^2 \leqslant 4\varepsilon(k-1)^2N^3\,. \tag{70}$$

Из (70) вытекает, что при фиксированном u количество x_k, для которых $|(F_u * S_k)(x_k) - \sigma_1\cdots\sigma_k N| > \varepsilon(k)N$, не превосходит

$$\frac{4\varepsilon(k-1)^2}{\varepsilon(k)^2}N \leqslant 2^{k-1}\tau N.$$

Следовательно, общее число $(x_1,\ldots,x_k)$, для которых не выполнено неравенство (66), не больше, чем

$$2^{k-1}\tau N + 2^{k-1}\tau N = 2^k\tau N.$$

Лемма 3 доказана.

Таким образом, если множества S_i являются α-равномерными для достаточно малого α, то "почти все" трансляции этих множеств имеют мощность пересечения такую же, как если бы S_i были случайными множествами.

Нам понадобится лемма о не α-равномерных множествах.

Лемма 4. *Пусть $A\subseteq\mathbb{Z}_2^n$, $|A| = \delta N$. Предположим, что A не является α-равномерным множеством, другими словами, найдется $\lambda\neq 0$ такое, что $|\widehat{A}(\lambda)| > \alpha N$. Пусть $H = \langle\lambda\rangle^\perp \subseteq \mathbb{Z}_2^n$ – пространство, перпендикулярное вектору λ. Тогда*

$$\sum_x (A*H)^2(x) \geqslant (\delta^2+\alpha^2)|H|^2N. \tag{71}$$

Доказательство. По неравенству (64)

$$\begin{aligned}\sum_x (A*H)^2(x) &= \frac{1}{N}\sum_{\xi\in\mathbb{Z}_2^n}|\widehat{A}(\xi)|^2|\widehat{H}(\xi)|^2\\ &\geqslant \frac{1}{N}\big(|\widehat{A}(0)|^2|\widehat{H}(0)|^2 + |\widehat{A}(\lambda)|^2|\widehat{H}(\lambda)|^2\big) \geqslant (\delta^2+\alpha^2)|H|^2N,\end{aligned}$$

что и доказывает лемму 4.

Нам понадобится еще одно определение α-равномерности.

Определение 9. Пусть $f\colon \mathbb{Z}_2^n \times \mathbb{Z}_2^n \to D$ – некоторая функция. Определим *прямоугольную* норму f, $\|f\|$, по формуле

$$\|f\|^4 = \sum_{x,x',y,y'} f(x,y)\overline{f(x',y)f(x,y')}f(x',y'). \tag{72}$$

Ясно, что

$$\|f\|^4 = \sum_{x,x'}\Big|\sum_y f(x,y)\overline{f(x',y)}\Big|^2, \tag{73}$$

поэтому правая часть (72) всегда неотрицательна. В [29] было доказано, что $\|\cdot\|$ действительно является нормой.

Определение 10. Пусть α – любое действительное число из интервала $(0,1)$. Пусть $E_1 \times E_2$ – некоторое подмножество $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$. Функция $f\colon E_1 \times E_2 \to D$ называется *α-равномерной относительно прямоугольной нормы*, если

$$\|f\|^4 \leqslant \alpha|E_1|^2|E_2|^2. \tag{74}$$

Пусть $A \subseteq \mathscr{P} = E_1 \times E_2$. Множество A называется *α-равномерным относительно прямоугольной нормы*, если функция $A - \delta_{\mathscr{P}}(A)\mathscr{P}$ является α-равномерной относительно этой нормы.

Назовем четверку вида $\{(x,y),(x',y),(x,y'),(x',y')\}$ *простейшим прямоугольником*. Множество $A \subseteq \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ содержит простейший прямоугольник, если оно содержит все 4 точки прямоугольника.

Пусть множество $A \subseteq \mathscr{P} = E_1 \times E_2$. Ясно, что количество простейших прямоугольников в A равно $\|A\|^4$. Применяя формулу (73) и неравенство Коши–Буняковского, получаем

$$\begin{aligned}\|A\|^4 &= \sum_{x,x'}\Big|\sum_y A(x,y)A(x',y)\Big|^2 \geqslant \frac{1}{|E_1|^2}\Big(\sum_{x,x'}\sum_y A(x,y)A(x',y)\Big)^2\\ &= \frac{1}{|E_1|^2}\Big(\sum_y\Big|\sum_x A(x,y)\Big|^2\Big)^2 \geqslant \frac{1}{|E_1|^2|E_2|^2}\Big(\sum_{x,y}A(x,y)\Big)^4\\ &= \delta_{\mathscr{P}}(A)^4|E_1|^2|E_2|^2.\end{aligned}$$

Значит, любое множество $A \subseteq \mathscr{P}$ содержит по крайней мере $\delta_{\mathscr{P}}(A)^4|E_1|^2|E_2|^2$ простейших прямоугольников. С другой стороны, легко показать, что количество простейших прямоугольников в случайных подмножествах $\mathscr{P}$ примерно равно $\delta_{\mathscr{P}}(A)^4|E_1|^2|E_2|^2$.

Множества, α-равномерные относительно прямоугольной нормы, характеризуются ясным комбинаторным свойством (см. [29]).

Теорема 38. *Пусть множество $A \subseteq E_1 \times E_2 = \mathscr{P}$ является α-равномерным относительно прямоугольной нормы. Тогда A содержит не более $(\delta + \alpha^{1/4})^4|E_1|^2|E_2|^2$ простейших прямоугольников.*

Доказательство. Пусть $f = A - \delta_{\mathscr{P}}(A)\mathscr{P}$ – балансовая функция множества A и $\delta = \delta_{\mathscr{P}}(A)$. Так как множество A является α-равномерным, то $\|f\|^4 \leqslant \alpha|E_1|^2|E_2|^2$. Имеем $A = f + \delta\mathscr{P}$. Отсюда

$$\|A(x,y)\|^4 \leqslant (\|f\| + \|\delta\mathscr{P}\|)^4 \leqslant (\delta + \alpha^{1/4})^4|E_1|^2|E_2|^2. \tag{75}$$

Теорема 38 доказана.

Таким образом, число простейших прямоугольников в множествах A, α-равномерных относительно прямоугольной нормы, примерно такое же, как и в случайных подмножествах $\mathscr{P}$. Можно сказать, что чем меньше α, тем ближе A к случайному множеству.

Пусть W – некоторое подпространство $\mathbb{Z}_2^n$. Ясно, что W изоморфно некоторому $\mathbb{Z}_2^m$ с $m \leqslant n$. Пусть также $E_1, E_2 \subseteq W$, $E_i = \beta_i|W|$, $\mathscr{P} = E_1 \times E_2$ и $A \subseteq \mathscr{P}$, $\delta_{\mathscr{P}}(A) = \delta$. Первый шаг доказательства теоремы 37 относится к ситуации, когда множества E_1, E_2 являются α-равномерными и, кроме того, само множество A является α'-равномерным относительно прямоугольной нормы. Мы докажем, что если α, α' достаточно малы (т.е. E_1, E_2 и A близки к случайным), то в A найдется достаточно большое число уголков. Основной инструмент при доказательстве – это неравенство Коши–Буняковского.

Теорема 39. *Пусть множества E_i являются $(2^{-36}\beta_1^{12}\beta_2^{12}\delta^{36})$-равномерными, а множество A является $2^{-8}\delta^{12}$-равномерным относительно прямоугольной нормы. Тогда A содержит не менее $\delta^3\beta_1^2\beta_2^2|W|^3/2$ троек вида $\{(x,y),(x+d,y),(x,y+d)\}$.*

Доказательство. Пусть $f_1, f_2, f_3\colon \mathscr{P} \to D$ – три произвольные функции. Рассмотрим функционал $T(f_1,f_2,f_3) = \sum_{x,y,z} f_1(x,y)f_2(y+z,y)f_3(x,x+z)$. Ясно, что T линеен по каждому аргументу. Кроме того, $T(A,A,A)$ равно числу троек $\{(x,y),(x+d,y),(x,y+d)\}$ в A (здесь мы используем специфику $\mathbb{Z}_2^n$). Пусть $f = A - \delta\mathscr{P}$ и $\eta = 2^{-8}\delta^{12}$. Тогда $T(A,A,A) = \delta T(\mathscr{P},A,A) + T(f,A,A)$ и $\|f\|^4 \leqslant \eta\beta_1^2\beta_2^2|W|^4$.

Пусть $g(z) = \sum_x A(x,x+z)$. Тогда $T(\mathscr{P},A,A) = \sum_z g(z)^2$. Так как W – подпространство $\mathbb{Z}_2^n$, то $g(z)$ равно нулю вне W. Имеем $\sum_z g(z) = \delta\beta_1\beta_2|W|^2$. Применяя неравенство Коши–Буняковского, получаем

$$T(A,A,A) \geqslant \delta^3\beta_1^2\beta_2^2|W|^3 + T(f,A,A). \tag{76}$$

Оценим второй член в правой части (76). Применяя неравенство Коши–Буняковского второй раз, находим

$$\begin{aligned} T(f,A,A) &= \sum_{y,z} A(y+z,y) \sum_x E_1(y+z)f(x,y)A(x,x+z) \\ &\leqslant \left(\sum_{y,z} E_1(y+z)E_2(y)\right)^{1/2} \\ &\quad \times \left(\sum_{x,x',y,z} E_1(y+z)A(x,x+z)A(x',x'+z)f(x,y)f(x',y)\right)^{1/2}. \end{aligned} \tag{77}$$

Имеем $\sum_{y,z} E_1(y+z)E_2(y) = \beta_1\beta_2|W|^2$. Далее,

$$\begin{aligned} \sigma &= \sum_{x,x',y,z} E_1(y+z)A(x,x+z)A(x',x'+z)f(x,y)f(x',y) \\ &= \sum_{x,x',z} A(x,x+z)A(x',x'+z) \sum_y E_1(y+z)E_2(x+z)E_2(x'+z)f(x,y)f(x',y). \end{aligned}$$

Пусть $\omega(x,x',y,y') = \sum_z E_1(y+z)E_1(y'+z)E_2(x+z)E_2(x'+z)$. Применяя неравенство Коши–Буняковского в третий раз, получаем

$$\sigma \leqslant \Big(\sum_{x,x',z} E_1(x)E_1(x')E_2(x+z)E_2(x'+z)\Big)^{1/2} \times \Big(\sum_{x,x',y,y'} \omega(x,x',y,y')f(x,y)f(x',y)f(x,y')f(x',y')\Big)^{1/2}. \tag{78}$$

Из леммы 3 вытекает, что

$$\sum_{x,x',z} E_1(x)E_1(x')E_2(x+z)E_2(x'+z) \leqslant 2\beta_1^2\beta_2^2|W|^3.$$

Используя неравенства (77), (78), находим

$$T(f,A,A)^4 \leqslant 2\beta_1^4\beta_2^4|W|^7 \sum_{x,x',y,y'} \omega(x,x',y,y')f(x,y)f(x',y)f(x,y')f(x',y'). \tag{79}$$

По лемме 3, применяемой к случаю $k=4$ и $\tau = 2^{-4}\beta_1^4\beta_2^4\eta$, $\kappa = 2^{-12}\beta_1^{12}\beta_2^{12}\eta^3$, существует не менее $(1-\beta_1^4\beta_2^4\eta)|W|^4$ значений (x,x',y,y'), для которых выполнено $|\omega(x,x',y,y') - \beta_1^2\beta_2^2|W||\leqslant \beta_1^4\beta_2^4\eta$. Отсюда

$$\Big|\sum_{x,x',y,y'} (\omega(x,x',y,y') - \beta_1^2\beta_2^2|W|)f(x,y)f(x',y)f(x,y')f(x',y')\Big| \leqslant 3\beta_1^4\beta_2^4\eta|W|^5. \tag{80}$$

По условию множество A является η-равномерным относительно прямоугольной нормы. Применяя последнее неравенство и (79), получаем

$$|T(f,A,A)| \leqslant 2\beta_1^2\beta_2^2\eta^{1/4}|W|^3. \tag{81}$$

Из (76) окончательно находим

$$T(A,A,A) \geqslant (\delta^3\beta_1^2\beta_2^2 - 2\beta_1^2\beta_2^2\eta^{1/4})|W|^3 \geqslant \delta^3\beta_1^2\beta_2^2|W|^3/2.$$

Теорема 39 доказана.

Предположим, что условие $2^{-8}\delta^{12}$-равномерности относительно прямоугольной нормы множества A в теореме 39 не выполнено. В следующем предложении мы докажем, что тогда существует достаточно большое множество $\mathscr{Q} \subseteq \mathscr{P}$, плотность A в котором больше δ на некоторую положительную величину.

Предложение 8. *Пусть $\mathscr{P} = E_1 \times E_2$, $A \subseteq \mathscr{P}$. Пусть также $\delta_{\mathscr{P}}(A) = \delta$ и A не η-равномерно относительно прямоугольной нормы с $\eta > 0$. Тогда существуют множества $F_i \subseteq E_i$, $i = 1,2$, такие, что $|F_i| \geqslant 2^{-8}\eta|E_i|$ и для $\mathscr{Q} = F_1 \times F_2$ выполнено $\delta_{\mathscr{Q}}(A) \geqslant \delta + 2^{-14}\eta^2$.*

При доказательстве предложения 8 оказывается удобным язык теории графов. Это не удивительно, поскольку существует тесная связь между α-равномерными множествами и так называемыми квазислучайными графами (более подробно см. [93], [94]).

Пусть $|E_1| = M_1$, $|E_2| = M_2$. Может так случится, что $E_1 \cap E_2 \neq \varnothing$. Мы хотим избежать этой ситуации. Пусть X есть биективный образ E_1, а Y – E_2 такие, что $X \cap Y = \varnothing$. Определим двудольный граф G, связанный с множеством A. Пусть X, Y – его доли и вершина $x \in X$ соединена с вершиной $y \in Y$ тогда и только тогда, когда $(x, y) \in A$. Ясно, что у графа G ровно $\delta M_1 M_2$ вершин. Обозначим через $\mathscr{N}(x)$ множество исходящих ребер из вершины $x \in X$ и той же буквой $\mathscr{N}(y)$ множество входящих ребер в $y \in Y$. Пусть также $d(x) = |\mathscr{N}(x)|$, $x \in X$, и $d(y) = |\mathscr{N}(y)|$, $y \in Y$.

Для доказательства предложения 8 нам понадобится несколько лемм.

Первая необходимая нам лемма утверждает, что "для почти всех" $x \in X$ можно считать $d(x)$ примерно равным δM_2. То же самое, по симметрии, относится и к $d(y)$.

Лемма 5. *Пусть $\varepsilon_1, \varepsilon_2 \in (0, 1)$. Предположим, что*

(a) *либо существует по меньшей мере $\varepsilon_1 M_1$ вершин $x \in X$, для которых $|d(x) - \delta M_2| > \varepsilon_2 M_2$,*

(b) *либо существует не менее $\varepsilon_2 M_2$ вершин $y \in Y$, для которых $|d(y) - \delta M_1| > \varepsilon_1 M_1$. Тогда найдутся множества $X' \subseteq X$, $Y' \subseteq Y$ такие, что $|X'| \geqslant \min(\varepsilon_1/2, \varepsilon_2/2) M_1$, $|Y'| \geqslant \min(\varepsilon_1/2, \varepsilon_2/2) M_2$ и $\delta_{X' \times Y'}(A) \geqslant \delta + \varepsilon_1 \varepsilon_2 / 2$.*

Доказательство. Можно считать, что выполнена первая альтернатива, иными словами, найдется по меньшей мере $\varepsilon_1 M_1$ вершин $x \in X$, для которых $|d(x) - \delta M_2| > \varepsilon_2 M_2$.

Предположим вначале, что существует не менее $\varepsilon_2 M_1 / 2$ вершин $x \in X$ таких, что $d(x) > (\delta + \varepsilon_2) M_2$. Пусть X' – множество этих x, а $Y' = Y$. Тогда $\delta_{X' \times Y'}(A) \geqslant \delta + \varepsilon_2$ и лемма доказана.

Пусть X_0 – множество тех $x \in X$, для которых $d(x) < (\delta - \varepsilon_2) M_2$. Положим $X' = X \setminus X_0$, $Y' = Y$, и пусть $|X'| = \kappa M_1$. Так как количество ребер в G равно $\delta M_1 M_2$, то

$$(\delta - \varepsilon_2)(1 - \kappa) M_1 M_2 + \kappa M_1 M_2 \geqslant \delta M_1 M_2,$$

откуда $\kappa \geqslant \varepsilon_2$. Имеем $|X_0| \geqslant \varepsilon_1 M_1 / 2$. Отсюда $\kappa \leqslant 1 - \varepsilon_1 / 2$ и

$$\delta_{X' \times Y'}(A) \geqslant \frac{\delta M_1 - (\delta - \varepsilon_2) M_1}{|X'|} = \delta + \varepsilon_2 \left(\frac{1}{\kappa} - 1 \right) \geqslant \delta + \frac{\varepsilon_1 \varepsilon_2}{2}. \tag{82}$$

Лемма 5 доказана.

Мы видим, что если выполнено (a) или (b), то предложение 8 доказано (подробнее см. ниже). Поэтому мы будем считать, что величины $d(x)$, $d(y)$ "почти всюду" равны δM_2 и δM_1 соответственно.

Следующую лемму можно считать обратной к теореме 38.

Лемма 6. *Пусть A не является η-равномерным множеством относительно прямоугольной нормы. Предположим, что для всех $x \in X$, кроме, может быть, $\eta M_1 / 56$ штук, выполнено неравенство $|d(x) - \delta M_2| \leqslant \eta M_2 / 56$ и для всех $y \in Y$, кроме, может быть, $\eta M_2 / 56$ штук ,выполнено $|d(y) - \delta M_1| \leqslant \eta M_1 / 56$. Тогда $\|A\|^4 \geqslant (\delta^4 + \eta/2) M_1^2 M_2^2$.*

Доказательство. Пусть $f(x,y) = A(x,y) - \delta X(x)Y(y)$. Раскрывая скобки в выражении $\|A\|^4 = \|f + \delta(X \times Y)\|^4$, получаем сумму σ, состоящую из 16 членов. Главный член в σ равен $\delta^4 M_1^2 M_2^2$, а член $\|f\|^4$ не меньше $\eta M_1^2 M_2^2$ по условию. Остальные 14 слагаемых в σ имеют вид

$$\sum_{x,x' \in X,\ y,y' \in Y} \delta \cdot f(x',y)g(x,y')h(x',y'), \tag{83}$$

где g и h – некоторые функции, $\|g\|_\infty$, $\|h\|_\infty \leqslant 1$. Оценим сумму (83). Имеем

$$\begin{aligned}\sigma' &= \left|\delta \sum_{x,x' \in X,\ y,y' \in Y} f(x',y)g(x,y')h(x',y')\right| \\ &\leqslant \sum_{x,x',y'} \left|\sum_y f(x',y)\right| = \sum_{x,x',y'} |d(x') - \delta M_2|. \end{aligned}\tag{84}$$

Используя предположения леммы относительно $d(x)$, получаем неравенство $\sigma' \leqslant \eta M_1^2 M_2^2/28$. Таким образом,

$$\|A\|^4 \geqslant (\delta^4 + \eta - 14\eta/28) M_1^2 M_2^2 = (\delta^4 + \eta/2) M_1^2 M_2^2.$$

Лемма 6 доказана.

Лемма 7. *Пусть* $\|A\|^4 \geqslant (\delta^4 + \eta/2)M_1^2 M_2^2$. *Предположим, что для всех* $x \in X$, *кроме, может быть,* $\eta M_1/32$ *штук, выполнено неравенство* $|d(x) - \delta M_2| \leqslant \eta M_2/32$ *и для всех* $y \in Y$, *кроме, может быть,* $\eta M_2/32$ *штук, выполнено* $|d(y) - \delta M_1| \leqslant \eta M_1/32$. *Тогда существуют множества* $X' \subseteq X$, $Y' \subseteq Y$ *такие, что* $|X'| \geqslant \eta M_1/32$, $|Y'| \geqslant \eta M_2/32$ *и* $\delta_{X' \times Y'}(A) \geqslant \delta + \eta/8$.

Доказательство. Пусть $(x,y) \in X \times Y$ и $e(x,y)$ – число ребер между $\mathscr{N}(x)$ и $\mathscr{N}(y)$. Легко видеть, что

$$\sum_{(x,y) \in A} e(x,y) = \|A\|^4 \geqslant (\delta^4 + \eta/2) M_1^2 M_2^2.$$

Пусть X_0 – множество $x \in X$, для которых $|d(x) - \delta M_2| \leqslant \eta M_2/32$, и Y_0 – множество $y \in Y$ таких, что $|d(y) - \delta M_1| \leqslant \eta M_1/32$. По условию $|X_0^c| = |X \setminus X_0| \leqslant \eta M_1/32$ и $|Y_0^c| = |Y \setminus Y_0| \leqslant \eta M_2/32$. Поэтому число ребер, имеющих начало в X_0^c и конец в Y_0^c, не больше $\eta M_1 M_2/16$. Следовательно,

$$\sum_{(x,y) \in A,\ x \in X_0, y \in Y_0} e(x,y) \geqslant (\delta^4 + \eta/4) M_1^2 M_2^2. \tag{85}$$

Из (85) вытекает, что существуют $x \in X_0$, $y \in Y_0$, для которых $e(x,y) \geqslant (\delta^3 + \eta/4\delta) M_1 M_2$. Положим $X' = \mathscr{N}(x)$ и $Y' = \mathscr{N}(y)$. Так как $x \in X_0$, $y \in Y_0$, то $|X'| \leqslant (\delta + \eta/32)M_1$ и $|Y'| \leqslant (\delta + \eta/32)M_2$. Отсюда

$$\delta_{X' \times Y'}(A) \geqslant \frac{\delta^3 + \eta/(4\delta)}{(\delta + \eta/32)^2} \geqslant \delta + \eta/8.$$

Применяя тот факт, что $x \in X_0$, $y \in Y_0$, еще раз, находим $|X'| \geqslant \delta M_1/2 > \eta M_1/32$ и $|Y'| \geqslant \delta M_2/2 > \eta M_2/32$. Лемма 7 доказана.

Доказательство предложения 8. Предположим, что существует не менее $\eta M_1/56$ вершин $x \in X$, для которых $|d(x) - \delta M_2| > \eta M_2/56$. Тогда по лемме 5 найдутся два множества F_1, F_2 таких, что $|F_i| \geqslant 2^{-8}\eta M_i$, $i = 1, 2$, и для $\mathscr{Q} = F_1 \times F_2$ выполнено $\delta_{\mathscr{Q}}(A) \geqslant \delta + 2^{-14}\eta^2$. Мы видим, что в этом случае предложение доказано. Аналогично рассматривается ситуация, когда существует не менее $\eta M_2/56$ вершин $y \in Y$, для которых $|d(y) - \delta M_1| > \eta M_1/56$.

Если $|d(x) - \delta M_2| \leqslant \eta M_2/56$ для всех $x \in X$, кроме, может быть, $\eta M_1/56$ штук, и аналогично для $d(y)$, то по лемме 6 выполнено $\|A\|^4 \geqslant \delta^4 + \eta/2$. Затем применяем лемму 7 и находим множества F_1, F_2, для которых выполнено $|F_i| \geqslant \eta M_i/32$ и $\delta_{\mathscr{Q}}(A) = \delta_{F_1 \times F_2}(A) \geqslant \delta + \eta/8$. Предложение 8 доказано.

Объединим, для удобства, теорему 39 и предложение 8.

Предложение 9 (первый этап доказательства теоремы 37). *Пусть W – подпространство $\mathbb{Z}_2^n$, $E_i \subseteq W$, $|E_i| = \beta_i|W|$, $i = 1, 2$, и $\mathscr{P} = E_1 \times E_2$. Пусть также $A \subseteq \mathscr{P}$, $\delta_{\mathscr{P}}(A) = \delta$ и A не содержит уголков. Предположим, что*

$$|W| > 2\delta^{-3}\beta_1^{-2}\beta_2^{-2} \tag{86}$$

и E_i, $i = 1, 2$, являются $2^{-36}\beta_1^{12}\beta_2^{12}\delta^{36}$-равномерным подмножествами W.

Тогда существуют множества $F_i \subseteq E_i$ такие, что $|F_i| \geqslant 2^{-16}\delta^{12}|E_i|$ и $\delta_{F_1 \times F_2}(A) \geqslant \delta + 2^{-30}\delta^{24}$.

Доказательство. Предположим, что A является η-равномерным относительно прямоугольной нормы с $\eta = 2^{-8}\delta^{12}$. По теореме 39 множество A содержит не менее $\delta^3\beta_1^2\beta_2^2|W|^3$ троек вида $\{(x, y), (x + d, y), (x, y + d)\}$. Число троек с $d = 0$ не больше $|W|^2$. Применяя неравенство (86), получаем, что A содержит уголок. Следовательно, множество A не является η-равномерным относительно прямоугольной нормы с $\eta = 2^{-8}\delta^{12}$. По предложению 8 существуют множества $F_i \subseteq E_i$ такие, что $|F_i| \geqslant 2^{-16}\delta^{12}|E_i|$ и $\delta_{F_1 \times F_2}(A) \geqslant \delta + 2^{-30}\delta^{24}$. Предложение 9 доказано.

Предложение 10 (второй этап доказательства теоремы 37). *Пусть $\delta, \tau, \sigma \in (0, 1)$ – некоторые числа, W – подпространство $\mathbb{Z}_2^n$, $F_i \subseteq W$, $|F_i| = \beta_i|W|$, $i = 1, 2$, и $\mathscr{Q} = F_1 \times F_2$. Пусть также $A \subseteq \mathscr{Q}$, $\delta_{\mathscr{Q}}(A) = \delta + \tau$ и*

$$|W| > \exp(16\sigma^{-2}(\beta_1\beta_2)^{-1}\tau^{-1}). \tag{87}$$

Тогда существуют подпространство $W' \subseteq W$, $\dim W' \geqslant \dim W - 16\sigma^{-2}(\beta_1\beta_2)^{-1}\tau^{-1}$, и $t_1, t_2 \in W$ такие, что множества $E_1' = (F_1 - t_1) \cap W'$, $E_2' = (F_2 - t_2) \cap W'$, $\mathscr{P}' = E_1' \times E_2'$ обладают следующими свойствами:

(a) $|\mathscr{P}'| \geqslant \beta_1\beta_2\tau|W'|^2/2$;

(b) *E_1', E_2' являются σ-равномерными подмножествами W';*

(c) $\delta_{\mathscr{P}'}(A - (t_1, t_2)) \geqslant \delta + \tau/4$.

Доказательство. Доказательство предложения представляет собой алгоритм. Опишем его в общих чертах. На j-м шаге алгоритма множество $W \times W$ будет разбито на *клетки*

$$C^{(i)} = (W^{(i)} + t_1^{(i)}) \times (W^{(i)} + t_2^{(i)}), \qquad W \times W = \bigsqcup_{i \in \mathscr{I}_j} C^{(i)}, \tag{88}$$

где $t_1^{(i)}, t_2^{(i)} \in W$, каждое $W^{(i)}$ представляет собой подпространство W размерности не меньше, чем $\dim W - j$, а $\mathscr{I}_j$ – некоторое множество индексов. При переходе к $(j+1)$-му шагу алгоритма некоторые клетки $C^{(i)}$, $i \in \mathscr{I}_j$, останутся без изменений. Для других $i \in \mathscr{I}_j$ будут выбраны подпространства $H^{(i)} \subseteq W^{(i)}$ коразмерности 1. Так как $W^{(i)} = H^{(i)} \sqcup (H^{(i)})^\perp$, то клетки $C^{(i)}$ разобьются на четыре подклетки $\widetilde{C}^{(i_k)}$, $k = 1, 2, 3, 4$, где

$$\widetilde{C}^{(i_1)} = (H^{(i)} + t_1^{(i)}) \times (H^{(i)} + t_2^{(i)}), \qquad \widetilde{C}^{(i_2)} = ((H^{(i)})^\perp + t_1^{(i)}) \times (H^{(i)} + t_2^{(i)}),$$
$$\widetilde{C}^{(i_3)} = (H^{(i)} + t_1^{(i)}) \times ((H^{(i)})^\perp + t_2^{(i)}), \quad \widetilde{C}^{(i_4)} = ((H^{(i)})^\perp + t_1^{(i)}) \times ((H^{(i)})^\perp + t_2^{(i)}).$$

Перейдем теперь непосредственно к доказательству. Пусть $\beta = \beta_1\beta_2$. На первом шаге алгоритма положим $t_1^{(1)} = t_2^{(1)} = 0$, $\mathscr{I}_1 = \{1\}$ и $C^{(1)} = W \times W$. Ясно, что тогда формулы (88) справедливы. Пусть мы провели j шагов алгоритма и построили клетки $C^{(i)}$, а также множество $\mathscr{I}_j$, удовлетворяющие формулам (88). Пусть $D_1^{(i)} = F_1 \cap (W^{(i)} + t_1^{(i)})$, $D_2^{(i)} = F_2 \cap (W^{(i)} + t_2^{(i)})$ и

$$\beta_1^{(i)} = \frac{|D_1^{(i)}|}{|W^{(i)} + t_1^{(i)}|}, \qquad \beta_2^{(i)} = \frac{|D_2^{(i)}|}{|W^{(i)} + t_2^{(i)}|}. \tag{89}$$

Пусть также $\beta^{(i)} = \beta_1^{(i)}\beta_2^{(i)}$. Ясно, что

$$\sum_{i \in \mathscr{I}_j} |C^{(i)}|\beta^{(i)} = \beta|W|^2. \tag{90}$$

Будем говорить, что клетка $C^{(i)}$ *тощая*, если $\beta^{(i)} < \beta\tau/2$. Разделим все не тощие клетки на два класса. В первый класс отнесем все клетки, для которых $D_1^{(i)} - t_1^{(i)}$ и $D_2^{(i)} - t_2^{(i)}$ являются σ-равномерными подмножествами $W^{(i)}$. Назовем эти клетки *равномерными*. Остальными не тощие клетки будем называть *не равномерными*.

Итак, для $i \in \mathscr{I}_j$ клетка $C^{(i)}$ может оказаться тощей, равномерной или не равномерной. Пусть $\mathscr{E}_j$, $\mathscr{U}_j$, $\mathscr{N}_j$ означают соответствующие подмножества $\mathscr{I}_j$. Если

$$\sum_{i \in \mathscr{N}_j} |C^{(i)}| < \tau\beta|W|^2/4, \tag{91}$$

то мы останавливаем алгоритм на j-м шаге. В противном случае мы разобьем клетки для всех $i \in \mathscr{N}_j$ и оставим клетки для $i \in \mathscr{E}_j \sqcup \mathscr{U}_j$ без изменения. Заметим, что при таком алгоритме для всякого $i \in \mathscr{N}_j$ выполнено $\dim W^{(i)} = n - j$. Применяя неравенство (91), находим, что существует не менее $\frac{\tau}{4}2^{2j}$ значений $i \in \mathscr{N}_j$. Без ограничения общности можно считать, что найдется не менее $\frac{\tau}{8}2^{2j}$ значений i таких, что $D_1^{(i)} - t_1^{(i)}$ не являются σ-равномерными подмножествами $W^{(i)}$. По лемме 4 для любого такого i существует подпространство $H^{(i)} \subseteq W^{(i)}$ коразмерности 1 такое, что

$$\frac{1}{2}(\delta^2_{H^{(i)}}(D_1^{(i)} - t_1^{(i)}) + \delta^2_{(H^{(i)})^\perp}(D_1^{(i)} - t_1^{(i)})) \geqslant \beta_1^{(i)2} + \sigma^2. \tag{92}$$

Разобьем клетку $C^{(i)}$ на четыре подклетки $C^{(i_k)}$, $k = 1, 2, 3, 4$, как это было сделано выше. Пусть $\beta_1^{(i_k)} = \delta_{C^{(i_k)}}(F_1)$, $\beta_2^{(i_k)} = \delta_{C^{(i_k)}}(F_2)$, $k = 1, 2, 3, 4$. Из (92) вытекает, что

$$\frac{1}{4}(\beta_1^{(i_1)2} + \beta_1^{(i_2)2} + \beta_1^{(i_3)2} + \beta_1^{(i_4)2}) \geqslant \beta_1^{(i)2} + \sigma^2. \tag{93}$$

Докажем, что алгоритм закончит свою работу после $16\sigma^{-2}\beta^{-1}\tau^{-1}$ шагов или раньше. Пусть

$$\operatorname{ind}(\mathscr{I}_j) := \frac{1}{2|W|^2} \sum_{i \in \mathscr{I}_j} |C^{(i)}|(\beta_1^{(i)2} + \beta_2^{(i)2}). \tag{94}$$

Применяя неравенство (93) и оценку

$$\sum_{i \in \mathscr{N}_j} |C^{(i)}| \geqslant \tau\beta|W|^2/4, \tag{95}$$

находим, что $\operatorname{ind}(\mathscr{I}_{j+1}) \geqslant \operatorname{ind}(\mathscr{I}_j) + \dfrac{1}{16}\tau\beta\sigma^2$. С другой стороны, $\operatorname{ind}(\mathscr{I}_j) \leqslant 1$ для всех j. Следовательно, алгоритм обязан закончить свою работу после $16\sigma^{-2}\beta^{-1}\tau^{-1}$ шагов.

Пусть алгоритм остановился на K-м шаге, $K \leqslant 16\sigma^{-2}\beta^{-1}\tau^{-1}$. Так как каждая равномерная клетка разбиения (88) не является тощей, то она удовлетворяет условию (a) предложения 10. Ясно также, что любая равномерная клетка удовлетворяет условию (b). Покажем, что найдется равномерная клетка, для которой выполнено и свойство (c). Имеем

$$\sum_{i \in \mathscr{N}_j} |C^{(i)}| < \tau\beta|W|^2/4. \tag{96}$$

Пусть $\delta^{(i)} = |A \cap C^{(i)}|/|C^{(i)} \cap (F_1 \times F_2)|$. Ясно, что $\delta_{C^{(i)}}(A) = \delta^{(i)}\beta^{(i)}$. Так как для всех $i \in \mathscr{E}_K$ выполнено $\beta^{(i)} < \beta\tau/2$, то

$$\sum_{i \in \mathscr{E}_K} |C^{(i)}|\delta^{(i)}\beta^{(i)} < \beta\tau|W|^2/2. \tag{97}$$

Применяя (90) и равенство $\delta_{\mathscr{Q}}(A) = \delta + \tau$, находим

$$\sum_{i \in \mathscr{U}_K \sqcup \mathscr{N}_K} |C^{(i)}|\delta^{(i)}\beta^{(i)} > \beta(\delta + \tau)|W|^2 - \beta\tau|W|^2/2 \geqslant \beta(\delta + \tau/2)|W|^2. \tag{98}$$

Предположим, что для всех $i \in \mathscr{U}_K$ выполнено $\delta^{(i)} < \delta + \tau/4$. Применяя (90) и (96), получаем противоречивое неравенство

$$\begin{aligned}\beta(\delta + \tau/2)|W|^2 &\leqslant \sum_{i \in \mathscr{U}_K} |C^{(i)}|\delta^{(i)}\beta^{(i)} + \sum_{i \in \mathscr{N}_K} |C^{(i)}|\delta^{(i)}\beta^{(i)} \\ &< (\delta + \tau/4) \sum_{i \in \mathscr{I}_K} |C^{(i)}|\beta^{(i)} + \tau\beta|W|^2/4 = \beta(\delta + \tau/2)|W|^2. \end{aligned} \tag{99}$$

Поэтому существует $i \in \mathscr{U}_K$, для которого выполнено $\delta^{(i)} \geqslant \delta + \tau/4$. Положим $W' = W^{(i)}$, $t_1 = t_1^{(i)}$, $t_2 = t_2^{(i)}$. Подпространство W' и векторы t_1, t_2 удовлетворяют всем условиям предложения 10. Предложение 10 доказано.

Прежде чем приступить к доказательству основного результата этого параграфа, объединим первый и второй этапы доказательства теоремы 37 в одно предложение.

Предложение 11. *Пусть W – подпространство $\mathbb{Z}_2^n$, $E_i \subseteq W$, $|E_i| = \beta_i|W|$, $i = 1, 2$, $\beta = \beta_1\beta_2$ и $\mathscr{P} = E_1 \times E_2$. Пусть также $A \subseteq \mathscr{P}$, $\delta_{\mathscr{P}}(A) = \delta$, E_1, E_2 являются $2^{-36}\beta^{12}\delta^{36}$-равномерными и*

$$|W| > \exp(2^{1681}\delta^{-1272}\beta^{-25}). \tag{100}$$

Предположим, что A не содержит уголков. Тогда существуют подпространство $W' \subseteq W$ и множества E_1', E_2', $\mathscr{P}' = E_1' \times E_2'$ такие, что

(a) *числа β_1', β_2' и β', задаваемые формулами $E_1' = \beta_1'|W|$, $E_2' = \beta_2'|W|$, $\beta' = \beta_1'\beta_2'$, удовлетворяют неравенству $\beta' \geqslant 2^{-63}\delta^{48}\beta$;*

(b) *E_1', E_2' являются $2^{-36}\beta'^{12}\delta^{36}$-равномерными подмножествами W';*

(c) $\dim W' \geqslant \dim W - 2^{1681}\delta^{-1272}\beta^{-25}$;

(d) *для некоторого $t \in W \times W$ выполнено $\delta_{\mathscr{P}'}(A - t) \geqslant \delta + 2^{-32}\delta^{24}$.*

Для доказательства предложения 11 достаточно применить предложение 9, а затем предложение 10. При этом параметры τ и σ из предложения 10 будут равны $2^{-30}\delta^{24}$ и $2^{-36}(\beta')^{12}\delta^{36}$ соответственно.

Приступим непосредственно к доказательству теоремы 37, которое представляет собой алгоритм. На нулевом шаге алгоритма положим $\mathscr{P}_0 = \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ и предположим, что $A \subseteq \mathscr{P}_0$ не содержит уголков.

Пусть мы провели i шагов алгоритма, $i \geqslant 0$. Тогда

(i) множество $\mathscr{P}_i = E_i^{(1)} \times E_i^{(2)}$ содержится в $W_i \times W_i$, где W_i – подпространство $\mathbb{Z}_2^n$ коразмерности d_i;

(ii) $|\mathscr{P}_i| = \beta_i|W_i|^2$ и $E_i^{(1)}$, $E_i^{(2)}$ являются $2^{-36}\beta_i^{12}\delta^{36}$-равномерными подмножествами W_i;

(iii) для некоторого $t \in \mathbb{Z}_2^n \times \mathbb{Z}_2^n$ выполнено $\delta_{\mathscr{P}_i}(A - t) \geqslant \delta + 2^{-32}\delta^{24}i$.

Если

$$|W_i| > \exp(2^{1681}\delta^{-1272}\beta_i^{-25}), \tag{101}$$

то мы применяем предложение 11 и проводим $(i+1)$-й шаг алгоритма. Так как

$$d_{i+1} \leqslant d_i + 2^{1681}\delta^{-1272}\beta_i^{-25}$$

и

$$\beta_{i+1} \geqslant 2^{-63}\delta^{48}\beta_i,$$

то $\beta_i \geqslant (\delta/2)^{63i}$ и $d_i \leqslant \delta^{-C_1 i}$, где C_1 – абсолютная константа.

Используя условие (d) предложения 11, мы, как и в доказательстве теоремы Рота, заключаем, что количество шагов алгоритма не превосходит $K = C_2\delta^{-23}$, где C_2 – другая абсолютная константа.

Предположим, что

$$N \gg \exp(\delta^{-C_3\delta^{-23}}), \tag{102}$$

где C_3 – абсолютная константа. Легко проверить, что неравенство (102) гарантирует выполнение условия (101) на всех шагах алгоритма, в частности, и на его последнем, K-м шаге. Следовательно, мы можем провести $(K+1)$-й шаг алгоритма. Полученное противоречие показывает, что вместо неравенства (102) мы

имеем оценку $N \ll \exp(\delta^{-C_3\delta^{-23}})$, из которой вытекает, что $\delta \ll (\log\log N)^{-1/24}$. Теорема 37 доказана.

В работах [31], [81] было получено приложение теоремы 36 к теории динамических систем. Прежде чем сформулировать нашу теорему, мы дадим несколько определений.

Пусть X – некоторое множество с сигма-алгеброй измеримых множеств $\mathscr{B}$. Пусть μ – конечная мера на $\mathscr{B}$. Не ограничивая общности, будем считать, что $\mu(X) = 1$.

Определение 11 (хаусдорфова мера). Рассмотрим меру $H_h(\,\cdot\,)$ на X, определенную следующим образом:

$$H_h(E) = \lim_{\delta\to 0} H_h^\delta(E), \tag{103}$$

где $h(t)$ – неотрицательная ($h(0) = 0$) непрерывная возрастающая функция, а $H_h^\delta(E) = \inf\{\sum h(\delta_j)\}$, где inf берется по не более чем счетным покрытиям E открытыми множествами $\{B_j\}$, $\operatorname{diam}(B_j) = \delta_j < \delta$.

Если $h(t) = t^\alpha$, то получаем обычную меру Хаусдорфа.

Внешняя мера $H_h(\,\cdot\,)$ является сигма-аддитивной на сигма-алгебре множеств, измеримых по Каратеодори (более подробные сведения можно найти, например, в [95]). Хорошо известно, что эта сигма-алгебра содержит все борелевские множества.

Будем говорить, что меры μ и H_h *согласованы*, если любое μ-измеримое множество является H_h-измеримым (в смысле измеримости по Каратеодори).

Пусть S и R – два *коммутирующих* отображения пространства X, сохраняющих меру μ.

Определение 12. Функция

$$C_{S,R}(x) = C_{S,R}^h(x) := \liminf_{n\to\infty} \{L^{-1}(n)\cdot\max\{h(d(S^n x, x)), h(d(R^n x, x))\}\},$$

где $L^{-1}(n) = 1/L(n)$, называется *константой одновременного (или кратного) возвращения* точки x.

Теорема 40 [31], [81]. *Пусть X – метрическое пространство, имеющее $H_h(X) < \infty$, а S, R – коммутирующие отображения X в себя, сохраняющие меру μ. Предположим, что меры μ и H_h согласованы. Тогда $C_{S,R}(x)$ – интегрируемая (по мере μ) функция и для любого μ-измеримого A выполнено*

$$\int_A C_{S,R}(x)\,d\mu \leqslant H_h(A). \tag{104}$$

Если же $H_h(A) = 0$, то $\int_A C_{S,R}(x)\,d\mu = 0$ без условия согласованности мер μ и H_h.

Об оценках функции $C_{S,R}(x)$ *снизу* см. статью [87].

§ 8. Арифметические прогрессии, составленные из простых чисел

Гипотеза о том, что в множестве простых чисел найдется арифметическая прогрессия любой длины, имеет более чем двухвековую историю. Первые упоминания о прогрессиях в простых числах можно найти в переписке Лагранжа и Варинга, которая датируется 1770 годом (см. [96]). Между тем первые достижения в этой области относятся лишь к 1938 году, когда Н. Г. Чудаков [97], используя метод тригонометрических сумм И. М. Виноградова, доказал, что множество простых чисел содержит арифметические прогрессии длины три (см. также [98], [99]). Что касается прогрессий длины больше, чем три, то до последнего времени этот вопрос оставался открытым.

Для поиска прогрессий в простых числах применялись компьютеры. Так в 1995 году А. Моран, П. Притчард и Э. Тайссен [100] обнаружили, используя компьютер, следующую арифметическую прогрессию длины 22, составленную из простых чисел:

$$11410337850553 + 4609098694200k,$$

где $k = 0, 1, \ldots, 21$. Этот рекорд держался почти 10 лет. В 2004 году М. Фрайнд, П. Джоблин и П. Андервуд нашли прогрессию из простых чисел длины 23 (см. [101]). Эта прогрессия начиналась с 56211383760397 и имела разность 44546738095860.

В 2004 году Б. Грин и Т. Тао доказали следующий результат о прогрессиях в простых числах (см. [24]).

Теорема 41 (Грин, Тао). *Для всех натуральных $k \geqslant 3$ множество простых чисел содержит арифметическую прогрессию длины k.*

В этом параграфе мы приведем схему доказательства теоремы Грина и Тао.

Как известно, в отрезке $[N]$ множество простых чисел $\mathscr{P}$ имеет плотность $\pi(N)/N \sim 1/\ln N = o(1)$, $N \to \infty$ (см., например, [35]). Поэтому мы не можем применить к $\mathscr{P}$ теорему Семереди 6. Одна из основных идей Грина и Тао состояла в том, чтобы получить обобщение теоремы Семереди на так называемые *псевдослучайные* множества (ниже мы дадим точное определение), которые могут иметь нулевую плотность. Говоря вообще, существует много параллелей между подходом Грина и Тао и эргодическим методом. Например, псевдослучайные множества являются аналогом слабо-перемешивающих динамических систем. Более подробно об этих параллелях см. обзор [102]. Во второй части своего доказательства Грин и Тао применяют недавние результаты Д. Гольдстона и К. Я. Ялдирима (см. [103]–[105]) и показывают, что простые числа обладают нужными псевдослучайными свойствами.

Мы начнем с более подробного обсуждения первой части доказательства Грина и Тао, в которой они получают обобщение теоремы Семереди для псевдослучайных множеств. Их доказательство существенным образом опирается на теорему Семереди. Говоря более точно, они показывают, что доказанная ими обобщенная теорема вытекает из обычной теоремы Семереди.

Нам будет удобно сформулировать теорему Семереди для группы $\mathbb{Z}_N$. Пусть N – произвольное простое число. Некоторая величина равна $o(1)$, если она стремится к нулю, когда N стремится к бесконечности, и равна $O(1)$, если она

ограничена при N, стремящемся к бесконечности. Как и ранее, мы используем обозначение $\nu_{\mathrm{const}}\colon \mathbb{Z}_N \to \mathbb{R}^+$ для постоянной функции, тождественно равной единице: $\nu_{\mathrm{const}} \equiv 1$.

ТЕОРЕМА 42 (Теорема Семереди). *Пусть $k \geqslant 3$ – натуральное число и $\delta > 0$ – вещественное число. Пусть также N – достаточно большое простое число, а $f\colon \mathbb{Z}_N \to \mathbb{R}^+$ – некоторая неотрицательная функция, удовлетворяющая оценкам*

$$0 \leqslant f(x) \leqslant \nu_{\mathrm{const}}(x) \quad \text{для всех} \quad x \in \mathbb{Z}_N \tag{105}$$

и

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N} f(x) \geqslant \delta. \tag{106}$$

Тогда для некоторой положительной постоянной $c'(k,\delta) > 0$, зависящей только от k и δ, выполнено

$$\frac{1}{N^2}\sum_{x,r\in\mathbb{Z}_N} f(x)f(x+r)\cdots f(x+(k-1)r) \geqslant c'(k,\delta). \tag{107}$$

Теорема 18 из § 4 и теорема 42 имеют два отличия. Первая из них относится к $\mathbb{Z}$, вторая – к $\mathbb{Z}_N$. Кроме того, в формулировке первой теоремы присутствуют функции, а в формулировке второй – множества. На самом деле обе эти теоремы эквивалентны и при этом константы $c(k,\delta)$ и $c'(k,\delta)$ выражаются друг через друга явным образом. Действительно, первое отличие несущественно (см., например, доказательство теоремы 20). Второе отличие тоже не является важным. В самом деле, для любой функции f, удовлетворяющей неравенствам (105), (106), рассмотрим множество $A = \{x : f(x) \geqslant \delta/2\}$. Тогда $|A| \geqslant \delta/2\cdot N$. Следовательно, по теореме 18 для характеристической функции множества A справедливо неравенство (31) с константой, равной $c(k,\delta/2)$. Тогда для функции f неравенство (107) выполнено с константой $c'(k,\delta) = (\delta/2)^k\cdot c(k,\delta/2)$.

Изложим схему доказательства теоремы 41. В своей работе Грин и Тао заменяют жесткое условие (105), накладываемое на функцию f, на более слабое. Назовем функцию $\nu(x)$ *мерой*, если $1/N\cdot\sum_{x\in\mathbb{Z}_N}\nu(x) = 1 + o(1)$. Ясно, что $\nu_{\mathrm{const}}(x)$ – мера. Другим примером меры является функция Мангольдта, которая сосредоточена на степенях простых чисел:

$$\Lambda(x) = \begin{cases} \log p, & \text{если } x = p^m, \in \mathbb{N}, \\ 0 & \text{иначе.} \end{cases}$$

Имеем $1/N\cdot\sum_{x\in\mathbb{Z}_N}\Lambda(x) = 1 + o(1)$ (см., например, [106]), следовательно, $\Lambda(x)$ – мера. В обобщении теоремы 42 доказывается, что тождественная единица $\nu_{\mathrm{const}}(x)$ из (105) может быть заменена на некоторую меру $\nu(x)$, удовлетворяющую двум условиям: условию линейных форм и корреляционному условию (ниже мы дадим точные определения). При этом мера $\nu(x)$ может возрастать, когда x стремится к бесконечности. После этого обобщение теоремы 42 применяется к некоторой конкретной мере $\nu_0(x)$, связанной с простыми числами. При проверке того, что $\nu_0(x)$ удовлетворяет условию линейных форм и корреляционному условию, существенным образом используются недавние работы Гольдстона и Ялдирима [103]–[105].

Определение 13 (условие линейных форм). Пусть $\nu\colon \mathbb{Z}_N \to \mathbb{R}^+$ – некоторая мера. Пусть также m_0, t_0, L_0 – натуральные числа, $L_0 < N$. Мера ν удовлетворяет (m_0, t_0, L_0)-условию линейных форм, если выполнено следующее. Пусть m, t – произвольные, $m \leqslant m_0$, $t \leqslant t_0$ и $(L_{ij})_{1\leqslant i\leqslant m,\ 1\leqslant j\leqslant t}$ – некоторые рациональные числа, числитель и знаменатель которых не превосходит по абсолютной величине L_0. Пусть также $b_i \in \mathbb{Z}_N$, $1 \leqslant i \leqslant m$, и $\psi_i\colon \mathbb{Z}_N^t \to \mathbb{Z}_N$ – линейные формы $\psi_i(\mathbf{x}) = \sum_{j=1}^t L_{ij}x_j + b_i$, где $\mathbf{x} = (x_1, \dots, x_t) \in \mathbb{Z}_N^t$ и рациональные числа L_{ij} интерпретируются как элементы $\mathbb{Z}_N$ стандартным образом. Пусть, кроме того, для всех $i = 1, \dots, m$ строки $(L_{ij})_{1\leqslant j\leqslant t} \in \mathbb{Q}^t$ ненулевые и никакая строчка не получается из другой умножением на рациональное число. Пусть, наконец, выполнено

$$\frac{1}{N^t}\sum_{\mathbf{x}\in\mathbb{Z}_N^t} \nu(\psi_1(\mathbf{x}))\cdots\nu(\psi_m(\mathbf{x})) = 1 + o_{L_0,m_0,t_0}(1). \tag{108}$$

Тогда ν удовлетворяет (m_0, t_0, L_0)-условию линейных форм.

Определение 14 (корреляционное условие). Пусть $\nu\colon \mathbb{Z}_N \to \mathbb{R}^+$ – некоторая мера. Пусть также m_0 – натуральное число и для всех $m = 1, \dots, m_0$ найдется функция $\tau_m\colon \mathbb{Z}_N \to \mathbb{R}^+$ такая, что для всех $q \geqslant 1$ справедливо неравенство

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N} \tau_m^q(x) = O_{m,q}(1), \tag{109}$$

и такая, что для всех $h_1, \dots, h_m \in \mathbb{Z}_N$ выполнено

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N} \nu(x+h_1)\nu(x+h_2)\cdots\nu(x+h_m) \leqslant \sum_{1\leqslant i<j\leqslant m} \tau_m(h_i - h_j). \tag{110}$$

Тогда мера ν удовлетворяет m_0-корреляционному условию.

Определение 15 (псевдослучайная мера). Пусть $\nu\colon \mathbb{Z}_N \to \mathbb{R}^+$ – некоторая мера. Мера ν называется *k-псевдослучайной*, если она удовлетворяет $(k2^{k-1}, 3k-4, k)$ – условию линейных форм и 2^{k-1}-корреляционному условию.

Ясно, что мера $\nu_{\mathrm{const}}(x)$ является k-псевдослучайной для всех натуральных k. Оказывается, k-псевдослучайные меры – это меры, близкие к $\nu_{\mathrm{const}}(x)$ в смысле равномерных норм Гауэрса (см. определение в § 5).

Предложение 12. *Пусть $\nu(x)$ есть k-псевдослучайная мера. Тогда для всех $1 \leqslant d \leqslant k-1$ выполнено*

$$\|\nu - \nu_{\mathrm{const}}\|_{U^d} = \|\nu - 1\| = o(1). \tag{111}$$

Доказательство. Из свойства монотонности норм Гауэрса (45) вытекает, что (111) достаточно доказать для $d = k-1$. Иными словами, достаточно показать, что

$$\sigma := \sum_{x\in\mathbb{Z}_N,\ h\in\mathbb{Z}_N^{k-1}} \prod_{\omega\in\{0,1\}^{k-1}} (\nu(x+\omega\cdot h) - 1) = o(N^k). \tag{112}$$

Левая часть (112) равна

$$\sum_{A\subseteq\{0,1\}^{k-1}}(-1)^{|A|}\sum_{x\in\mathbb{Z}_N,\ h\in\mathbb{Z}_N^{k-1}}\prod_{\omega\in A}\nu(x+\omega\cdot h). \tag{113}$$

Для всякого фиксированного множества A выражение

$$\sum_{x\in\mathbb{Z}_N,\ h\in\mathbb{Z}_N^{k-1}}\prod_{\omega\in A}\nu(x+\omega\cdot h) \tag{114}$$

может быть переписано в виде

$$\sum_{\mathbf{z}\in\mathbb{Z}_N^k}\nu(\psi_1(\mathbf{z}))\cdots\nu(\psi_{|A|}(\mathbf{z})), \tag{115}$$

где $\mathbf{z}=(x,h_1,\dots,h_{k-1})$ и $\psi_1,\dots,\psi_{|A|}$ – ненулевые линейные формы $\psi_\omega(\mathbf{z}):=x+\omega\cdot h$, $\omega\in A$. Ясно, что никакая из этих форм не получается из другой умножением на рациональное число. Так как мера ν является k-псевдослучайной, то она удовлетворяет $(k2^{k-1},3k-4,k)$-условию линейных форм и, в частности, $(2^{k-1},k,1)$-условию линейных форм. Следовательно, каждое выражение вида (114) равно $N^k+o(N^k)$. Отсюда

$$\sigma=N^k\sum_{A\subseteq\{0,1\}^{k-1}}(-1)^{|A|}(1+o(1))=o(N^k),$$

что и требовалось доказать.

Сформулируем обобщение теоремы Семереди, доказанное Грином и Тао.

Теорема 43 (теорема Семереди для псевдослучайных мер). *Пусть k – натуральное число, $k\geqslant 3$ и $0<\delta\leqslant 1$. Пусть также $\nu\colon\mathbb{Z}_N\to\mathbb{R}^+$ является k-псевдослучайной мерой и функция $f\colon\mathbb{Z}_N\to\mathbb{R}^+$ удовлетворяет неравенствам*

$$0\leqslant f(x)\leqslant\nu(x)\quad\text{для всех}\quad x\in\mathbb{Z}_N \tag{116}$$

и

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N}f(x)\geqslant\delta. \tag{117}$$

Тогда для положительной постоянной $c'(k,\delta)>0$ из теоремы 42 выполнено

$$\frac{1}{N^2}\sum_{x,r\in\mathbb{Z}_N}f(x)f(x+r)\cdots f(x+(k-1)r)\geqslant c'(k,\delta). \tag{118}$$

Чтобы вывести из теоремы 43 теорему 41, необходимо предъявить псевдослучайную меру $\nu(x)$ и функцию $f(x)$, которые бы удовлетворяли условиям (116) и (117).

В качестве функции $f(x)$ можно попытаться взять функцию Мангольдта $\Lambda(x)$. Как было замечено ранее, $1/N\cdot\sum_{x\in\mathbb{Z}_N}\Lambda(x)=1+o(1)$, следовательно, $\Lambda(x)$ удовлетворяет (117). Теперь надо найти k-псевдослучайную меру $\nu(x)$ такую, чтобы для некоторой положительной константы $c(k)$ выполнялось неравенство $\nu(x)\geqslant c(k)\Lambda(x)$. Если такая мера будет предъявлена, то по теореме 43 мы найдем арифметическую прогрессию длины k в множестве чисел

вида $p, p^2, p^3, \dots, p \in \mathscr{P}$. Это, конечно, еще не доказывает теорему 41, так как члены найденной арифметической прогрессии могут не оказаться простыми числами. На самом деле, легко показать, что старшие степени простых чисел $p^2, p^3, \dots$ дадут вклад, равный $o(1)$, в сумму (118). Поэтому, если бы мы нашли k-псевдослучайную меру $\nu(x)$ такую, что $\nu(x) \geqslant c(k)\Lambda(x)$, $c(k) > 0$, то теорема 41 была бы доказана.

К сожалению, k-псевдослучайной меры с требуемым свойством не существует. Мы приведем здесь схематическое доказательство этого факта. Легко показать, что для всякого фиксированного целого $q > 1$ любая псевдослучайная мера равномерно распределена по всем q классам вычетов $a \pmod q$. Пусть $\varphi(x)$ – функция Эйлера. Известно, что величина $\varphi(x)/x$ может быть сделана сколь угодно малой (см., например, [36; с. 35]), поэтому существует q такое, что $\varphi(q)/q < 1/c(k)$. С другой стороны, если для класса вычетов a выполнено $(a, q) > 1$, то простых чисел в таком классе не существует. Так как вклад старших степеней простых чисел $p^2, p^3, \dots$ в среднее значение функции Мангольдта равен $o(1)$, то найдется класс вычетов a, для которого $1/N \cdot \sum_{x\in\mathbb{Z}_N,\ x\equiv a \pmod q} \Lambda(x) \geqslant 1/\varphi(q) + o(1)$. Так как $\varphi(q)/q < 1/c(k)$ и $1/N \cdot \sum_{x\in\mathbb{Z}_N, x\equiv a \pmod q} \nu(x) = 1/q + o(1)$, то неравенство $\nu(x) \geqslant c(k)\Lambda(x)$ не может быть верным для всех x.

Итак, мы видим, что "неравномерности" в распределении простых чисел не позволяют найти псевдослучайную меру с требуемыми свойствами. Чтобы избежать описанные выше трудности, Грин и Тао предложили подход, который они назвали W-прием.

Пусть $w(N)$ – некоторая функция, медленно возрастающая к бесконечности (порядок роста $w(N)$ будет выбран позже), и пусть $W = \prod_{p\in[w(N)]} p$ – произведение простых чисел из отрезка $[w(N)]$. Определим измененную функцию Мангольдта $\widetilde{\Lambda}\colon \mathbb{Z}^+ \to \mathbb{R}^+$ по формуле

$$\widetilde{\Lambda}(x) = \begin{cases} \dfrac{\varphi(W)}{W}\log(Wx+1), & \text{если } Wx+1 \text{ – простое число,} \\ 0 & \text{иначе.} \end{cases}$$

Если $w(N) \ll \log\log N$, то, применяя теорему Дирихле об арифметических прогрессиях, получаем $\sum_{x\in\mathbb{Z}_N} \widetilde{\Lambda}(x) = N(1+o(1))$. Таким образом, для $\widetilde{\Lambda}(x)$, так же как и для $\Lambda(x)$, неравенство (117) выполнено. Будем считать в дальнейшем, что $w(N) \ll \log\log N$. Главное отличие $\widetilde{\Lambda}(x)$ от функции Мангольдта состоит в том, что для $\widetilde{\Lambda}(x)$ существует k-псевдослучайная мера $\nu(x)$ такая, что $\nu(x) \geqslant c(k)\Lambda(x)$, $c(k) > 0$. Говоря более строго, справедливо следующее предложение.

Предложение 13. *Пусть $\varepsilon_k = 1/(2^k(k+4)!)$ и N – достаточно большое простое число. Тогда существует k-псевдослучайная мера $\nu\colon \mathbb{Z}_N \to \mathbb{R}^+$ такая, что для всех $x \in [\varepsilon_k N, 2\varepsilon_k N]$ выполнено $\nu(x) \geqslant k^{-1}2^{-k-5}\widetilde{\Lambda}(x)$.*

Выведем из предложения 13 теорему 41. Пусть $f\colon \mathbb{Z}_N \to \mathbb{R}^+$ – функция такая, что $f(x) = k^{-1}2^{-k-5}\widetilde{\Lambda}(x)$ для всех $x \in [\varepsilon_k N, 2\varepsilon_k N]$ и $f(x) = 0$ – иначе. Применяя теорему Дирихле об арифметических прогрессиях, находим

$$\frac{1}{N}\sum_{x\in\mathbb{Z}_N} f(x) = \frac{k^{-1}2^{-k-5}}{N} \sum_{x\in[\varepsilon_k N, 2\varepsilon_k N]} \widetilde{\Lambda}(x) = k^{-1}2^{-k-5}\varepsilon_k(1+o(1)). \qquad (119)$$

Применяя теперь предложение 13 и теорему 43, получаем

$$\frac{1}{N^2}\sum_{x,r\in\mathbb{Z}_N} f(x)f(x+r)\cdots f(x+(k-1)r) \geqslant c'(k,k^{-1}2^{-k-5})+o(1). \qquad (120)$$

Вклад в сумму (120) слагаемых с $r=0$ равен $O((\log N)^k/N)=o(1)$. Следовательно, мы можем считать, что суммирование в (120) проходит по $r\neq 0$. Так как $\varepsilon_k < 1/k$, то все числа $x, x+r, \ldots, x+(k-1)r$ принадлежат $[N]$. Значит, суммирование в (120) проходит по числам $x, r \in [N]$, $r\neq 0$, таким, что $x+r,\ldots,x+(k-1)r$ принадлежат $[N]$, и, следовательно, в множестве простых чисел найдется нетривиальная арифметическая прогрессия длины k. Теорема 41 доказана.

Таким образом, чтобы установить справедливость результата Грина и Тао, достаточно доказать предложение 13, построив мажорирующую k-псевдослучайную меру $\nu(x)$.

Нам понадобится определение, данное Гольдстоном и Ялдиримом (см. [103]–[105]).

Определение 16 (Гольдстон, Ялдирим). Пусть N – простое число и R – некоторый вещественный параметр, зависящий от N. Тогда

$$\Lambda_R(x) := \sum_{d|x,d\leqslant R}\mu(d)\log(R/d) = \sum_{d|x}\mu(d)\log(R/d)_+, \qquad (121)$$

где μ – функция Мёбиуса и $\log(x)_+ = \max(\log x, 0)$.

Используя определение 16, Грин и Тао строят мажорирующую k-псевдослучайную меру $\nu\colon \mathbb{Z}_N \to \mathbb{R}^+$.

Определение 17. Пусть $R = N^{k^{-1}2^{-k-4}}$, $\varepsilon_k = 1/(2^k(k+4)!)$. Тогда

$$\nu(x) := \begin{cases} \dfrac{\varphi(W)}{W}\,\dfrac{\Lambda_R(Wn+1)^2}{\log R}, & \text{если } x\in[\varepsilon_k N, 2\varepsilon_k N],\\ 1, & \text{если } x\in\mathbb{Z}_N\setminus[\varepsilon_k N, 2\varepsilon_k N].\end{cases}$$

Докажем, что $\nu(x)$ мажорирует $\widetilde{\Lambda}(x)$.

Лемма 8. *Для всех $x\in\mathbb{Z}_N$ выполнено $\nu(x)\geqslant 0$. Более того, для достаточно больших N и всех $x\in[\varepsilon_k N, 2\varepsilon_k N]$ выполнено $\nu(x)\geqslant k^{-1}2^{-k-5}\widetilde{\Lambda}(x)$.*

Доказательство. Первое утверждение леммы тривиально. Если число $Wx+1$ не является простым, то второе утверждение леммы также тривиально. Пусть $Wx+1$ – простое, и пусть N таково, что $Wx+1 > R$. Тогда в сумме (121) присутствует только одно слагаемое с $d=1$. Отсюда получаем, что $\Lambda_R(Wx+1)=\log R$ и $\nu(x) = \dfrac{\varphi(W)}{W}\log R \geqslant k^{-1}2^{-k-5}\widetilde{\Lambda}(x)$. Лемма 8 доказана.

Нам осталось доказать, что ν является k-псевдослучайной мерой. Для этого надо проверить, что ν удовлетворяет условию линейных форм и корреляционному условию. Развивая метод работы [105], Грин и Тао доказали два предложения, из которых вытекает справедливость условий (108), (109), (110) для

меры ν. Мы не будем останавливаться на этом подробно, отсылая заинтересованного читателя к статье [24], и просто сформулируем указанные предложения.

Предложение 14. *Пусть m, t – целые положительные числа. Пусть $\psi_i(\mathbf{x}) := \sum_{j=1}^t L_{ij} + b_j$, $i \in [m]$, – линейные формы с целыми коэффициентами L_{ij} такими, что $|L_{ij}| \leqslant \sqrt{w(N)}/2$, $i \in [m]$, $j \in [t]$. Пусть также $\theta_i = W\psi_i + 1$ и $B = \prod_{i=1}^t I_i \subseteq \mathbb{R}^t$, где I_i, $i \in [m]$, – интервалы длины не меньше, чем R^{10m}. Предположим, что функция $w(N)$ возрастает к бесконечности достаточно медленно. Тогда*

$$\frac{1}{|B|}\sum_{\mathbf{x}\in B}\Lambda_R(\theta_1(\mathbf{x}))^2\cdots\Lambda_R(\theta_m(\mathbf{x}))^2 = (1+o_{m,t}(1))\left(\frac{W\log R}{\varphi(W)}\right)^m. \tag{122}$$

Предложение 15. *Пусть $m \geqslant 1$ – целое число и I – интервал длины не меньше, чем R^{10m}. Пусть также $h_1,\dots,h_m$ – различные целые, $|h_i| \leqslant N^2$, $i \in [m]$, и*

$$\Delta := \prod_{1\leqslant i<j\leqslant m}|h_i - h_j|.$$

Предположим, что функция $w(N)$ возрастает к бесконечности достаточно медленно. Тогда

$$\begin{aligned}\frac{1}{|I|}\sum_{x\in I}\Lambda_R(W(x+h_1)+1)^2\cdots\Lambda_R(W(x+h_m)+1)^2 \\ \leqslant (1+o_m(1))\left(\frac{W\log R}{\varphi(W)}\right)^m\prod_{p|\Delta}(1+O_m(p^{-1/2})).\end{aligned} \tag{123}$$

§ 9. Теорема Радо о системах линейных уравнений

В § 2 мы доказали теорему Рота 3, которая утверждает, что любое подмножество $[N]$ без арифметических прогрессий длины три имеет мощность, по порядку не большую, чем $1/\log\log N$. В работе [38] Рот обобщил этот результат.

Пусть $U = (u_{ij})$ есть матрица размера $m \times n$, все элементы которой целые. Множество A называется *$\mathscr{U}$-множеством*, если в A не существует n *различных* элементов $x_1,\dots,x_n$, удовлетворяющих m уравнениям

$$\sum_{j=1}^n u_{ij}x_j = 0, \qquad i = 1,\dots,m. \tag{124}$$

Пусть

$$a_U(N) = \frac{1}{N}\max\{|A| : A \subseteq [N],\ A \in \mathscr{U}\}.$$

В терминах функции $a_U(N)$ результат Рота может быть переформулирован следующим образом. Если U есть (1×3)-матрица $(1,-2,1)$, то $a_U(N) \ll 1/\log\log N$. Возникает вопрос: при каких ограничениях на матрицу U можно утверждать, что $a_U(N) \to 0$ при $N \to \infty$?

Сформулируем основной результат работы [38].

ТЕОРЕМА 44 (Рот). *Пусть матрица U удовлетворяет двум условиям:*
(a) *для всех $i = 1, \dots, m$ выполнено $\sum_{j=1}^{n} u_{ij} = 0$;*
(b) *существует m линейно-независимых столбцов матрицы U, обладающих следующим свойством: если удалить любой из этих столбцов, то оставшиеся $n-1$ столбцов матрицы U можно разбить на два множества, каждое из которых содержит m линейно-независимых столбцов.*

Тогда

$$a_U(N) \ll \frac{1}{(\log\log N)^{1/l^2}}\,.$$

Заметим, что условие (a) теоремы 44 необходимо для того, чтобы $a_U(N) \to 0$ при $N \to \infty$. Действительно, если для некоторого $q \in [n]$ и некоторого $D \in \mathbb{Z}$, $D \neq 0$, выполнено

$$\sum_{j=1}^{n} u_{qj} = D,$$

то все x_j, равные 1 по модулю $|D|+1$, не удовлетворяют q-му уравнению системы (124). Следовательно, $a_U(N) \geqslant 1/(|D|+1) > 0$.

Напротив, второе условие теоремы 44 не является необходимым. Рассмотрим матрицу U размера 2×4,

$$U = \begin{pmatrix} 1 & -2 & 1 & 0 \\ 0 & 1 & -2 & 1 \end{pmatrix}.$$

Тогда матрица U не удовлетворяет второму условию теоремы 44, поскольку из этого условия вытекает, что $n \geqslant 2m+1$. С другой стороны, $a_U(N) = a_4(N)$ и по теореме Семереди $a_4(N) \to 0$ при $N \to \infty$. Мы опишем все матрицы U, для которых выполнено $\lim_{N\to\infty} a_U(N) = 0$, несколько позднее. А сейчас сформулируем интересный результат Р. Радо (см. [39]–[41]).

ОПРЕДЕЛЕНИЕ 18. Пусть $U = (u_{ij})$ – матрица размера $m \times n$, все элементы которой целые. Система уравнений (124) называется *регулярной в* $\mathbb{N}$, если для любой раскраски $\mathbb{N}$ в конечное число цветов найдется монохроматическое решение системы (124).

Заметим, что числа $x_1, \dots, x_n$ не предполагаются различными.

ТЕОРЕМА 45 (Радо). *Пусть $U = (u_{ij})$ – матрица размера $m \times n$, все элементы которой целые. Система уравнений (124) является регулярной в $\mathbb{N}$ тогда и только тогда, когда найдутся столбцы $c_1, \dots, c_n$ и числа k_i, $1 \leqslant k_1 < \dots < k_t = n$, такие, что новые столбцы*

$$A_i = \sum_{j=k_{i-1}+1}^{k_i} C_j$$

удовлетворяют условиям
(a) *A_1 является нулевым столбцом;*
(b) *для $i = 1, \dots, t$ столбец A_i есть линейная комбинация $C_1, \dots, C_{k_{i-1}}$ с рациональными коэффициентами.*

Матрицы, для которых выполнены условия (a) и (b) теоремы 45, будем называть *регулярными*.

В случае, когда $m = 1$, теорема Радо записывается наиболее просто.

Теорема 46 (Радо). *Пусть n – натуральное число и $c_1, \dots, c_n$ – ненулевые целые числа. Система уравнений*

$$c_1x_1 + \dots + c_nx_n = 0 \tag{125}$$

является регулярной в $\mathbb{N}$ тогда и только тогда, когда найдется непустое множество $I \subseteq [n]$ такое, что сумма $\sum_{i\in I} c_i$ равна нулю.

Например, уравнения $x - 2y + z = 0$ и $x + y - z = 0$ являются регулярными, а уравнение $x + y - 5z = 0$ – нет. Если $x - 2y + z = 0$, то числа x, y, z образуют арифметическую прогрессию. Заметим, что для этого уравнения теорема 46 тривиальна, поскольку можно взять $x = y = z = 1$. Теорема Ван дер Вардена 1 для случая $k = 3$ позволяет утверждать, что для всякой раскраски $\mathbb{N}$ в конечное число цветов существуют *различные* x, y, z одного цвета, для которых выполнено $x - 2y + z = 0$. Что касается уравнения $x + y - z = 0$, то существование в любой конечной раскраске $\mathbb{N}$ монохроматического решения этого уравнения было доказано ранее И. Шуром в работе [37].

Мы не будем здесь полностью доказывать теорему 46, ни, тем более, теорему 45. Тем не менее справедливость необходимого условия теоремы 46 установить достаточно просто.

Итак, пусть для любого непустого множества $I \subseteq [n]$ сумма $\sum_{i\in I} c_i$ не равна нулю. Найдем раскраску $\mathbb{N}$ в конечное число цветов, для которой не существует монохроматического решения уравнения (125). Пусть p – простое число, которое будет выбрано позже. Мы раскрасим в $p-1$ цветов множество $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$. Ясно, что это даст нам раскраску и множества $\mathbb{N}$.

Любое $q \in \mathbb{Q}^*$ может быть записано единственным образом в виде

$$q = \frac{p^j a}{b}, \qquad j \in \mathbb{Z}, \quad a \in \mathbb{Z}, \quad b \in \mathbb{N}, \quad p \nmid a, \quad p \nmid b, \quad (a, b) = 1. \tag{126}$$

Если q представлено в виде (126), то раскрасим q в цвет $S_p(q)$, где $S_p(q) = ab^{-1} \pmod p \in \mathbb{Z}_p^*$. Раскраска S_p множества $\mathbb{Q}^*$ в $(p-1)$ цвет обладает следующим свойством: если $S_p(x) = S_p(y)$, то для всех $\alpha \in Q^*$ выполнено $S_p(\alpha x) = S_p(\alpha y)$.

Так как число подмножеств $I \subseteq [n]$ конечно и для всякого непустого $I \subseteq [n]$ выполнено $\sum_{i\in I} c_i \neq 0$, то найдется простое p, для которого $\sum_{i\in I} c_i \neq 0 \pmod p$ для всех $\varnothing \neq I \subseteq [n]$.

Предположим, что $x_1, \dots, x_n \in \mathbb{N}$ – монохроматическое решение (125) для раскраски S_p. Так как для любого $\mu \in \mathbb{Q}^*$ набор $\mu x_1, \dots, \mu x_n$ также будет монохроматическим, то можно считать без ограничения общности, что наибольший общий делитель $x_1, \dots, x_n$ равен единице. Перенумеровав, если это необходимо, числа $x_1, \dots, x_n$, найдем $1 \leqslant s \leqslant n$ такое, что p не делит $x_1, \dots, x_s$ и делит $x_{s+1}, \dots, x_n$. Имеем

$$\sigma = \sum_{j=1}^{n} c_jx_j \equiv \sum_{j=1}^{k} c_jx_j \equiv 0 \pmod p.$$

Так как $x_1, \dots, x_n$ имеют один и тот же цвет, то $x_1 \equiv \dots \equiv x_n \equiv a \pmod p$, где $a \not\equiv 0 \pmod p$. Отсюда

$$\sigma \equiv a \cdot \sum_{j=1}^{k} c_j \equiv 0 \pmod p.$$

Следовательно, $\sum_{j=1}^{k} c_j \equiv 0 \pmod p$. Противоречие.

Скажем несколько слов о результатах, связанных с теоремой 45. В работе [107] был найден аналог теоремы Радо для произвольных абелевых групп. Фюрстенберг [17] доказал теорему Радо с помощью методов эргодической теории. В статьях [108]–[110] были получены результаты, аналогичные теореме 45, для некоторых нелинейных уравнений. Другие результаты, обобщающие теорему Радо, могут быть найдены в [111] и [17].

Теперь мы можем описать все матрицы U, для которых $\lim_{N\to\infty} a_U(N) = 0$. Ясно, что такие матрицы обязаны удовлетворять условию теоремы 45. Кроме того, для них должно быть выполнено первое условие теоремы 44. Оказывается, эти необходимые условия являются и достаточными. Говоря точнее, справедлив следующий результат (см. [42]), вытекающий из теоремы Семереди.

Теорема 47 (Франкл, Грэхем, Рёдл). *Пусть $U = (u_{ij})$ – регулярная матрица размера $m \times n$, все элементы которой целые. Предположим, что система уравнений $U\mathbf{x} = 0$ имеет хотя бы одно решение $\mathbf{x}' = (x'_1, \dots, x'_n)$, все элементы x'_i которого попарно различны. Тогда следующие два утверждения эквивалентны*:

(a) $\sum_{j=1}^{n} u_{ij} = 0$, $i = 1, \dots, m$;

(b) *для любого множества $E \subseteq \mathbb{N}$, $D^*(E) > 0$, система уравнений $U\mathbf{x} = 0$ имеет решение $\mathbf{x} = (x_1, \dots, x_n)$, все элементы x_i которого принадлежат E и попарно различны.*

Доказательство. (1)⇒(2) Пусть $\mathbf{x}' = (x'_1, \dots, x'_n)$ – решение системы уравнений $U\mathbf{x}' = 0$, все элементы x'_i которого попарно различны. Пусть $N = \max x'_i$. Так как множество X имеет положительную верхнюю плотность, то по теореме Семереди в X существует арифметическая прогрессия длины N. Пусть $c + jd$ – элементы этой прогрессии, $j = 0, 1, \dots, N$. Пусть также $\mathbf{y} = c \cdot \mathbf{1} + d \cdot \mathbf{x}'$, где $\mathbf{1} = (1, \dots, 1)$. Применяя свойство (a), получаем $A\mathbf{y} = 0$. Так как $N = \max x'_i$, то все компоненты вектора $\mathbf{y}$ принадлежат множеству X, что и требовалось.

(2)⇒(1) Пусть N – натуральное число такое, что $N > \sum_{i,j} |a_{ij}|$. Пусть также $X = \{Ny + 1 : y \in \mathbb{N}\}$. Тогда верхняя плотность множества X равна $1/N$. Пусть $\mathbf{x} = (x_1, \dots, x_n) \in X$ – решение системы уравнений $U\mathbf{x} = 0$. Тогда для некоторых $y_i \in \mathbb{N}$ выполнено $x_i = Ny_i + 1$ и

$$0 = \sum_{j=1}^{n} u_{ij} x_j = N\left(\sum_{j=1}^{n} u_{ij} y_j\right) + \sum_{j=1}^{n} u_{ij}. \tag{127}$$

Из равенства (127) следует, что $\sum_{j=1}^{n} u_{ij} = 0$ для всех $i = 1, \dots, m$. Действительно, если для некоторого $i \in [m]$ выполнено $\sum_{j=1}^{n} u_{ij} y_j = 0$, то и $\sum_{j=1}^{n} u_{ij} = 0$. Если же для этого i имеем $\sum_{j=1}^{n} u_{ij} y_j \neq 0$, то из-за выбора N снова $\sum_{j=1}^{n} u_{ij} = 0$. Теорема 47 доказана.

§ 10. Другие результаты об арифметических прогрессиях

Задачи, которыми мы занимались до сих пор, можно описать следующим образом. Пусть некоторое множество A содержится в некотором "базовом" множестве B и имеет достаточно большую плотность относительно B. Тогда множество A содержит набор точек $x_1, \dots, x_m$, обладающий некоторыми наперед заданными свойствами.

При этом в качестве B выступало множество целых чисел (теорема Семереди), отрезок $[N]$ (теорема Рота), двумерная решетка $[N]^2$ или $\mathbb{Z}_2^n \times \mathbb{Z}_2^n$ (теоремы 36 и 37), простые числа (теорема 10) и другие множества. В качестве же свойств, которым должен удовлетворять набор точек $x_1, \dots, x_m$ из A, мы, в основном, рассматривали свойство точек образовывать арифметическую прогрессию той или иной длины, либо же образовывать уголок (теоремы 36 и 37), либо удовлетворять системе линейных уравнений (теоремы 44, 45 и 47).

В этом параграфе мы рассмотрим задачи об арифметических прогрессиях, не вписывающиеся в указанную схему, а именно задачи о *критических множествах*, вопросы, связанные с арифметическими прогрессиями в *суммах*, и, наконец, теоремы о *радугах*.

В работах [62], [112] Э. Крут изучал вопрос о структуре критических множеств в $\mathbb{Z}_p$ без арифметических прогрессий длины три. Пусть $\rho > 0$ – вещественное число. Множество $C \subseteq \mathbb{Z}_p$ мощности не меньше, чем ρp, называется *ρ-критическим*, если C содержит наименьшее число арифметических прогрессий длины три среди всех множеств, имеющих мощность не меньше, чем ρp. В [62] Крут доказал, что критические множества имеют сильную аддитивную структуру. Его теорема опирается на известную гипотезу о простых числах.

Гипотеза 4. *Для всех $\theta > 0$ и для всех достаточно больших x отрезок $[x, x + x^\theta]$ содержит простое число.*

В настоящий момент гипотеза 4 доказана для всех $\theta > 0.525$ (см. [113]).

Теорема 48 (Крут). *Пусть $\rho_0 \in (0, 1)$. Существуют числа $\rho \in (0, \rho_0)$ и $d \in (0, 1)$, а также бесконечно много простых p такие, что для всякого ρ-критического множества $C \subseteq \mathbb{Z}_p$ существует b, $1 \leqslant b \leqslant p - 1$, для которого выполнено*

$$|C \cap (C + bj)| \geqslant |C| \left(1 - \frac{K}{|\log \rho|}\right), \qquad j = 0, 1, \dots, p^d,$$

где $K > 0$ – абсолютная константа.

Результат Крута можно переформулировать следующим образом. Если C – ρ-критическое множество, то $C \approx A + B$, где $B = \{0, b, 2b, \dots, [p^d]b\}$. Здесь знак $\approx$ означает, что мощность симметрической разности $S \triangle (A + B)$ не превосходит $O(|C| \log^{-1}(1/\rho))$. Следовательно, чем меньше ρ, тем ближе становится C к сумме $A + B$. Заметим, что множество, построенное в теореме 20 из § 4, как раз имеет вид $A + B$, где B – некоторая арифметическая прогрессия.

В статье [112] Крут получил безусловный результат о структуре критических множеств.

Теорема 49 (Крут). *Пусть $\rho \in (0,1)$ и p – достаточно большое натуральное число. Тогда всякое ρ-критическое множество $C \subseteq \mathbb{Z}_p$ содержит арифметическую прогрессию длины не меньше, чем $\log^{1/4+o(1)} p$.*

Теперь рассмотрим задачи об арифметических прогрессиях в суммах, т.е. в множествах вида $A_1 + A_2 + \cdots + A_k$. Оказывается, такие множества содержат на удивление длинные арифметические прогрессии. В последнее время появилось много работ по этой тематике, см., например, [114]–[126]. Мы не можем даже упомянуть все имеющиеся здесь результаты, а коснемся лишь некоторых из них. В работе [114] Ж. Бургейн получил следующий результат.

Теорема 50 (Бургейн). *Пусть $A, B \subseteq [N]$ – некоторые множества, причем $|A| = \gamma N$, $|B| = \delta N$. Тогда существует абсолютная константа $c > 0$ такая, что множество $A + B$ содержит арифметическую прогрессию длины не меньше, чем $\exp(c(\gamma\delta \log N)^{1/3} - \log\log N)$.*

С другой стороны, И. Ружа нашел нижнюю оценку для длины максимальной арифметической прогрессии в множестве $A + A$ (см. [115]).

Теорема 51 (Ружа). *Пусть $\varepsilon > 0$ – произвольное число. Тогда найдется число $p_0(\varepsilon)$ такое, что для всех простых p, $p > p_0(\varepsilon)$, существует симметричное (т.е. $A = -A$) множество $A \subseteq \mathbb{Z}_p$, $|A| > (1/2 - \varepsilon)p$, такое, что $A + A$ не содержит арифметических прогрессий, длины которых больше, чем $\exp((\log p)^{2/3+\varepsilon})$.*

Так как для любого множества $A \subseteq \mathbb{Z}_p$, $|A| \geqslant p/2$, выполнено $A + A = \mathbb{Z}_p$, то константа $1/2$ в теореме 51 является неулучшаемой. Сравним теоремы 50 и 51. Предположим, что параметры γ и δ в теореме 50 не зависят от N. Тогда по этой теореме для любого A множество $A + A$ содержит арифметическую прогрессию длины не меньше, чем $\exp(c(\log N)^{1/3})$, где c – некоторая константа. С другой стороны, по теореме 51 найдется A такое, что $A + A$ не содержит прогрессий длины больше, чем $\exp(c(\log N)^{2/3})$. Как мы видим, оценки в теоремах Бургейна и Ружи достаточно близки.

В работе [117] Г. А. Фрейман, Х. Хальберстам и И. Ружа рассмотрели вопрос об арифметических прогрессиях в множествах вида $A + A + A$ и доказали следующий результат (см. также [118]).

Теорема 52 (Фрейман, Хальберстам, Ружа). *Пусть N – натуральное число, $\delta > 0$ и $A \subseteq \mathbb{Z}_N$ – произвольное множество мощности δN. Тогда множество $A + A + A$ содержит арифметическую прогрессию длины не меньше, чем $c\delta N^{C\delta^3}$, где $c, C > 0$ – абсолютные константы.*

В той же статье три названных автора доказали теорему, аналогичную теореме 51, а именно, они построили множество $A \subseteq \mathbb{Z}_N$ такое, что $A + A + A$ не содержит арифметических прогрессий, длины которых больше, чем $2N^{\log(1/\delta)}$.

В работе [116] Б. Грин улучшил обе теоремы 50 и 52.

Теорема 53 (Грин). *Пусть $A, B \subseteq [N]$ – некоторые множества, причем $|A| = \gamma N$, $|B| = \delta N$. Тогда существует абсолютная константа $C > 0$ такая, что множество $A + B$ содержит арифметическую прогрессию длины не меньше, чем $\exp(C(\gamma\delta \log N)^{1/2} - \log\log N)$.*

Теорема 54 (Грин). *Пусть N – натуральное число, $\delta > 0$ и $A \subseteq \mathbb{Z}_N$ – произвольное множество мощности δN. Тогда множество $A + A + A$ содержит арифметическую прогрессию длины не меньше, чем $2^{-24}\delta^5(\log(1/\delta))^{-2}N^{\delta^2/(250\log(1/\delta))}$.*

В последней части этого параграфа мы рассмотрим вопросы, связанные с арифметическими прогрессиями в радугах.

Пусть $c\colon \mathbb{N} \to \{R, G, B\}$ – произвольная раскраска множества натуральных чисел в цвета R, G и B. Из теоремы Ван дер Вардена вытекает, что для любой такой раскраски $\mathbb{N}$ существует монохроматическая арифметическая прогрессия длины три. Возникает вопрос: можно ли утверждать, что для произвольной раскраски c всегда найдется арифметическая прогрессия, все элементы которой раскрашены в разные цвета? Вопросы такого рода называются *антирамсеевскими* (см. первую работу по этой тематике [127], а также [128]). Как мы увидим чуть позже, вообще говоря, ответ на поставленный выше вопрос отрицательный. Тем не менее, в работе [129] был получен следующий результат (см. также [130], [131]).

Арифметическая прогрессия, составленная из чисел a_1, a_2, a_3, называется *радугой*, если $c(a_i) \neq c(a_j)$ для всех $i \neq j$. Определим множества $R_c(n) := [n] \cap \{i : c(i) = R\}$ и, аналогично, $G_c(n)$, $B_c(n)$.

Теорема 55 [129]. *Пусть c – произвольная раскраска $\mathbb{N}$. Пусть также*

$$\limsup_{n\to\infty}(\min\{|R_c(n)|, |G_c(n)|, |B_c(n)|\} - n/6) = +\infty. \tag{128}$$

Тогда в раскраске c существует радуга.

Вместо раскраски натурального ряда можно рассматривать раскраску множества вычетов $\mathbb{Z}_n$. Радугой в $\mathbb{Z}_n$ называются вычеты a_1, a_2, a_3, раскрашенные в три разных цвета, такие, что $a_1 + a_2 \equiv 2a_3 \pmod n$. Из теоремы 55 вытекает следствие.

Следствие 4. *Пусть n – натуральное число и c – произвольная раскраска $\mathbb{Z}_n$. Пусть также $R_c = \{i : c(i) = R\}$, $G_c = \{i : c(i) = G\}$ и $B_c = \{i : c(i) = B\}$. Если $\min(|R_c|, |G_c|, |B_c|) > n/6$, то раскраска c содержит радугу.*

Действительно, пусть c – произвольная раскраска $\mathbb{Z}_n$. Рассмотрим раскраску $\overline{c}$ множества $\mathbb{N}$ такую, что $\overline{c}(i) := c(i \pmod n)$. По условию $\min(|R_c|, |G_c|, |B_c|) > n/6$. Отсюда

$$\limsup_{n\to\infty}(\min\{|R_c(n)|, |G_c(n)|, |B_c(n)|\} - n/6) = +\infty.$$

Применяя теорему 55, находим радугу в $\overline{c}$, что дает нам радугу в c.

Следующее предложение показывает, что константа $1/6$ в неравенстве (128) не может быть заменена ни на какую меньшую.

Предложение 16. *Существует раскраска c множества $\mathbb{N}$ такая, что для всех $n \in \mathbb{N}$ выполнено*

$$\min\{|R_c(n)|, |G_c(n)|, |B_c(n)|\} = [(n+2)/6].$$

Доказательство. Рассмотрим раскраску c множества $\mathbb{N}$:

$$c(i) = \begin{cases} R, & \text{если } i \equiv 1 \pmod 6, \\ G, & \text{если } i \equiv 4 \pmod 6, \\ B & \text{иначе.} \end{cases} \tag{129}$$

Легко видеть, что c не содержит радуг и для всех n выполнено

$$\min\{|R_c(n)|, |G_c(n)|, |B_c(n)|\} = |G_c(n)| = [(n+2)/6].$$

§ 11. Заключение

Мы заканчиваем настоящий обзор формулировкой нескольких нерешенных проблем, связанных с теоремой Семереди и задачами об арифметических прогрессиях. Часть из этих проблем уже была сформулирована в предыдущих параграфах.

Наиболее сложной нерешенной задачей остается гипотеза Эрдёша–Турана 2. Как было показано в § 5, эта гипотеза тесно связана с проблемой изучения поведения функции $a_k(N)$. Заметим, что даже в простейшем случае $k = 3$ точный порядок роста $a_3(N)$ до сих пор остается неизвестным. Недавно Грин и Тао анонсировали результат о верхней оценке величины $a_k(N)$, $k \geqslant 4$, вида $a_k(N) \ll 1/(\log N)^{C_k}$, $C_k > 0$ – абсолютная константа, и доказали аналогичный результат для функции $a_4(N)$ в группах $\mathbb{Z}_p^n$, где p – простое, $p \neq 2, 3$ (см. [33]).

Другая возникающая задача состоит в получении количественного варианта теоремы Бергельсона–Лейбмана 8. Эта теорема может быть переформулирована на языке теории чисел следующим образом.

Теорема 56 (Бергельсон, Лейбман). *Пусть $\delta > 0$ – действительное число. Пусть также $p_1, p_2, \dots, p_k$ – многочлены такие, что $p_i(\mathbb{N}) \subseteq \mathbb{N}$ и $p_i(0) = 0$, $i = 1, \dots, k$. Тогда существует натуральное $N(\delta, p_1, \dots, p_k)$ такое, что для любого множества $A \subseteq [N]$, $|A| \geqslant \delta N$, найдутся натуральные числа a, d такие, что все числа $a + p_i(d)$, $i = 1, \dots, k$, принадлежат множеству A.*

Под словами “количественный вариант теоремы 56” мы понимаем результат, в котором устанавливается явная верхняя оценка величины $N(\delta, p_1, \dots, p_k)$.

Если $k = 2$ и $p_1(n) \equiv 0$ и $p_2(n) = n^2$, то количественный аналог теоремы Бергельсона–Лейбмана известен (см. теорему 30). Тем не менее действительный порядок роста функции $N(\delta, p_1, p_2)$ не найден даже в этом простом случае. Это дает возможность сформулировать следующий вопрос.

Вопрос. *Пусть $\varepsilon > 0$ и $N > N_0(\varepsilon)$ – достаточно большое натуральное число. Существует ли множество $A \subseteq [N]$, $|A| > N^{1-\varepsilon}$, такое, что $A - A$ не содержит ненулевых квадратов?*

В работе [132] Ружа показал, что если $\varepsilon = 0.267$, то существует множество $A \subseteq [N]$, $|A| > N^{1-\varepsilon}$, такое, что разность двух любых элементов из A не является ненулевым квадратом.

В связи с теоремами 34–36 возникает вопрос о получении многомерных количественных аналогов теорем об уголках, а также количественной версии теоремы Холса–Джуита 31. Очень интересен вопрос о получении аналога теоремы 56 в случае, если A есть множество простых чисел.

Автор выражает глубокую благодарность доктору физико-математических наук Н. Г. Мощевитину за постоянное внимание к работе, а также М. Г. Рюминой за гостеприимство.

Список литературы

[1] B. L. Van der Waerden, "Beweis einer Baudetschen Vermutung", *Nieuw Arch. Wisk.*, **15** (1927), 212–216.

[2] А. Я. Хинчин, *Три жемчужины теории чисел*, УРСС, М., 2004.

[3] Р. Грэхем, *Начала теории Рамсея*, М., Мир, 1984.

[4] R. L. Graham, B. L. Rothschild, J. H. Spencer, *Ramsey theory*, Wiley, New York, 1980.

[5] В. А. Успенский, *Лекции о вычислимых функциях*, Физматгиз, М., 1960.

[6] S. Shelah, "Primitive recursive bounds for van der Waerden numbers", *J. Amer. Math. Soc.*, **1**:3 (1988), 683–697.

[7] K. F. Roth, "On certain sets of integers", *J. London Math. Soc.*, **28** (1953), 104–109.

[8] E. Szemerédi, "Integer sets containing no arithmetic progressions", *Acta Math. Hungar.*, **56**:1–2 (1990), 155–158.

[9] D. R. Heath-Brown, "Integer sets containing no arithmetic progressions", *J. London Math. Soc.* (2), **35**:3 (1987), 385–394.

[10] J. Bourgain, "On triples in arithmetic progression", *Geom. Funct. Anal.*, **9**:5 (1999), 968–984.

[11] J. Bourgain, "A Szemerédi type theorem for sets of positive density in $\mathbb{R}^k$", *Israel J. Math.*, **54**:3 (1986), 307–316.

[12] I. Z. Ruzsa, E. Szemerédi, "Triple systems with no six points carrying three triangles", *Combinatorics*, Proceedings of the Fifth Hungarian colloquium (Keszthely, 1976), Colloq. Math. Soc. János Bolyai, **18**, North-Holland, Amsterdam, 1978, 939–945.

[13] E. Szemerédi, "On sets of integers containing no four elements in arithmetic progression", *Acta Math. Acad. Sci. Hungar.*, **20**:1–2 (1969), 89–104.

[14] E. Szemerédi, "On sets of integers containing no k elements in arithmetic progression", *Acta Arith.*, **27** (1975), 199–245.

[15] H. Furstenberg, "Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions", *J. Anal. Math.*, **31** (1977), 204–256.

[16] H. Furstenberg, Y. Katznelson, D. Ornstein, "The ergodic theoretical proof of Szemerédi's theorem", *Bull. Amer. Math. Soc.* (*N.S.*), **7**:3 (1982), 527–552.

[17] H. Furstenberg, *Recurrence in ergodic theory and combinatorial number theory*, M. B. Porter Lectures, Princeton Univ. Press, Princeton, NJ, 1981.

[18] H. Furstenberg, Y. Katznelson, "An ergodic Szemerédi theorem for commuting transformations", *J. Anal. Math.*, **34** (1978/1979), 275–291.

[19] V. Bergelson, A. Leibman, "Polynomial extentions of van der Waerden's and Szemerédi's theorems", *J. Amer. Math. Soc.*, **9**:3 (1996), 725–753.

[20] H. Furstenberg, Y. Katznelson, "A density version of the Hales–Jewett theorem", *J. Anal. Math.*, **57** (1991), 64–119.

[21] A. Leibman, "Multiple recurrence theorem for measure preserving actions of a nilpotent group", *Geom. Funct. Anal.*, **8**:5 (1998), 853–931.

[22] W. T. Gowers, "A new proof of Szemerédi's theorem", *Geom. Funct. Anal.*, **11**:3 (2001), 465–588.

[23] W. T. Gowers, "A new proof of Szemerédi's theorem for arithmetic progressions of length four", *Geom. Funct. Anal.*, **8**:3 (1998), 529–551.

[24] B. Green, T. Tao, "The primes contain arbitrarily long arithmetic progressions", *Ann. of Math.* (в печати); arXiv: math.NT/0404188.

[25] B. Green, "On arithmetic structures in dense sets of integers", *Duke Math. J.*, **144**:2 (2002), 215–238.

[26] J. Bourgain, M.-C. Chang, "Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_Q^*$, where Q is composite with few prime factors", *Geom. Funct. Anal.*, **16**:2 (2006), 327–366.

[27] J. Bourgain, A. A. Glibichuk, S. V. Konyagin, "Estimates for the number of sums and products and for exponential sums in fields of prime order", *J. London Math. Soc.* (2), **73**:2 (2006), 380–398.

[28] И. Д. Шкредов, "Об одной задаче Гауэрса", *Докл. РАН*, **400**:2 (2005), 169–172.

[29] И. Д. Шкредов, "Об одной задаче Гауэрса", *Изв. РАН. Сер. матем.*, **70**:2 (2006), 179–221.

[30] И. Д. Шкредов, "Об одном обобщении теоремы Семереди", *Докл. РАН*, **405**:3 (2005), 315–319.

[31] I. D. Shkredov, *On a Generalization of Szemerédi's Theorem*, arXiv: math.NT/0503639.

[32] B. Green, T. Tao, *An inverse theorem for the Gowers U^3 norm*, arXiv: math.NT/0503014.

[33] B. Green, T. Tao, *New bounds for Szemerédi's Theorem. I: Progressions of length* 4 *in finite field geometries*, arXiv: math.CO/0509560.

[34] B. Green, "Roth's theorem in the primes", *Ann. of Math.* (2), **161**:3 (2005), 1609–1636.

[35] А. А. Бухштаб, *Теория чисел*, Просвещение, М., 1966.

[36] И. М. Виноградов, *Основы теории чисел*, Лань, СПб., 2004.

[37] I. Schur, *Jahresber. Deutsch. Math.-Verein.*, **25**:4–6 (1916), 114–117.

[38] K. F. Roth, "On certain sets of integers, II", *J. London Math. Soc.*, **29** (1954), 20–26.

[39] R. Rado, "Verallgemeinerung eines Satzes von van der Waerden mit Anwendungen auf ein Problem der Zahlentheorie", *Sitz. Preuß. Akad. Wiss. Phys.-Math. Kl.*, **17** (1933), 589–596.

[40] R. Rado, "Studien zur Kombinatorik", *Math. Z.*, **36**:1 (1933), 424–470.

[41] R. Rado, "Some recent results in combinatorial analysis", *Comptes Rendus du Congrès International des Mathématiciens*, vol. 2 (Oslo, 1936), 1937, 20–21.

[42] P. Frankl, R. L. Graham, V. Rödl, "Quantitative theorems for regular systems of equations", *J. Combin. Theory Ser. A*, **47**:2 (1988), 246–261.

[43] T. Tao, *A quantitative ergodic theory proof of Szemerédi's theorem*, arXiv: math.CO/0405251.

[44] N. Alon, J. H. Spencer, *The probabilistic method*, Wiley, New York, 1992.

[45] F. A. Behrend, "On sets of integers which contain no three terms in arithmetic progression", *Proc. Natl. Acad. Sci. USA*, **32** (1946), 331–332.

[46] R. Salem, D. C. Spencer, *Proc. Natl. Acad. Sci. USA*, **28** (1942), 561–563.

[47] R. Salem, D. C. Spencer, "On sets which do not contain a given number of terms in arithmetical progression", *Nieuw Arch. Wisk.* (2), **23** (1950), 133–143.

[48] I. Laba, M. T. Lacey, *On sets of integers not containing long arithmetic progressions*, arXiv: math.CO/0108155.

[49] R. A. Rankin, "Sets of integers containing not more than a given number of terms in arithmetic progression", *Proc. Roy. Soc. Edinburgh Sect. A*, **65**:4 (1960/1961), 332–344.

[50] R. A. Rankin, "Representations of a number af the sum of a large number os squares", *Proc. Roy. Soc. Edinburgh Sect. A*, **65**:4 (1960/1961), 318–331.

[51] P. Erdös, P. Turán, "On some sequences of integers", *J. London Math. Soc.*, **11** (1936), 261–264.

[52] L. Moser, "On non-averaging sets of integers", *Canadian J. Math.*, **5** (1953), 245–252.
[53] W. T. Gowers, "Lower bounds of tower type for Szemerédi's uniformity lemma", *Geom. Funct. Anal.*, **7**:2 (1997), 322–337.
[54] E. Szemerédi, "Regular partitions of graphs", *Problèmes combinatoires et théorie des graphes* (Orsay, 1976), Colloq. Internat. CNRS, **260**, CNRS, Paris, 1978, 399–401.
[55] J. Komlós, M. Simonovits, "Szemerédi's regularity lemma and its applications in graph theory", *Combinatorics*, Paul Erdös is eighty (Keszthely, 1993), Bolyadi Soc. Math. Stud., **2**, eds. D. Miklós, V. T. Sós, T. Szönyi, János Bolyai Math. Soc., Budapest, 1996, 295–352.
[56] Y. Kohayakawa, "Szemerédi's regularity lemma for sparse graphs", *Foundations of computational mathematics* (Rio de Janeiro), Springer-Verlag, Berlin, 1997, 216–230.
[57] R. L. Graham, V. Rödl, "Numbers in Ramsey theory", *Surveys in combinatorics* (New Cross, 1987), London Math. Soc. Lecture Note Ser., **123**, Cambridge Univ. Press, Cambridge, 1987, 111–153.
[58] B. Nagle, V. Rödl, M. Schacht, "The counting lemma for regular k-uniform hypergraphs", *Random Structures Algorithms*, **28**:2 (2006), 113–179.
[59] W. T. Gowers, "Quasirandomness, counting and regularity for 3-uniform hypergraphs", *Combin. Probab. Comput.*, **15**:1–2 (2006), 143–184.
[60] W. T. Gowers, *Hypergraph regularity and the multidimensional Szemerédi theorem*, `http://www.dpmms.cam.ac.uk/~wtg10/papers.html`.
[61] P. Varnavides, "On certain sets of positive density", *J. London Math. Soc.*, **34** (1959), 358–360.
[62] E. Croot, *A structure theorem for positive density sets having the minimal number of* 3*-term arithmetic progressions*, `arXiv: math.NT/0305318`.
[63] A. Samorodnitsky, L. Trevisan, *Gowers uniformity, influence of variables, and PCPs*, `arXiv: math.CO/0510264`.
[64] Г. А. Фрейман, *Начала структурной теории сложения множеств*, Казань, 1966.
[65] Y. Bilu, "Structure of sets with small sumset", *Structure theory of sets addition*, Astérisque, **258**, 1999, 77–108.
[66] I. Ruzsa, "Generalized arithmetic progressions and sumsets", *Acta Math. Hungar.*, **65**:4 (1994), 379–388.
[67] M.-C. Chang, "A polynomial bound in Freiman's theorem", *Duke Math. J.*, **113**:3 (2002), 399–419.
[68] S. L. G. Choi, "On arithmetic progressions in sequences", *J. London Math. Soc.* (2), **10**:4 (1975), 427–430.
[69] А. Пуанкаре, "Новые методы небесной механики", *Избранные труды*, т. 2, Наука, М., 1972.
[70] А. Б. Каток, Б. Хасселблат, *Введение в современную теорию динамических систем*, Факториал, М., 1999.
[71] V. Bergelson, A. Leibman, "Set-polynomials and polynomial extension of the Hales–Jewett theorem", *Ann. of Math.* (2), **150**:1 (1999), 33–75.
[72] A. Sárcözy, "On difference sets of sequences of integers, I", *Acta Math. Acad. Sci. Hungar.*, **31**:1–2 (1978), 125–149.
[73] A. Sárközy, "On difference sets of sequences of integers, III", *Acta Math. Acad. Sci. Hungar.*, **31**:3–4 (1978), 355–386.
[74] S. Srinivasan, "On a result of Sárközy and Furstenberg", *Nieuw. Arch. Wisk.* (4), **3**:3 (1985), 275–280.
[75] J. Pintz, W. L. Steiger, E. Szemerédi, "On sets of natural numbers whose difference set contains no squares", *J. London Math. Soc.* (2), **37**:2 (1988), 219–231.
[76] A. W. Hales, R. I. Jewett, "Regularity and positional games", *Trans. Amer. Math. Soc.*, **106**:2 (1963), 222–229.

[77] R. McCutcheon, *Elemental methods in ergodic Ramsey theory*, Lecture Notes in Math., **1722**, Springer-Verlag, Berlin, 1999.

[78] M. D. Boshernitzan, "Quantitative recurrence results", *Invent. Math.*, **113**:3 (1993), 617–631.

[79] Н. Г. Мощевитин, "Об одной теореме Пуанкаре", *УМН*, **53**:1 (1998), 223–224.

[80] И. Д. Шкредов, "О возвращаемости в среднем", *Матем. заметки*, **72**:4 (2002), 625–632.

[81] I. D. Shkredov, *On multiple recurrence*, `arXiv: math.DS/0406413`.

[82] V. Afraimovich, J. R. Chazottes, B. Saussol, "Pointwise dimensions for Poincaré recurrence associated with maps and special flows", *Discrete Contin. Dyn. Syst.*, **9**:2 (2003), 263–280.

[83] L. Barreira, Y. Pesin, J. Schmeling, "Dimension and product structure of hyperbolic measures", *Ann. of Math.* (2), **149**:3 (1999), 755–783.

[84] L. Barreira, B. Saussol, "Hausdorff dimension of measures via Poincaré recurrence", *Comm. Math. Phys.*, **219**:2 (2001), 443–463.

[85] L. Barreira, B. Saussol, "Product structure of Poincaré recurrence", *Ergodic Theory Dynam. Systems*, **22**:1 (2002), 33–61.

[86] B. Saussol, S. Troubetzkoy, S. Vaienti, "Recurrence, dimensions, and Lyapunov exponents", *J. Statist. Phys.*, **106**:3–4 (2002), 623–634.

[87] И. Д. Шкредов, "О динамических системах с медленной скоростью возвращения", *Матем. сб.*, **197**:11 (2006), 143–158.

[88] M. Ajtai, E. Szemerédi, "Sets of lattice points that form no squares", *Studia Sci. Math. Hungar.*, **9** (1974/1975), 9–11.

[89] V. H. Vu, "On a question of Gowers", *Ann. Combin.*, **6**:2 (2002), 229–233.

[90] J. Solymosi, "Note on a generalization of Roth's theorem", *Discrete and computational geometry*, Algorithms Combin., **25**, Springer, Berlin, 2003, 825–827.

[91] G. N. Sárcözy, S. Selkow, *On a question of Gowers concerning isosceles right-angle triangles*, `http://citeseer.ist.psu.edu/569945.html`, 2003.

[92] B. Green, "Finite field models in additive combinatorics", *Surveys in combinatorics 2005*, London Math. Soc. Lecture Note Ser., **327**, Cambridge Univ. Press, Cambridge, 2005, 1–27.

[93] F. R. K. Chung, R. L. Graham, R. M. Wilson, "Quasi-random graphs", *Combinatorica*, **9**:4 (1989), 345–362.

[94] F. R. K. Chung, R. L. Graham, "Quasi-random subsets of Z_n", *J. Combin. Theory Ser. A*, **61**:1 (1992), 64–86.

[95] В. И. Богачев, *Основы теории меры*, т. 1, 2, НИЦ "Регулярная и хаотическая динамика", М., Ижевск, 2003.

[96] L. E. Dickson, *History of the theory of numbers*, vol. III, Carnegie Inst. of Washington, Washington, DC, 1919, 1920, 1923.

[97] Н. Г. Чудаков, "О плотности совокупности четных чисел, непредставимых как сумма двух нечетных простых", *Изв. АН СССР. Сер. матем.*, 1938, № 1, 25–40.

[98] J. G. van der Corput, "Über Summen von Primzahlen und Primzahlquadraten", *Math. Ann.*, **116**:1 (1939), 1–50.

[99] S. Chowla, "There exists an infinity of 3-combinations of primes in A.P.", *Proc. Lahore Philos. Soc.*, **6**:2 (1944), 15–16.

[100] P. A. Pritchard, A. Moran, A. Thyssen, "Twenty-two primes in arithmetic progression", *Math. Comp.*, **64**:211 (1995), 1337–1339.

[101] M. Frind, P. Jobling, P. Underwood, 23 *primes in arithmetic progression*, `http://primes.plentyoffish.com`.

[102] B. Host, B. Kra, "Nonconventional ergodic averages and nilmanifolds", *Ann. of Math.* (2), **161**:1 (2005), 397–488.

[103] D. A. Goldston, C. Y. Yildirim, "Higher correlations of divisor sums related to primes. I: Triple correlations", *Integers*, **3** (2003), paper A5.
[104] D. Goldston, C. Y. Yildirim, *Higher correlations of divisor sums related to primes, III: k-correlations*, arXiv: math.NT/0209102.
[105] D. A. Goldston, Y. Motohashi, J. Pintz, C. Y. Yildirim, "Small gaps between primes", *Proc. Japan Acad. Ser. A Math. Sci.*, **82**:4 (2006), 61–65.
[106] G. H. Hardy, E. M. Wright, *An introduction to the theory of numbers*, Clarendon Press, Oxford, 1960.
[107] W. Deuber, "Partitions theorems for Abelian groups", *J. Combin. Theory Ser. A*, **19**:1 (1975), 95–108.
[108] S. D. Adhikari, "A note on a question of Erdös", *Exposition. Math.*, **15**:4 (1997), 367–371.
[109] T. C. Brown, V. Rödl, "Monochromatic solutions to equations with unit fractions", *Bull. Austral. Math. Soc.*, **43**:3 (1991), 387–392.
[110] H. Lefmann, "On partition regular systems of equations", *J. Combin. Theory Ser. A*, **58**:1 (1991), 35–53.
[111] W. Deuber, "Partitionen und lineare Gleichungssysteme", *Math. Z.*, **133**:2 (1973), 109–123.
[112] E. Croot, "Long arithmetic progressions in critical sets", *J. Combin. Theory Ser. A*, **113**:1 (2006), 53–66; arXiv: math.NT/0403082.
[113] R. C. Baker, G. Harman, J. Pintz, "The difference between consecutive primes, II", *Proc. London Math. Soc.* (3), **83**:3 (2001), 532–562.
[114] J. Bourgain, "On aritmetic progressions in sums of sets of integers", *A Tribute of Paul Erdös*, Cambridge Univ. Press, Cambridge, 1990, 105–109.
[115] I. Z. Ruzsa, "Arithmetic progressions in sumsets", *Acta Arith.*, **60**:2 (1991), 191–202.
[116] B. Green, "Arithmetic progressions in sumsets", *Geom. Funct. Anal.*, **12**:3 (2002), 584–597.
[117] G. A. Freiman, H. Halberstam, I. Z. Ruzsa, "Integer sum sets containing long arithmetic progressions", *J. London Math. Soc.* (2), **46**:2 (1992), 193–201.
[118] I. Z. Ruzsa, "Arithmetical progressions and the number of sums", *Period. Math. Hungar.*, **25**:1 (1992), 105–111.
[119] A. Sárközy, "Finite addition theorems, I", *J. Number Theory*, **32**:1 (1989), 114–130.
[120] A. Sárközy, "Finite addition theorems, II", *J. Number Theory*, **48**:2 (1994), 197–218.
[121] A. Sárközy, "Finite addition theorems, III", Groupe de travail en théorie analytique et élémentaire des nombres, 1989–1990, *Publ. Math. Orsay*, **92-01** (1992), 105–122.
[122] V. F. Lev, "Optimal representations by sumsets and subset sums", *J. Number Theory*, **62**:1 (1997), 127–143.
[123] V. F. Lev, "Blocks and progressions in subset sums sets", *Acta Arith.*, **106**:2 (2003), 123–142.
[124] E. Szemerédi, V. H. Vu, "Long arithmetic progressions in sum-sets and the number of x-sum-free sets", *Proc. London Math. Soc.* (3), **90**:2 (2005), 273–296.
[125] E. Szemerédi, V. H. Vu, "Finite and infinite arithmetic progressions in sumsets", *Ann. of Math.* (2), **163**:1 (2006), 1–35.
[126] J. Solymosi, "Arithmetic progressions in sets with small sumsets", *Combin. Probab. Comput.*, **15**:4 (2006), 597–603.
[127] P. Erdös, P. Turán, "On a problem of Sidon in additive number theory, and on some related problems", *J. London Math. Soc.*, **16** (1941), 212–215.
[128] T. Jiang, "Anti-Ramsey numbers of subdivided graphs", *J. Combin. Theory Ser. B*, **85**:2 (2002), 361–366.
[129] V. Jungić, J. Licht, M. Mahdian, J. Nešetřil, R. Radoičić, "Rainbow arithmetic progressions and anti-Ramsey results", *Combin. Probab. Comput.*, **12**:5–6 (2003), 599–620.

[130] V. Jungić, R. Radoičić, "Rainbow 3-term arithmetic progressions", *Integers*, **3** (2003), paper A18.

[131] M. Axenovich, D. Fon-Der-Flaass, "On rainbow arithmetic progressions", *Electron. J. Combin.*, **11**:1 (2004), Research paper 1.

[132] I. Z. Ruzsa, "Difference sets without squares", *Period. Math. Hungar.*, **15**:3 (1984), 205–209.

И. Д. Шкредов (I. D. Shkredov)
Московский государственный университет
им. М. В. Ломоносова
E-mail: ishkredov@rambler.ru

Поступила в редакцию
27.03.2006