КУРС АНАЛИТИЧЕСКОЙ ТЕОРИИ ЧИСЕЛ

Гаральд Гельфготт

23 октября 2014 г.

1 Введение

Аналитическая теория чисел определяется двумя способами – при помощи её методов и её основных объектов изучения. Методы включают в себя комплексный анализ, анализ Фурье, функциональный анализ и так далее. Основные объекты изучения аналитической теории чисел – количество, распределение, рост.

Как правило, основная тема вводного курса аналитической теории чисел это доказательство закона распределения простых чисел и, естественно, свойства ζ-функции Римана. Это центральные вопросы, но мы ими в этом курсе заниматься не будем.

Наша цель в другом. Мы хотим дать общее представление об аналитической теории чисел, придав особое внимание областям современных исследований.

Мы будем придерживаться следующего плана:

1. Аддитивная структура и свойства произвольных подмножеств множества целых чисел $\mathbb{Z}$ и, в общем случае, произвольных подмножеств любого коммутативной группы.

2. Аддитивная структура определённых подмножеств $\mathbb{Z}$, таких как множество простых чисел.

3. Свойства (такие как рост) подмножеств произвольной группы.

Одна из самых важных тем в современной теории чисел – модулярные формы. Из-за недостатка времени, они не входят в наш минимальный план. Зато, если в конце останется время, мы рассмотрим их основную теорию и одно из приложений.

2 Аддитивная комбинаторика

Пусть множество A конечно и $|A|$ обозначает количество элементов в множестве A.

Теорема. (Рот, 1953) *Пусть $A \subset \{1, \dots, N\}$. Пусть ρ обозначает плотность множества A в множестве целых чисел от единицы до N, то есть $\rho = \frac{|A|}{N}$. Пусть $N > N_0$, где N_0 зависит от ρ следующим образом*

$$N_0 \leqslant e^{e^{\frac{C}{\rho}}}, \qquad \text{то есть} \qquad \rho \geqslant \frac{CN}{\log\log N}$$

где C – абсолютная константа. Тогда

$$\exists a, d \neq 0 \in \mathbb{Z} : \quad a, a+d, a+2d \in A.$$

Доказательство. Существование $a, d \in \mathbb{Z}$, $d \neq 0$, таких что $a, a+d, a+2d \in A$, эквивалентно существованию $a_1, a_2, a_3 \in A$ таких что $a_1 + a_3 = 2a_2$, $a_1 < a_2 < a_3$, что в свою очередь эквивалентно условию

$$(1_A \star 1_A \star 1_{-2A})(0) > |A|,$$

где

$$1_A(n) = \begin{cases} 1, & \text{если } n \in A; \\ 0, & \text{если } n \notin A, \end{cases}$$

и свертка определяется равенством

$$f \star g(n) = \sum_{m_1+m_2=n} f(m_1)g(m_2),$$

и

$$-2A = \{-2x,\ x \in A\}.$$

Почему мы требуем "$> |A|$"? Количество "тривиальных"прогрессий вида a, a, a с $a \in A$ – это точно $|A|$. Мы хотим знать, есть ли нетривиальные прогрессии в A.

Напоминание. *Пусть $f : \mathbb{Z} \longrightarrow \mathbb{C}$. Тогда её преобразование Фурье определяется функцией*

$$\hat{f}(\alpha) = \sum_{n \in \mathbb{Z}} f(n)e(\alpha n),$$

где $e(t) = e^{2\pi i t}$, $\alpha \in \mathbb{R}/\mathbb{Z}$. В общем случае, если f и $\hat{f}$ абсолютно интегрируемы, то выполнена формула обращения

$$\hat{\hat{f}}(\alpha) = f(-\alpha),\ \textit{то есть}$$

$$f(n) = \int_{\mathbb{R}/\mathbb{Z}} \hat{f}(\alpha)e(-\alpha)d\alpha.$$

Также выполнено свойство

$$\widehat{f \star g} = \hat{f} \cdot \hat{g}.$$

Таким образом

$$(1_A \star 1_A \star 1_{-2A})(0) = \int_{\mathbb{R}/\mathbb{Z}} 1_A \star \widehat{1_A \star 1_{-2A}}(\alpha)d\alpha =$$

$$= \int_{\mathbb{R}/\mathbb{Z}} (\hat{1}_A(\alpha))^2(\hat{1}_{-2A}(\alpha))d\alpha = \int_{\mathbb{R}/\mathbb{Z}} (\hat{1}_A(\alpha))^2(\hat{1}_A(-2\alpha))d\alpha.$$

Мы хотим показать, что этот интеграл больше, чем $|A|$.

Идея доказательства заключается в следующем:

$$\hat{1}_{\{1,\dots,N\}}(0) = N,\ \ \hat{1}_{\{1,\dots,N\}}(\alpha) \approx 0,\ \ \alpha \nsim 0.$$

Пусть A случайное множество. Тогда или выполнено

$$\hat{1}_A \sim \rho\hat{1}_{\{1,\dots,N\}}$$

или существует $\alpha \nsim 0$, такое что $|\hat{1}_A(\alpha)|$ далеко от $|A|$. В первом случае, как мы увидим $|A|$ ведёт себя в некотором смысле как $\{1, \dots, N\}$, или как случайное множество плотности ρ, с точки зрения существования арифметических прогрессий с тремя элементами. Отсюда следует, что в $|A|$ существует арифметическая прогрессия с тремя элементами. В последнем случае A не ведет себя как $\{1, \dots, N\}$; у A есть структура, и мы будем использовать в доказательстве эту структуру.

Более формально, пусть

$$f_A(n) = 1_A(n) - \rho 1_{\{1,\dots,N\}}.$$

Возможны два случая

1.

$$\forall \alpha \in \mathbb{R}/\mathbb{Z} \;\; |\hat{f}_A(\alpha)| < \varepsilon N,$$

где ε будет выбрано позже. Тогда

$$(1_A \star 1_A \star 1_{-2A})(0) = \int_{\mathbb{R}/\mathbb{Z}} (\hat{1}_A(\alpha))^2 (\hat{1}_A(-2\alpha)) d\alpha$$

$$= \underbrace{\int_{\mathbb{R}/\mathbb{Z}} \rho(\hat{1}_A(\alpha))^2 (\hat{1}_{\{1,\dots,N\}})(-2\alpha) d\alpha}_{=\rho 1_A \star 1_A \star 1_{\{-2,\dots,-2N\}}(0) = \rho |A|^2 = \rho^3 N^2} + \underbrace{\int_{\mathbb{R}/\mathbb{Z}} (\hat{1}_A(\alpha))^2 \hat{f}(-2\alpha) d\alpha}_{|\cdot| < \varepsilon N \int_{\mathbb{R}/\mathbb{Z}} |\hat{1}_A(\alpha)|^2 d\alpha = \varepsilon N \sum_n |\hat{1}_A(n)|^2 = \varepsilon N |A|}$$

Тогда выбирая $\varepsilon = \rho^2 - \frac{1}{N}$, мы получаем

$$(1_A \star 1_A \star 1_{-2A})(0) > \rho^3 N^2 - \left(\rho^2 - \frac{1}{N}\right) |A| N = \rho^3 N^2 - \rho^2 |A| N + |A| = |A|,$$

что завершает первый случай.

2.

$$\exists \alpha \in \mathbb{R}/\mathbb{Z} \;\; |\hat{f}(\alpha)| \geqslant \rho^2 N - 1$$

Тогда согласно следствию из принципа Дирихле

$$\forall Q \exists a, q \leqslant Q \quad \left|\alpha - \frac{a}{q}\right| \leqslant \frac{1}{qQ}. \tag{1}$$

это означает что $\alpha n \bmod 1$ (и $e(\alpha n)$) почти постоянны на арифметических прогрессиях длиной меньше, чем Q по модулю q.

Мы можем представить множество $\{1, \dots, N\}$ в виде объединения непересекающихся арифметических прогрессий по модулю q длиной L, то есть

$$\{1, \dots, N\} = \left(\bigcup_{P \in \mathcal{P}} P\right) \cup O,$$

где $\mathcal{P}$ - семейство непересекающихся арифметических прогрессий длиной L по модулю q, $|\mathcal{P}| \leqslant \frac{N}{L}$ и остаток O удовлетворяет условию $|O| < qL$.

Для любого $P \in \mathcal{P}$ и для любого $n \in P$

$$e(\alpha n) = e(\alpha(n_0 + lq)) = e(\alpha n_0) e(l\alpha q) = e(\alpha n_0) e(l\{\alpha q\}),$$

где $\{x\}$ – это дробная часть числа x. Заметим, что согласно (1)

$$|e(l\{\alpha q\}) - 1| \leqslant 2\pi \frac{L}{Q}$$

и поэтому

$$\left|\sum_{n \in P} f_A(n) e(\alpha n)\right| \leqslant \left|\sum_{n \in P} f_A(n) e(\alpha n_0)\right| + \sum_{n \in P} |f_A(n)| \, |e(l\{\alpha q\}) - 1| \leqslant \left|\sum_{n \in P} f_A(n)\right| + 2\pi \frac{L}{Q}.$$

Таким образом

$$\begin{aligned} \rho^2 N - 1 &\leqslant |\hat{f}(\alpha)| = \left|\sum_n f(n) e(\alpha n)\right| \\ &\leqslant \sum_{P \in \mathcal{P}} \left|\sum_{n \in P} f_A(n) e(\alpha n)\right| + \sum_{n \in O} |f_A(n)| \leqslant \sum_{P \in \mathcal{P}} \left|\sum_{n \in P} f_A(n)\right| + 2\pi \frac{|\mathcal{P}| L}{Q} + qL. \end{aligned} \tag{2}$$

Замечаем, что

$$\sum_{P\in\mathcal{P}}\sum_{n\in P} f_A(n) = \sum_{n\notin O}(1_A(n)-\rho) \leqslant |A| - \rho N + |O| = |O| \leq qL - 1. \tag{3}$$

Мы можем добавить выражения (2) и (3)

$$\sum_{P\in\mathcal{P}}\left(\sum_{n\in P} f_A(n) + \left|\sum_{n\in P} f_A(n)\right|\right) \geqslant \rho^2 N - \frac{2\pi|\mathcal{P}|L^2}{Q} - 2qL$$
$$\geqslant \rho^2 N - \frac{2\pi NL}{Q} - 2QL \geqslant \frac{\rho^2 N}{2},$$

где мы выбираем

$$Q = \lfloor\sqrt{\pi N}\rfloor, \qquad L = \lfloor\frac{\rho^2 Q}{8\pi}\rfloor \geq \frac{\rho^2 Q}{8\pi} - 2.$$

Почему мы добавляем (2) и (3)? В общем случае верно, что

$$x + |x| = \begin{cases} 2x, & \text{если } x \geqslant 0; \\ 0, & \text{если } x < 0, \end{cases}$$

Поэтому согласно принципу Дирихле, из (2) следует, что $\exists P \in \mathcal{P}$, такое что

$$\sum_{n\in P} f_A(n) \geqslant \frac{\rho^2 N}{4|\mathcal{P}|}.$$

Мы заключаем, что

$$|A\cap P| \geqslant \sum_{n\in P} 1_A(n) = \rho|P| + \sum_{n\in P} f_A(n)$$
$$\geqslant \rho L + \frac{\rho^2 N}{4|\mathcal{P}|} \geqslant \left(\rho + \frac{\rho^2}{4}\right) L,$$

так как $|\mathcal{P}| \leqslant \frac{N}{L}$.

Рассмотрим множество

$$A^{'} = \frac{A\cap P - n_0}{q} + 1,$$

где n_0 – первый член в P. Мы знаем, что

$$A^{'} \subset \{1,\dots,L\}, \;\; |A^{'}| \geqslant \left(\rho + \frac{\rho^2}{4}\right) L.$$

если мы нашли $a, a+d, a+2d \in A^{'}$, то в A существует арифметическая прогрессия с элементами $aq+n_0, aq+n_0+dq, aq+n_0+2dq$.

Если же такие элементы не могут быть найдены, то рассмотрим множество $A^{''}$, которое строится из A' так же, как A' строилось из A. Мы повторим процесс снова и снова и, таким образом, мы либо придём к первому случаю, то есть мы нашли арифметическую прогрессию с тремя элементами и теорема доказана, либо будем всегда попадать во второй случай, то есть

$$|A| = \rho N, \quad A \subset \{1,\dots,N\}$$
$$|A^{'}| \geqslant \left(\rho + \frac{\rho^2}{4}\right) N^{'} = \rho^{'} N^{'}, \quad A^{'} \subset \{1,\dots,N^{'}\},$$
$$|A^{''}| \geqslant \left(\rho + \frac{\rho^2}{4} + \frac{\rho + \frac{\rho^2}{4}}{4}\right) N^{''} = \rho^{''} N^{''}, \quad A^{''} \subset \{1,\dots,N^{''}\},$$
$$\dots$$

Эту процедуру можно повторять до тех пор пока не выполнено условие, что

$$N^{(k)} \geqslant 1.$$

Однако, плотность на k-м шаге $\rho^{(k)}$ не может быть больше 1, потому что это не имеет смысла. Легко видеть, что плотность на k-м шаге $\rho^{(k)}$ станет больше, чем 2ρ, когда $k \geqslant \frac{4}{\rho}$ и больше единицы, когда $k \geqslant \frac{4}{\rho} + \frac{1}{\rho} = \frac{5}{\rho}$ (потому что $\log \frac{1}{\rho} < \frac{1}{\rho}$).

В то же время

$$N^{(j+1)} \geqslant \frac{\rho^2 \sqrt{N^{(j)}}}{8\sqrt{\pi}} - 2,$$

и это выражение, в свою очередь больше либо равно, чем $\rho^2\sqrt{N^{(j)}}/15$, если

$$\frac{\rho^2 \sqrt{N^{(j)}}}{8} \geqslant 35.$$

Поэтому

$$\begin{aligned}\log N^{(k)} &\geqslant \frac{1}{2}\log N^{(k-1)} - \log\frac{15}{\rho^2} \geqslant \frac{1}{2}\left(\frac{1}{2}\log N^{(k-2)} - \log\frac{15}{\rho^2}\right) - \log\frac{15}{\rho^2} \quad \geqslant \dots \\ &\geqslant \frac{1}{2^k}\log N - 2\log\frac{15}{\rho^2}.\end{aligned}$$

Таким образом $N^{(k)} \geqslant 35$, если

$$\log N \geqslant 2^k \left(2\log\frac{15}{\rho^2} + \log 35\right).$$

Мы приходим к противоречию, если

$$\log N \geqslant 2^{\frac{5}{\rho}} \left(2\log\frac{8}{\rho^2} + \log 24\right),$$

что случается, если

$$\rho \geqslant \frac{C}{\log\log N}, \quad \text{и } N \geqslant N_0$$

где C – константа большая, чем $5\log 2$, N_0 – постоянная, зависящая от C. □

Доказательство было разбито на два случая

- A ведёт себя как случайное или типичное множество (т.е. у f нет больших коэффициентов Фурье), и тогда мы использовали его случайность,
- A – не ведёт себя как случайное множество. Тогда на A может быть найдена структура, которую мы использовали в доказательстве. Анализ Фурье – это один из нескольких способов задать такую структуру.

Теперь мы обсудим дальнейшие направления работы в этой области.

1. В 1975 Э. Семереди доказал, что для любого $\rho > 0$ и $k > 1$ существует N_0, такое что если $A \subset \{1, \dots, N\}$ и $|A| \geqslant \rho N$, где $N \geqslant N_0$, тогда существуют

$$\exists a, d \neq 0 \in \mathbb{Z} \;\; a, a+d, a+2d, \dots, a+(k-1)d \in A.$$

   Г. Фюрстенберг представил эргодическое доказательство той же самой теоремы. Т. Гауэрс показал как доказать эту же теорему с лучшими значениями для N_0, разработав метод, обобщающий идеи доказательства Рота.

В доказательстве Гаэурса также присутсвует дихотомия между случаем, когда A ведёт себя как случайное множество и случаем, когда мы можем найти структуру на множестве A. Самое основное различие заключается в том, что методы, придуманные Гауэрсом для нахождения структуры являются более общими, чем классический анализ Фурье, и поэтому можим обнаружить существование длинних прогрессии.

Б. Грин и Т. Тао доказали, что сочетания этих методов и других идей достаточно, чтобы доказать, что в множестве простых чисел существует произвольно длинная арифметическая прогрессия, несмотря на то, что существует только приблизительно $\frac{N}{\log N}$ простых чисел в множестве $\{1, \dots, N\}$.

2. Как мы видели, в доказательстве нам необходимо

$$\rho \geqslant \frac{C}{\log\log N}.$$

Существует ряд улучшений данной оценки (или, что то же самое, улучшений оценки для N_0 через ρ). Например, в работе Ж. Бургана итерация в доказательстве прямо основывается не на арифметических прогрессиях, а на так называемый множествах Бора

$$B(S, \alpha) = \{n \in \mathbb{Z} \, \forall \alpha \in S \;\; |e(\alpha n) - 1| < \varepsilon\}.$$

Мы будем использовать эти множества в последующих лекциях.

(Часто множества Бора определяются в $\mathbb{Z}/N\mathbb{Z}$ вместо $\mathbb{Z}$. Это происходит потому, что доказательства теоремы Рота часто начинаются с переходом из $\mathbb{Z}$ в $\mathbb{Z}/N\mathbb{Z}$. Этот способ удобен, и мы будем его иногда использовать в дальнейшем).

Самая сильная граница была найдена Т. Сандерсом (2010) с требованием, что

$$\rho \geqslant \frac{N(\log\log N)^5}{\log N}.$$

Получить границу $\frac{N}{\log N}$ – открытая проблема (схожее утверждение называется гипотеза Эрдеша-Турана).

В следующий раз мы начнём доказательство теоремы Фреймана-Ружа, которая утверждает, что если множество обладает некоторым типичным свойством (рост), то оно очень близко к обобщённой арифметической прогрессии.

Гаральд Гельфготт(Harald Helfgott)
CNRS - Paris VI/VII
E-mail: harald.helfgott@gmail.com