Великие потрясения: о теории чисел в XXI веке

С.В. Конягин, И.Д. Шкредов

2016 год, октябрь, Москва

Теорема Грина–Тао о прогрессиях

Верхней плотностью множества $A \subseteq \mathbf{N}$ называется величина

$$D^*(A) := \limsup_{N\to\infty} \frac{|A \cap \{1, \ldots, N\}|}{N}.$$

Теорема (Семереди, 1975)

Если $D^*(A) > 0$, то множество A содержит арифметические прогрессии любой длины, то есть наборы $\{a, a+d, \ldots, a+kd\} \in A$, $d \neq 0$.

Количественные оценки для случая $k = 3$ были получены до Семереди Ротом (1953), затем Хиф–Брауном (1987), Бургейном (1999, 2008), Сандерсом (2011,2012), Блюмом (2015).
Оценки для $k > 3$ получены Гауэрсом (1998–2001).

Прогрессии в простых числах

Все числа ниже — простые

$$11410337850553 + 4609098694200k\,, \qquad k = 0, 1, \ldots, 21\,.$$

Теорема (Чудаков, Ван дер Корпут, Човла, 1938–1944)

Простые числа содержат бесконечно много арифметических прогрессий длины три.

В доказательстве использовался метод Виноградова.

Теорема (Грин–Тао, 2008)

Простые числа содержат бесконечно много арифметических прогрессий *произвольной* длины.

Грин–Тао–Циглер, 2012: число таких прогрессий/произвольные линейные формы с простыми.

Примеры, 1

Прогрессии длины k, составленные из простых.

Теорема (Грин–Тао–Циглер, 2012)

Число прогресий длины 4, составленных из простых $p_1 < p_2 < p_3 < p_4 \leqslant N$ равно

$$(1 + o(1))\mathfrak{S}_1 \frac{N^2}{\log^4 N},$$

где

$$\mathfrak{S}_1 = \frac{3}{4} \prod_{p \geqslant 5} \left(1 - \frac{3p-1}{(p-1)^3}\right).$$

Примеры, 2

Усиление теоремы Виноградова о простых числах.

Теорема (Грин–Тао–Циглер, 2012)

Пусть N — нечетное число. Тогда количество представлений N в виде $N = p_1 + p_2 + p_3$ таких, что $p_1 - p_2 \in \mathcal{P} - 1$ равно

$$(1 + o(1))\mathfrak{S}_2 \frac{N^2}{\log^4 N},$$

где $\mathfrak{S}_2 =$

$$\frac{1}{3} \prod_{p \geqslant 3,\, p \mid N^3 - N} \left(1 - \frac{p^2 - 4p + 1}{(p-1)^4}\right) \cdot \prod_{p \geqslant 3,\, p \nmid N^3 - N} \left(1 + \frac{4p - 1}{(p-1)^4}\right).$$

В доказательстве Грина–Тао (а затем и Грина–Тао–Циглер) с помощью методов эргодической теории теорема Семереди об арифметических прогрессиях была перенесена на некоторый класс $\mathfrak{C}$ семейств множеств, имеющих нулевую плотность. При этом авторам потребовалось развить метод Гауэрса. Затем, используя вычисления и идеи из работ Голдстона–Пинца–Мотохаши–Ялдирима 2003–2008 гг. Грин и Тао, с помощью теоретико–числовой техники, проверили, что семейство простых принадлежит классу $\mathfrak{C}$.

В исследованиях Грина–Тао–Циглер, помимо инструментов, описанных выше, потребовалось еще более глубокое использование эргодической теории, в частности, теорем о нуль–последовательностях.

Авторами была полностью решена задача о строении функций $f : \mathbb{C} \to \mathbb{D}$, норма Гауэрса которых большая

$$\|f\|_d^{2^d} := \mathbb{E}_{x,\vec{h}} \prod_{\o \in \{0,1\}^d} \mathcal{C}^{|\omega|} f_\omega(x + \omega \cdot \vec{h}) \geqslant \delta\,.$$

Например,

$$\|f\|_3^8 := \mathbb{E}_{x,a,b,c} f(x)\overline{f(x+a)}\,\overline{f(x+b)}\,\overline{f(x+c)}$$

$$f(x+a+b)f(x+a+c)f(x+b+c)\overline{f(x+a+b+c)}\,.$$

Оказывается, что норма f большая тогда и только тогда, когда f имеет большое скалярное произведение с нуль–последовательностью, то есть последовательностью вида $g(T^n x)$, где g — регулярная функция, $x \in X$ и (X, T) — некоторая специальная динамическая система.

Ограниченные расстояния между соседними простыми числами

Одна из старейших и наиболее известных проблем теории простых чисел – проблема близнецов: верно ли, что существует бесконечно много пар простых чисел, разность которых равна 2? Если обозначить n-ое простое число через p_n, то проблема близнецов формулируется в виде: верно ли, что $p_{n+1} - p_n = 2$ для бесконечно многих n? Задача представлялась безнадежной, поэтому изучался ее слабый вариант: доказать существование бесконечно многих n, для которых разность $p_{n+1} - p_n$ "достаточно мала". Так как в силу асимптотического закона распределения простых чисел разность $p_{n+1} - p_n$ в среднем примерно равна $\log p_n$, то хотелось бы показать, что она может быть существенно меньше $\log p_n$.

Обозначим

$$E_1 = \liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n}.$$

Харди и Литтлвуд (1926) доказали, что $E_1 < 1$ в предположении обобщенной гипотезы Римана.
Безусловное доказательство этого неравенства получил Эрдеш (1940). Риччи в 1954 году показал, что $E_1 \leqslant 15/16$.
Верхние оценки величины E_1 улучшали многие математики: Бомбьери и Дэвенпорт (1965), Пильтяй (1972), Учияма (1975), Хаксли (1977, 1984). Наконец, Майер в 1988 году доказал, что $E_1 < 0.25$.
В 2005 году Голдстон, Пинц и Ялдирим установили, что $E_1 = 0$. Вскоре они показали, что

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^{1/2}(\log\log p_n)^2} < \infty.$$

Пусть $h_1, \ldots, h_k$– различные целые числа,

$$H = \{h_1, \ldots, h_k\}.$$

Через $\Lambda(n)$ обозначается функция фон Мангольдта, равная $\log p$, если n есть степень простого числа p. Оценка количества $n \leqslant N$ таких, что все числа $n + h_1, \ldots, n + h_k$ являются простыми, по-существу сводится к оценке суммы

$$\sum_{n \leqslant N} \Lambda(n + h_1) \ldots \Lambda(n + h_k).$$

Предлагается заменить функцию Λ на аппроксимирующую ее сглаженную функцию Λ_R (зависящую от некоторого параметра R). Сама по себе эта идея не привела к новым результатам.

Голдстон, Пинц и Ялдирим пишут, что далее они используют идею Хиф-Бруна (1997) о наборах почти простых чисел, восходящую к Сельбергу (1951). Вместо функции $\Lambda(n)$ рассматривается функция $\Lambda_l(n)$, "ответственная" за наличие у n не более l простых делителей. Затем эта функция сглаживается и аппроксимируется.

Жанг (2013) установил существование такого числа H, что для бесконечного множества чисел n выполнено неравенство $p_{n+1} - p_n \leqslant H$. Известно, что можно взять $H = 246$. В 2013 году Майнард доказал, что для любого натурального k существует такое H_k, что для бесконечного множества чисел n выполнено неравенство $p_{n+k} - p_n \leqslant H_k$. Можно взять $H_k \ll k^3 e^{4k}$.

Большие расстояния между соседними простыми числами

Рассмотрим определенную при $X \geqslant 3$ функцию

$$G(X) = \max_{p_{n+1} \leqslant X} (p_{n+1} - p_n).$$

Асимптотический закон распределения простых чисел утверждает, что

$$\pi(X) \sim X / \log X \quad (X \to \infty).$$

Из него вытекает, что

$$G(X) \geqslant (1 + o(1)) \log X (X \to \infty).$$

В 1931 году Вестзынфиус (Westzynthius) доказал, что

$$G(X) \to \infty \quad (X \to \infty).$$

Используя его идеи, Эрдеш (1935) и Ранкин (1938) улучшили оценку снизу для $G(X)$. Обозначим

$$F(X) = \log X \log\log X (\log\log\log X)^{-2} \log\log\log\log X,$$

где X достаточно велико. Результат Ранкина гласит, что

$$G(X) \geqslant (c + o(1))F(X), \quad c > 0.$$

Вначале неравенство было доказано для $c = 1/3$. Значение c улучшалось многими авторами (Шонхейдж, Ранкин, Майер и Померанц). Пинц (1997) показал, что можно взять $c = 2e^{\gamma}$,

$$\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \log n \right).$$

Недавно было показано, что

$$\lim_{x\to\infty} \frac{G(X)}{F(X)} = \infty.$$

Это сделали независимо Форд, Грин, К., Тао и Майнард. В первой работе использовалось развитие теории Грина - Тао - Циглер о длинных арифметических прогрессиях и других конфигурациях, образованных простыми числами. Во второй работе использовалось развитие результатов Майнарда о существовании малых интервалов со многими простыми числами. В (пока не опубликованной) работе пяти авторов показано, что для некоторой эффективной постоянной $c > 0$ и достаточно большого X

$$G(X) \geqslant cF(X) \log\log\log X.$$

Тернарная проблема Гольдбаха

В письме Л. Эйлеру от 7 июня 1742 года Х. Гольдбах предложил гипотетическое утверждение о простых числах, и Эйлер незамедлительно свел его к следующей гипотезе, которую по его словам Гольдбах ранее ему поставил: каждое положительное число есть сумма не более трех простых чисел. В настоящее время гипотеза разделена на две:

слабая, или тернарная, гипотеза Гольдбаха утверждает, что всякое нечетное число, большее 5, есть сумма трех простых чисел;

сильная, или бинарная, гипотеза Гольдбаха утверждает, что всякое четное число, большее 2, есть сумма двух простых чисел.

В 1933 году Л. Шнирельман доказал, что всякое целое число $n > 1$ представимо в виде суммы не более K простых; значение K указано не было. Эта основополагающая статья в наше время рассматривается как одна из первых работ по аддитивной комбинаторике. В 1969 году Климов указал явное значение $K = 6 \cdot 10^9$. Далее K улучшали Климов, Р. Вон, Ж.-М. Дешулье, Х. Риссель и Р. Вон. В 2012 году Т. Тао доказал, что каждое нечетное число, большее 1, есть сумма не более пяти простых.

В 1937 году И.М. Виноградов (Новый метод в аналитической теории чисел, Труды МИАН, т. 10 (1937), 5–122) доказал тернарную гипотезу Гольдбаха для всех нечетных чисел, превосходящих некоторого числа C. Первое доказательство было неэффективным. В 1947 году И.М. Виноградов (Метод тригонометрических сумм в теории чисел, Труды МИАН, т. 23 (1947), 3–109) предложил эффективное доказательство. Отметим, что аргументы К.К. Марджанишвили (1941) также позволяли получить эффективную оценку. Более того, К.Г. Бороздкин в своей неопубликованной докторской диссертации, выполненной под руководством Виноградова, показал, что можно взять $C = \exp(\exp(\exp(41.96)))$. В 1956 году он улучшил оценку до $C = \exp(\exp(16.038))$. М.-Ч. Лю и Т. Вонг (2002) получили $C = 2 \cdot 10^{1346}$.

В 2013 году Х.А. Хельфгот решил тернарную проблему Гольдбаха, доказав, что можно взять $C = 10^{29}$. С другой стороны, совместно с Д. Платтом он проверил на компьютере справедливость гипотезы для нечетных чисел до $C = 10^{29}$. Позже также в 2013 году он улучшил свое доказательство до $C = 10^{27}$, отметив, что численная проверка нечетных чисел до этой границы может быть сделана на домашнем компьютере в течение уикенда. Хельфгот использовал схему оригинального доказательства Виноградова и привнес в доказательство ряд новых идей, на первый взгляд казавшимися далекими от поставленной цели, включая большое решето.

Проблема Какея в конечных полях

Задача об иголке состоит в определении минимальной площади фигуры на плоскости, в которой единичный отрезок, иглу, можно развернуть на 180 градусов, вернув его в исходное положение с обращенной ориентацией. Этот вопрос рассматривал Какея. Он доказал, что для выпуклых областей минимальная площадь достигается для равностороннего треугольника с высотой 1. Безикович установил, что иглу можно развернуть в фигуре сколь угодно малой площади. Это является следствием существования построенного им компактного множества K нулевой меры, содержащей единичный отрезок в каждом направлении. Однако, K имеет хаусдорфову размерность 2.

Определим множество Безиковича в $\mathbb{R}^n$ как множество нулевой меры, содержащее единичный отрезок в любом направлении. Гипотеза Безиковича утверждает, что множества Безиковича имеют размерность n (по Хаусдорфу и Минковскому), то есть равна размерности объемлющего пространства. Гипотеза Какея верна при $n = 2$ (Рой, 1971). Вольфф (1995) показал, что в n-мерном пространстве размерность множества Безиковича должна быть по крайней мере $(n + 2)/2$. В 2002 году Кац и Тао доказали, что размерность не может быть меньше $(2 - \sqrt{2})(n - 4) + 3$. Эта оценка лучше для $n > 4$.

В 1999 году Вольфф сформулировал аналог задачи об игле для конечных полей. Пусть $\mathbb{F}$– конечное поле. Множество $K \subset \mathbb{F}^n$ называется множеством Безиковича, если для любого вектора $y \in \mathbb{F}^n$ Существует такой $x \in \mathbb{F}^n$, что $\{x + ty : t \in \mathbb{F}\} \subset K$. Аналог проблемы Какея в конечных полях имел следующий вид: верно ли, что $|K| \geqslant c_n|\mathbb{F}|^n$? Легко показать, что это так при $n = 2$; в этом случае $|K| \geqslant |\mathbb{F}|(|\mathbb{F}| + 1)/2$. Отметим, что для нечетных $q \to \infty$, $q = |\mathbb{F}|$, асимптотика точная. Однако, для $n > 2$ известные оценки до 2008 года были более слабыми: $|K| \geqslant c_n|\mathbb{F}|^{(n+2)/2}$ (Вольфф) и $|K| \geqslant c_n|\mathbb{F}|^{4n/7}$ (Роджерс, 2001; Мокенхаупт и Тао, 2004).

В 2008 году гипотеза в конечных полях была доказана Двиром: имеет место неравенство $|K| \geqslant \frac{1}{n!}|\mathbb{F}|^n$, вытекающее из более точного

$$|K| \geqslant M := \binom{q+n-1}{n}, \quad q = |\mathbb{F}|.$$

Для доказательства последнего неравенства Двир предложил метод, названный полиномиальным. Рассмотрим линейное пространство многочлнов над $\mathbb{F}$ от n переменных степени меньше q. Его размерность равна M. Следовательно, если $|K| < M$, то найдется ненулевой многочлен P, зануляющийся на K.

Представим P в виде $P = \sum_{i=0}^{q-1} P_i$, где P_i есть однородная часть степени i многочлена P. Для любого $y \in \mathbb{F}^n$ найдется $x \in \mathbb{F}^n$ такой, что $P(x + ay) = 0$ для любого $a \in \mathbb{F}$. Фиксируем x и y. Тогда $P(x + ay)$ является тождественно равным нулю многочленом степени не выше $q - 1$ от a. Поэтому все коэффициенты этого многочлена равны нулю. В частности, коэффициент при a^{q-1} равен нулю. Значит, $P_{q-1}(y) = 0$. Так как это верно для любого $y \in \mathbb{F}^n$, то многочлен P_{q-1} нулевой. Аналогичными рассуждениями мы получаем последовательно, что многочлены $P_{q-2}, \ldots, P_1$ также нулевые. Следовательно, все коэффициенты многочлена P равны нулю. Противоречие.

Вскоре (2009) Двир, Коппаты, Сараф и Судан еще точнее оценили мощность множества Безиковича:

$$|K| \geqslant \frac{1}{2^n} q^n.$$

Эта оценка близка к верхней оценке: для любого n существует множество Безиковича K такое, что

$$|K| \geqslant \frac{1}{2^{n-1}} q^n + O\left(q^{n-1}\right),$$

где неявная константа в O может зависеть от n.

Полиномиальный метод

Пусть даны n точек на плоскости. Эрдеш (1946) спросил сколько различных расстояний может быть между этими n точками. Он доказал, что если взять квадрат $\sqrt{n} \times \sqrt{n}$ точек обычной целочисленной решетки, то различных расстояний будет $n/\sqrt{\log n}$. Оценка сверху вида $n/\sqrt{\log n}$ называется *гипотезой Эрдеша о различных расстояниях*. Этой задачей занимались Мозер (1952), Чанг–Семереди–Троттер (1992), Шоймоши–Тот (2001), Катц–Тардош (2004) и др.

Теорема (Катц–Тардош, 2004)

Число различных расстояний между любыми n точками на плоскости не меньше, чем $n^{0.8641}$.

С помощью полиномиального метода Гут–Катц получили такой результат.

Теорема (Гут–Катц, 2012)

Число различных расстояний между любыми n точками на плоскости не меньше, чем $n/\log n$.

Таким образом, результат выше отличается от верхней оценки только степенью логарифма.

Множество $A \subseteq \{1, 2, \ldots, N\}$ не содержит арифметические прогрессии длины три, если

$$x + y = 2z\,, \qquad x, y, z \in A \implies x = y = z\,. \tag{1}$$

Наилучшая оценка на мощность множества без прогрессий длины три принадлежит Блюму (2015), который доказал, что

$$|A| \ll \frac{N(\log\log N)^4}{\log N}\,.$$

Нижние оценки сильно отличаются от верхних.

Теорема (Беренд, 1947)

Для всякого N найдется множество $A \subseteq \{1, 2, \ldots, N\}$ без прогрессий длины три и такое, что

$$|A| \gg N \cdot \exp(-2\sqrt{2\ln 2 \log N})\,.$$

Рассмотрим модельную задачу о множествах $A \subseteq \mathbb{F}_3^n$ без решений уравнения (1).

Теорема (Мешулам, 1995)

Пусть $A \subseteq \mathbb{F}_3^n$ не имеет прогрессий длины три. Тогда

$$|A| \ll \frac{3^n}{n}.$$

Теорема (Бэйтман–Катц, 2012)

Пусть $A \subseteq \mathbb{F}_3^n$ не имеет прогрессий длины три. Тогда для некоторой константы $c > 0$ выполнено

$$|A| \ll \frac{3^n}{n^{1+c}}.$$

Известные нижние оценки на мощность множеств, не имеющих прогрессий длины три, используют конструкции, являющиеся декартовыми произведениями маломерных конкретных примеров множеств, без решений уравнения $x + y = 2z$.
Приведем наилучший на сегодняшний день результат.

Теорема (Эдель, 2004)

Для всякого n найдется множество $A \subseteq \mathbb{F}_3^n$ без прогрессий длины три и такое, что

$$|A| \gg 2.2^n .$$

Аналогичные теоремы есть и в произвольных $\mathbb{F}_p^n$.

Недавно с помощью полиномиального метода (построение многочлена от многих переменных, зануляющегося на множестве A без прогрессий длины три) была доказана

Теорема (Крут–Лев–П. Пах, 2016)

Пусть $A \subseteq \mathbb{F}_4^n$ не имеет прогрессий длины три. Тогда

$$|A| \ll 4^{0.927n}.$$

Этот метод был перенесен Элленбергом–Гийсвийтом на все группы $\mathbb{F}_q^n$. Сформулируем их результат в случае $q = 3$.

Теорема (Элленберг–Гийсвийт, 2016)

Пусть $A \subseteq \mathbb{F}_3^n$ не имеет прогрессий длины три. Тогда

$$|A| \ll (2.756)^n.$$

Спасибо за внимание!