Теорема Романова, нерегулярности в распределении простых

Александр Калмынин

Распределение простых чисел
16 декабря 2020

1. Теорема Бруна-Титчмарша и разности между простыми числами

В одной из предыдущих лекций мы использовали теорему Бруна-Титчмарша в следующем виде:

Теорема

При $x \geq q^2$ *и* $(a, q) = 1$ *выполнено неравенство*

$$\pi(x; q, a) \leq \frac{2x}{\varphi(q) \ln x/q}$$

1. Теорема Бруна-Титчмарша и разности между простыми числами

В одной из предыдущих лекций мы использовали теорему Бруна-Титчмарша в следующем виде:

Теорема

При $x \geq q^2$ *и* $(a, q) = 1$ *выполнено неравенство*

$$\pi(x; q, a) \leq \frac{2x}{\varphi(q) \ln x/q}$$

Так как для доказательства теоремы Эрдёша о циклических числах нам нужна только оценка по порядку, то мы докажем несколько более слабое утверждение.

1. Теорема Бруна-Титчмарша и разности между простыми числами

В одной из предыдущих лекций мы использовали теорему Бруна-Титчмарша в следующем виде:

Теорема

При $x \geq q^2$ *и* $(a,q)=1$ *выполнено неравенство*

$$\pi(x;q,a) \leq \frac{2x}{\varphi(q)\ln x/q}$$

Так как для доказательства теоремы Эрдёша о циклических числах нам нужна только оценка по порядку, то мы докажем несколько более слабое утверждение. А именно, развитый нами метод комбинаторного решета позволяет доказать следующий факт:

1. Теорема Бруна-Титчмарша и разности между простыми числами

Теорема 1

Существует такая константа $C > 0$, *что при* $x \geq q^2$ *и* $(a, q) = 1$ *справедливо соотношение*

$$\pi(x; q, a) \leq \frac{Cx}{\varphi(q) \ln x/q}.$$

1. Теорема Бруна-Титчмарша и разности между простыми числами

Теорема 1

Существует такая константа $C > 0$, *что при* $x \geq q^2$ *и* $(a, q) = 1$ *справедливо соотношение*

$$\pi(x; q, a) \leq \frac{Cx}{\varphi(q) \ln x/q}.$$

Для того, чтобы доказать это соотношение, обозначим $y = x/q$ и возьмём $z = y^{1/5}$. Положим также $\mathcal{A} = \{qn + a, n \leq y\}$. Тогда, очевидно,

$$\mathcal{S}(\mathcal{A}, z) + \pi(z) \geq \pi(x; q, a).$$

1. Теорема Бруна-Титчмарша и разности между простыми числами

Теорема 1

Существует такая константа $C > 0$, что при $x \geq q^2$ и $(a,q) = 1$ справедливо соотношение

$$\pi(x; q, a) \leq \frac{Cx}{\varphi(q) \ln x/q}.$$

Для того, чтобы доказать это соотношение, обозначим $y = x/q$ и возьмём $z = y^{1/5}$. Положим также $\mathcal{A} = \{qn + a, n \leq y\}$. Тогда, очевидно,

$$\mathcal{S}(\mathcal{A}, z) + \pi(z) \geq \pi(x; q, a).$$

Как мы знаем из предыдущей лекции (Теорема 3), множество $\mathcal{D}^+ = \{d = p_1 \dots p_l : p_m < y_m \text{ для нечётных } m \text{ и } p_i > p_{i+1}\}$ задаёт верхнее комбинаторное решето для всех y_m. Выберем, как и в предыдущих рассуждениях, $y_m = z^{\beta^m}$ и $\beta = \frac{4}{5}$.

1. Теорема Бруна-Титчмарша и разности между простыми числами

Для доказательства Теоремы 1 естественно было бы воспользоваться Теоремой 4 предыдущей лекции, однако в её доказательстве мы предполагали, что множество $\mathcal{A}$ фиксировано, так что следует действовать несколько аккуратнее.

1. Теорема Бруна-Титчмарша и разности между простыми числами

Для доказательства Теоремы 1 естественно было бы воспользоваться Теоремой 4 предыдущей лекции, однако в её доказательстве мы предполагали, что множество $\mathcal{A}$ фиксировано, так что следует действовать несколько аккуратнее. Применяя наше комбинаторное решето, получаем

$$\mathcal{S}(\mathcal{A}, z) \leq XV^+(z) + O\left(|\mathcal{D}_z^+|^{1+o(1)}\right),$$

где $|\mathcal{D}_z^+| \leq z^{1+2\beta^2+2\beta^4+\ldots} = z^{(1+\beta^2)/(1-\beta^2)} = y^{41/45}$.

1. Теорема Бруна-Титчмарша и разности между простыми числами

Для доказательства Теоремы 1 естественно было бы воспользоваться Теоремой 4 предыдущей лекции, однако в её доказательстве мы предполагали, что множество $\mathcal{A}$ фиксировано, так что следует действовать несколько аккуратнее. Применяя наше комбинаторное решето, получаем

$$\mathcal{S}(\mathcal{A}, z) \leq XV^{+}(z) + O\left(|\mathcal{D}_z^{+}|^{1+o(1)}\right),$$

где $|\mathcal{D}_z^{+}| \leq z^{1+2\beta^2+2\beta^4+\dots} = z^{(1+\beta^2)/(1-\beta^2)} = y^{41/45}$.
Как мы знаем,

$$V^{+}(z) \leq V(z) + \sum_{n} V_n(z),$$

где $V(z) = \prod_{p \leq z} (1 - g(p))$ и

$$V_n(z) \leq V(y_n) \left(\sum_{y_n \leq p \leq z} g(p) \right)^n \frac{1}{n!}.$$

1. Теорема Бруна-Титчмарша и разности между простыми числами

В нашем случае,

$$|A_d| = \frac{y}{d} + O(1)$$

при $(d, q) = 1$ и 0 иначе. Следовательно,

1. Теорема Бруна-Титчмарша и разности между простыми числами

В нашем случае,

$$|A_d| = \frac{y}{d} + O(1)$$

при $(d, q) = 1$ и 0 иначе. Следовательно,

$$g(p) = \begin{cases} \frac{1}{p} \text{ если } p \nmid q \\ 0 \text{ если } p \mid q. \end{cases}$$

1. Теорема Бруна-Титчмарша и разности между простыми числами

В нашем случае,

$$|A_d| = \frac{y}{d} + O(1)$$

при $(d, q) = 1$ и 0 иначе. Следовательно,

$$g(p) = \begin{cases} \frac{1}{p} \text{ если } p \nmid q \\ 0 \text{ если } p \mid q. \end{cases}$$

Оценка на $V_n(z)$ тогда выглядит таким образом:

$$V_n(z) \leq V(y_n) \left(\sum_{y_n \leq p \leq z} \frac{1}{p} \right)^n \frac{1}{n!} \leq (1 + o(1)) V(z) s_n^n / n! e^{s_n},$$

где

$$s_n = \sum_{y_n \leq p \leq z} \frac{1}{p} = \ln \frac{\ln z}{\ln y_n} + o(1) = n \ln 5/4 + o(1).$$

1. Теорема Бруна-Титчмарша и разности между простыми числами

Отсюда выводим

$$V_n(z) \leq V(z)(1+o(1))\frac{(5/4n\ln 5/4)^n}{n!} \leq V(z)(5e/4\ln 5/4+o(1))^n \leq V(z)0.76^n$$

Отсюда выводим

$$V_n(z) \leq V(z)(1+o(1))\frac{(5/4n\ln 5/4)^n}{n!} \leq V(z)(5e/4\ln 5/4+o(1))^n \leq V(z)0.76^n$$

так что

$$V^+(z) \leq 5.2V(z) \ll \prod_{p\leq z}\left(1-\frac{1}{p}\right)\prod_{p|q}\left(1-\frac{1}{p}\right)^{-1} \asymp \frac{q}{\varphi(q)\ln z} \asymp \frac{q}{\varphi(q)\ln x/q},$$

1. Теорема Бруна-Титчмарша и разности между простыми числами

Отсюда выводим

$$V_n(z) \le V(z)(1+o(1))\frac{(5/4n\ln 5/4)^n}{n!} \le V(z)(5e/4\ln 5/4+o(1))^n \le V(z)0.76^n$$

так что

$$V^+(z) \le 5.2V(z) \ll \prod_{p\le z}\left(1-\frac{1}{p}\right)\prod_{p|q}\left(1-\frac{1}{p}\right)^{-1} \asymp \frac{q}{\varphi(q)\ln z} \asymp \frac{q}{\varphi(q)\ln x/q},$$

откуда

$$\mathcal{S}(\mathcal{A}, z) \ll yV(z) \ll \frac{yq}{\varphi(q)\ln x/q},$$

что и требовалось доказать.

1. Теорема Бруна-Титчмарша и разности между простыми числами

Из проведенного рассуждения видно, что Теорема 4 в действительности применима, если наша функция $g(p)$ ограничена сверху некоторой фиксированной функцией $g_1(p)$, удовлетворяющей

$$\sum_{p \le y} g_1(p) = \ln \ln y + c + o(1).$$

1. Теорема Бруна-Титчмарша и разности между простыми числами

Из проведенного рассуждения видно, что Теорема 4 в действительности применима, если наша функция $g(p)$ ограничена сверху некоторой фиксированной функцией $g_1(p)$, удовлетворяющей

$$\sum_{p \le y} g_1(p) = \ln \ln y + c + o(1).$$

Попробуем приложить данное рассуждение к другой ситуации. На прошлой лекции мы использовали следующее вспомогательное утверждение:

Теорема 2

Для всех a справедлива оценка

$$r_a(x) := \{p, q \le x : p - q = a\} \ll \frac{a}{\varphi(a)} \frac{x}{\ln^2 x}.$$

1. Теорема Бруна-Титчмарша и разности между простыми числами

Ясно, что для доказательства достаточно считать, что $a < x$. Положим $\mathcal{A} = \{n(n+a), n \leq x\}$. Очевидно, что

$$\mathcal{S}(\mathcal{A}, z) + \pi(z) \geq r_a(x).$$

1. Теорема Бруна-Титчмарша и разности между простыми числами

Ясно, что для доказательства достаточно считать, что $a < x$. Положим $\mathcal{A} = \{n(n+a), n \leq x\}$. Очевидно, что

$$\mathcal{S}(\mathcal{A}, z) + \pi(z) \geq r_a(x).$$

Вычислим $|\mathcal{A}_d|$. Ясно, что

$$|\mathcal{A}_d| = \frac{xf(d)}{d} + O(f(d)),$$

где $f(d)$ есть число решений уравнения $x(x+a) = 0$ в $\mathbb{Z}/d\mathbb{Z}$.

1. Теорема Бруна-Титчмарша и разности между простыми числами

Ясно, что для доказательства достаточно считать, что $a < x$. Положим $\mathcal{A} = \{n(n+a), n \leq x\}$. Очевидно, что

$$\mathcal{S}(\mathcal{A}, z) + \pi(z) \geq r_a(x).$$

Вычислим $|\mathcal{A}_d|$. Ясно, что

$$|\mathcal{A}_d| = \frac{xf(d)}{d} + O(f(d)),$$

где $f(d)$ есть число решений уравнения $x(x+a) = 0$ в $\mathbb{Z}/d\mathbb{Z}$. В силу Китайской Теоремы об Остатках, $f(d)$ — мультипликативная функция. Легко видеть, что для простых p выполнено

$$f(p) = \begin{cases} 2 \text{ если } p \mid a \\ 1 \text{ если } p \nmid a. \end{cases}$$

1. Теорема Бруна-Титчмарша и разности между простыми числами

Таким образом, наша функция $g(d) = \frac{f(d)}{d}$ ограничена сверху функцией $g_1(d) = \frac{2^{\omega(d)}}{d}$, так что Теорема 4 применима и для некоторого небольшого c при $z = x^c$ имеем

$$\mathcal{S}(\mathcal{A}, z) \ll xV(z).$$

1. Теорема Бруна-Титчмарша и разности между простыми числами

Таким образом, наша функция $g(d) = \frac{f(d)}{d}$ ограничена сверху функцией $g_1(d) = \frac{2^{\omega}(d)}{d}$, так что Теорема 4 применима и для некоторого небольшого c при $z = x^c$ имеем

$$\mathcal{S}(\mathcal{A}, z) \ll xV(z).$$

Из соотношения

$$V(z) \asymp \prod_{2<p\leq z}\left(1-\frac{2}{p}\right)\prod_{p|a}\left(1-\frac{1}{p}\right)^{-1} \asymp \frac{a}{\varphi(a)}\frac{1}{\ln^2 z} \asymp \frac{a}{\varphi(a)}\frac{1}{\ln^2 x},$$

получаем утверждение Теоремы 2.

Таким образом, наша функция $g(d) = \frac{f(d)}{d}$ ограничена сверху функцией $g_1(d) = \frac{2^{\omega}(d)}{d}$, так что Теорема 4 применима и для некоторого небольшого c при $z = x^c$ имеем

$$\mathcal{S}(\mathcal{A}, z) \ll xV(z).$$

Из соотношения

$$V(z) \asymp \prod_{2<p\le z}\left(1-\frac{2}{p}\right)\prod_{p|a}\left(1-\frac{1}{p}\right)^{-1} \asymp \frac{a}{\varphi(a)}\frac{1}{\ln^2 z} \asymp \frac{a}{\varphi(a)}\frac{1}{\ln^2 x},$$

получаем утверждение Теоремы 2. Предполагается, что верна такая гипотеза об аддитивных сдвигах простых чисел:

1. Теорема Бруна-Титчмарша и разности между простыми числами

Гипотеза 1

Для любых попарно различных $a_1, \ldots, a_k$ *выполнено*

$$\#\{n \leq x : n + a_i \text{ просты для всех } i \leq k\} \gg C(\mathbf{a}) \frac{x}{\ln^k x},$$

где

1. Теорема Бруна-Титчмарша и разности между простыми числами

Гипотеза 1

Для любых попарно различных $a_1, \ldots, a_k$ *выполнено*

$$\#\{n \le x : n + a_i \text{ просты для всех } i \le k\} \gg C(\mathbf{a}) \frac{x}{\ln^k x},$$

где

$$C(\mathbf{a}) = \prod_p \left(1 - \frac{\nu(\mathbf{a}; p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-k}$$

и $\nu(\mathbf{a}; p)$ *есть число решений сравнения* $(n + a_1) \ldots (n + a_k) \equiv 0 \pmod{p}$.

1. Теорема Бруна-Титчмарша и разности между простыми числами

Гипотеза 1

Для любых попарно различных $a_1, \ldots, a_k$ выполнено

$$\#\{n \le x : n + a_i \text{ просты для всех } i \le k\} \gg C(\mathbf{a}) \frac{x}{\ln^k x},$$

где

$$C(\mathbf{a}) = \prod_p \left(1 - \frac{\nu(\mathbf{a}; p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-k}$$

и $\nu(\mathbf{a}; p)$ есть число решений сравнения $(n + a_1) \ldots (n + a_k) \equiv 0 \pmod{p}$.

Если $C(\mathbf{a}) \ne 0$, то набор $a_1, \ldots, a_k$ называется допустимым. Например, $\{0, 2\}$ — допустимый набор, а $\{0, 2, 4\}$ — нет.

2. Теорема Романова

В прошлый раз мы доказали теорему Романова

Теорема (Н. П. Романов, 1934)

Множество чисел, представимых в виде $2^k + p$ для некоторого натурального k и некоторого простого p, имеет положительную плотность.

по модулю следующего вспомогательного утверждения:

2. Теорема Романова

В прошлый раз мы доказали теорему Романова

Теорема (Н. П. Романов, 1934)

Множество чисел, представимых в виде $2^k + p$ для некоторого натурального k и некоторого простого p, имеет положительную плотность.

по модулю следующего вспомогательного утверждения:

Теорема 3

Справедливо неравенство

$$\sum_{2^k \le x} \frac{2^k - 1}{\varphi(2^k - 1)} \ll \ln x.$$

2. Теорема Романова

В прошлый раз мы доказали теорему Романова

Теорема (Н. П. Романов, 1934)

Множество чисел, представимых в виде $2^k + p$ для некоторого натурального k и некоторого простого p, имеет положительную плотность.

по модулю следующего вспомогательного утверждения:

Теорема 3

Справедливо неравенство

$$\sum_{2^k \le x} \frac{2^k - 1}{\varphi(2^k - 1)} \ll \ln x.$$

Здесь мы докажем Теорему 3 при помощи оценок на гладкие числа.

2. Теорема Романова

Поймем сначала, насколько сильно наша оценка отличается от тривиальной. Для этого заметим, что

$$\frac{n}{\varphi(n)} \ll \ln\ln n.$$

2. Теорема Романова

Поймем сначала, насколько сильно наша оценка отличается от тривиальной. Для этого заметим, что

$$\frac{n}{\varphi(n)} \ll \ln\ln n.$$

В самом деле,

$$\frac{n}{\varphi(n)} = \prod_{p|n}\left(1-\frac{1}{p}\right) \ll \exp\left(\sum_{p|n}\frac{1}{p}\right).$$

2. Теорема Романова

Поймем сначала, насколько сильно наша оценка отличается от тривиальной. Для этого заметим, что
$$\frac{n}{\varphi(n)} \ll \ln\ln n.$$
В самом деле,
$$\frac{n}{\varphi(n)} = \prod_{p|n}\left(1-\frac{1}{p}\right) \ll \exp\left(\sum_{p|n}\frac{1}{p}\right).$$
Разобьем сумму на два слагаемых: по $p \leq \ln n$ и по $p > \ln n$. Очевидно, число простых делителей n не превосходит $\frac{\ln n}{\ln 2}$.

2. Теорема Романова

Поймем сначала, насколько сильно наша оценка отличается от тривиальной. Для этого заметим, что

$$\frac{n}{\varphi(n)} \ll \ln\ln n.$$

В самом деле,

$$\frac{n}{\varphi(n)} = \prod_{p|n}\left(1-\frac{1}{p}\right) \ll \exp\left(\sum_{p|n}\frac{1}{p}\right).$$

Разобьем сумму на два слагаемых: по $p \le \ln n$ и по $p > \ln n$. Очевидно, число простых делителей n не превосходит $\frac{\ln n}{\ln 2}$. Следовательно,

$$\sum_{p|n, p>\ln n}\frac{1}{p} \le \frac{\ln n}{\ln 2}\frac{1}{\ln n} \ll 1.$$

2. Теорема Романова

Поймем сначала, насколько сильно наша оценка отличается от тривиальной. Для этого заметим, что

$$\frac{n}{\varphi(n)} \ll \ln\ln n.$$

В самом деле,

$$\frac{n}{\varphi(n)} = \prod_{p|n}\left(1-\frac{1}{p}\right) \ll \exp\left(\sum_{p|n}\frac{1}{p}\right).$$

Разобьем сумму на два слагаемых: по $p \le \ln n$ и по $p > \ln n$. Очевидно, число простых делителей n не превосходит $\frac{\ln n}{\ln 2}$. Следовательно,

$$\sum_{p|n, p>\ln n}\frac{1}{p} \le \frac{\ln n}{\ln 2}\frac{1}{\ln n} \ll 1.$$

С другой стороны, в первой сумме можно опустить условие $p \mid n$, и тогда получится

$$\sum_{p|n, p\le\ln n}\frac{1}{p} \le \sum_{p\le\ln n}\frac{1}{p} \le \ln\ln\ln n + O(1),$$

2. Теорема Романова

откуда и получаем требуемое. Таким образом, каждое слагаемое в интересующей нас сумме есть $O(\ln\ln x)$, а значит тривиальная оценка— $O(\ln x \ln\ln x)$. Мы же попытаемся выиграть дополнительный двойной логарифм.

откуда и получаем требуемое. Таким образом, каждое слагаемое в интересующей нас сумме есть $O(\ln\ln x)$, а значит тривиальная оценка— $O(\ln x \ln\ln x)$. Мы же попытаемся выиграть дополнительный двойной логарифм. Для этого заметим, что

$$\left(1-\frac{1}{p}\right)^{-1}=\left(1-\frac{1}{p^2}\right)^{-1}\left(1+\frac{1}{p}\right),$$

откуда

$$\frac{n}{\varphi(n)}\leq\prod_p\left(1-\frac{1}{p^2}\right)^{-1}\prod_{p|n}\left(1+\frac{1}{p}\right)=\frac{\pi^2}{6}\sum_{d|n}\frac{\mu(d)^2}{d}.$$

откуда и получаем требуемое. Таким образом, каждое слагаемое в интересующей нас сумме есть $O(\ln\ln x)$, а значит тривиальная оценка— $O(\ln x \ln\ln x)$. Мы же попытаемся выиграть дополнительный двойной логарифм. Для этого заметим, что

$$\left(1-\frac{1}{p}\right)^{-1}=\left(1-\frac{1}{p^2}\right)^{-1}\left(1+\frac{1}{p}\right),$$

откуда

$$\frac{n}{\varphi(n)}\le\prod_p\left(1-\frac{1}{p^2}\right)^{-1}\prod_{p|n}\left(1+\frac{1}{p}\right)=\frac{\pi^2}{6}\sum_{d|n}\frac{\mu(d)^2}{d}.$$

Пользуясь этим соотношением, получаем

$$\sum_{2^k\le x}\frac{2^k-1}{\varphi(2^k-1)}\ll\sum_{2^k\le x}\sum_{d|2^k-1}\frac{\mu(d)^2}{d}\ll\ln x\sum_d\frac{1}{d\ell_2(d)},$$

2. Теорема Романова

Здесь $\ell_2(d)$ — порядок числа 2 по модулю d, то есть наименьшее l такое, что $d \mid 2^l - 1$. Условие $d \mid 2^k - 1$ эквивалентно $\ell_2(d) \mid k$, так что для данного d получается $O(\ln x/\ell_2(d))$ слагаемых.

2. Теорема Романова

Здесь $\ell_2(d)$ — порядок числа 2 по модулю d, то есть наименьшее l такое, что $d \mid 2^l - 1$. Условие $d \mid 2^k - 1$ эквивалентно $\ell_2(d) \mid k$, так что для данного d получается $O(\ln x / \ell_2(d))$ слагаемых. Таким образом, нам остается доказать, что ряд

$$\sum_d \frac{1}{d\ell_2(d)}$$

сходится.

2. Теорема Романова

Здесь $\ell_2(d)$ — порядок числа 2 по модулю d, то есть наименьшее l такое, что $d \mid 2^l - 1$. Условие $d \mid 2^k - 1$ эквивалентно $\ell_2(d) \mid k$, так что для данного d получается $O(\ln x/\ell_2(d))$ слагаемых. Таким образом, нам остается доказать, что ряд

$$\sum_d \frac{1}{d\ell_2(d)}$$

сходится. Разобьем натуральные числа на два класса: к первому отнесём те, для которых $\ell_2(d) > (\ln d)^2$, а ко второму все остальные.

2. Теорема Романова

Здесь $\ell_2(d)$ — порядок числа 2 по модулю d, то есть наименьшее l такое, что $d \mid 2^l - 1$. Условие $d \mid 2^k - 1$ эквивалентно $\ell_2(d) \mid k$, так что для данного d получается $O(\ln x/\ell_2(d))$ слагаемых. Таким образом, нам остается доказать, что ряд

$$\sum_d \frac{1}{d\ell_2(d)}$$

сходится. Разобъем натуральные числа на два класса: к первому отнесём те, для которых $\ell_2(d) > (\ln d)^2$, а ко второму все остальные. Ряд

$$\sum_d \frac{1}{d \ln^2 d}$$

сходится, так что слагаемые из первого класса нас не интересуют.

Здесь $\ell_2(d)$ — порядок числа 2 по модулю d, то есть наименьшее l такое, что $d \mid 2^l - 1$. Условие $d \mid 2^k - 1$ эквивалентно $\ell_2(d) \mid k$, так что для данного d получается $O(\ln x/\ell_2(d))$ слагаемых. Таким образом, нам остается доказать, что ряд

$$\sum_d \frac{1}{d\ell_2(d)}$$

сходится. Разобъем натуральные числа на два класса: к первому отнесём те, для которых $\ell_2(d) > (\ln d)^2$, а ко второму все остальные. Ряд

$$\sum_d \frac{1}{d \ln^2 d}$$

сходится, так что слагаемые из первого класса нас не интересуют. Пусть $E(t)$ есть число $d \le t$, лежащих во втором классе. Найдем оценку для $E(t)$. Ясно, что для каждого d, дающего вклад в $E(t)$, найдется $N \le (\ln t)^2$, такое, что $d \mid 2^N - 1$. С другой стороны, у $2^N - 1$ не более N простых делителей.

2. Теорема Романова

Это означает, что существует K, не превосходящее $(\ln t)^4$, и простые числа $q_1 < \ldots < q_K$, такие, что любой простой делитель числа $d \leq t$, принадлежащего второму классу, имеет вид q_i для некоторого i.

Это означает, что существует K, не превосходящее $(\ln t)^4$, и простые числа $q_1 < \ldots < q_K$, такие, что любой простой делитель числа $d \le t$, принадлежащего второму классу, имеет вид q_i для некоторого i. Пусть теперь $p_1, \ldots, p_K$ — K первых простых чисел. Если мы отправим число $d = q_1^{\alpha_1} \ldots q_K^{\alpha_K}$ в $d' = p_1^{\alpha_1} \ldots p_K^{\alpha_K}$, то оно не увеличится. Кроме того, отображение $d \mapsto d'$, очевидно, является инъективным.

2. Теорема Романова

Это означает, что существует K, не превосходящее $(\ln t)^4$, и простые числа $q_1 < \ldots < q_K$, такие, что любой простой делитель числа $d \le t$, принадлежащего второму классу, имеет вид q_i для некоторого i. Пусть теперь $p_1, \ldots, p_K$ — K первых простых чисел. Если мы отправим число $d = q_1^{\alpha_1} \ldots q_K^{\alpha_K}$ в $d' = p_1^{\alpha_1} \ldots p_K^{\alpha_K}$, то оно не увеличится. Кроме того, отображение $d \mapsto d'$, очевидно, является инъективным. Так как $p_K \ll K \ln K \le (\ln t)^5$, то данное рассуждение даёт нам оценку

$$E(t) \le \Psi(t, (\ln t)^5).$$

2. Теорема Романова

Это означает, что существует K, не превосходящее $(\ln t)^4$, и простые числа $q_1 < \ldots < q_K$, такие, что любой простой делитель числа $d \le t$, принадлежащего второму классу, имеет вид q_i для некоторого i. Пусть теперь $p_1, \ldots, p_K$ — K первых простых чисел. Если мы отправим число $d = q_1^{\alpha_1} \ldots q_K^{\alpha_K}$ в $d' = p_1^{\alpha_1} \ldots p_K^{\alpha_K}$, то оно не увеличится. Кроме того, отображение $d \mapsto d'$, очевидно, является инъективным. Так как $p_K \ll K \ln K \le (\ln t)^5$, то данное рассуждение даёт нам оценку

$$E(t) \le \Psi(t, (\ln t)^5).$$

Можно завершить данную оценку, вспомнив теорему Ранкина о размере $\Psi(x, y)$. Вместо этого, давайте воспроизведем доказательство Ранкина, поскольку в данном случае оно особенно удобно.

Лемма 1

Для $A > 1$ справедлива оценка

$$\Psi(t, (\ln t)^A) \le t^{1-1/A+o(1)}.$$

2. Теорема Романова

Для доказательства заметим, что при $d \le t$

$$1 \le \left(\frac{t}{d}\right)^{1-1/A},$$

так что

2. Теорема Романова

Для доказательства заметим, что при $d \le t$

$$1 \le \left(\frac{t}{d}\right)^{1-1/A},$$

так что

$$\Psi(t, (\ln t)^A) \le t^{1-1/A} \sum_{d\ —\ (\ln t)^A-\text{гладкое}} d^{1/A-1} =$$

$$t^{1-1/A} \prod_{p \le (\ln t)^A} \left(1 - \frac{1}{p^{1-1/A}}\right)^{-1} \ll t^{1-1/A} \exp\left(\sum_{p \le (\ln t)^A} \frac{1}{p^{1-1/A}}\right)$$

2. Теорема Романова

Для доказательства заметим, что при $d \leq t$

$$1 \leq \left(\frac{t}{d}\right)^{1-1/A},$$

так что

$$\Psi(t, (\ln t)^A) \leq t^{1-1/A} \sum_{d\text{ — }(\ln t)^A-\text{гладкое}} d^{1/A-1} =$$

$$t^{1-1/A} \prod_{p \leq (\ln t)^A} \left(1 - \frac{1}{p^{1-1/A}}\right)^{-1} \ll t^{1-1/A} \exp\left(\sum_{p \leq (\ln t)^A} \frac{1}{p^{1-1/A}}\right)$$

Из асимптотического закона распределения простых получаем

$$\sum_{p \leq (\ln t)^A} \frac{1}{p^{1-1/A}} \ll \frac{\ln t}{(\ln \ln t)^{1-1/A}} = o(\ln t),$$

откуда и получаем требуемое.

2. Теорема Романова

Итак, $E(t) \ll t^{4/5}$, так что $n-$ное по возрастанию число из второго класса растёт хотя бы как $n^{5/4}$. Следовательно,

2. Теорема Романова

Итак, $E(t) \ll t^{4/5}$, так что $n-$ное по возрастанию число из второго класса растёт хотя бы как $n^{5/4}$. Следовательно,

$$\sum_{d \text{ из } 2 \text{ класса}} \frac{1}{d\ell_2(d)} \ll \sum_n \frac{1}{n^{5/4}} \ll 1,$$

что и завершает доказательство Теоремы 3.

2. Теорема Романова

Итак, $E(t) \ll t^{4/5}$, так что $n-$ное по возрастанию число из второго класса растёт хотя бы как $n^{5/4}$. Следовательно,

$$\sum_{d \text{ из } 2 \text{ класса}} \frac{1}{d\ell_2(d)} \ll \sum_n \frac{1}{n^{5/4}} \ll 1,$$

что и завершает доказательство Теоремы 3. Можно ожидать, что сходные результаты верны и для других множеств чисел вида $u_m + p$, где u_m — некоторая экспоненциально возрастающая последовательность. Наше доказательство легко обобщается на случай $u_m = a^m$.

2. Теорема Романова

Итак, $E(t) \ll t^{4/5}$, так что $n-$ное по возрастанию число из второго класса растёт хотя бы как $n^{5/4}$. Следовательно,

$$\sum_{d \text{ из 2 класса}} \frac{1}{d\ell_2(d)} \ll \sum_n \frac{1}{n^{5/4}} \ll 1,$$

что и завершает доказательство Теоремы 3. Можно ожидать, что сходные результаты верны и для других множеств чисел вида $u_m + p$, где u_m — некоторая экспоненциально возрастающая последовательность. Наше доказательство легко обобщается на случай $u_m = a^m$. В 1951 г. П. Эрдёш показал, что то же самое верно для $u_m = f(a^m)$, где f — фиксированный многочлен.

Итак, $E(t) \ll t^{4/5}$, так что $n-$ное по возрастанию число из второго класса растёт хотя бы как $n^{5/4}$. Следовательно,

$$\sum_{d \text{ из 2 класса}} \frac{1}{d\ell_2(d)} \ll \sum_n \frac{1}{n^{5/4}} \ll 1,$$

что и завершает доказательство Теоремы 3. Можно ожидать, что сходные результаты верны и для других множеств чисел вида $u_m + p$, где u_m — некоторая экспоненциально возрастающая последовательность. Наше доказательство легко обобщается на случай $u_m = a^m$. В 1951 г. П. Эрдёш показал, что то же самое верно для $u_m = f(a^m)$, где f — фиксированный многочлен. В 2010 году Э. Ли доказал аналог теоремы Романова для $u_m = F_m$.

2. Теорема Романова

Итак, $E(t) \ll t^{4/5}$, так что $n-$ное по возрастанию число из второго класса растёт хотя бы как $n^{5/4}$. Следовательно,

$$\sum_{d \text{ из 2 класса}} \frac{1}{d\ell_2(d)} \ll \sum_n \frac{1}{n^{5/4}} \ll 1,$$

что и завершает доказательство Теоремы 3. Можно ожидать, что сходные результаты верны и для других множеств чисел вида $u_m + p$, где u_m — некоторая экспоненциально возрастающая последовательность. Наше доказательство легко обобщается на случай $u_m = a^m$. В 1951 г. П. Эрдёш показал, что то же самое верно для $u_m = f(a^m)$, где f — фиксированный многочлен. В 2010 году Э. Ли доказал аналог теоремы Романова для $u_m = F_m$. С другой стороны, оказывается, что для некоторых просто определенных последовательностей теорема Романова неверна, в частности:

Теорема (А. Н. Васильев, 2016)

Множество чисел, представимых в виде $\binom{2m}{m} + p$ имеет плотность 0.

3. Нерегулярности в распределении простых чисел

Когда обсуждается распределение простых чисел, в качестве одной из моделей можно рассматривать случайную модель Крамера, в которой натуральное число $n \leq x$ является "случайным простым" с вероятностью $\frac{1}{\ln n}$.

3. Нерегулярности в распределении простых чисел

Когда обсуждается распределение простых чисел, в качестве одной из моделей можно рассматривать случайную модель Крамера, в которой натуральное число $n \leq x$ является "случайным простым" с вероятностью $\frac{1}{\ln n}$. Конечно, такая модель не всегда адекватно отражает свойства множества простых чисел. Например, недостаточно быстро стремится к нулю вероятность того, что числа n и $n+1$ одновременно— случайные простые.

3. Нерегулярности в распределении простых чисел

Когда обсуждается распределение простых чисел, в качестве одной из моделей можно рассматривать случайную модель Крамера, в которой натуральное число $n \leq x$ является "случайным простым" с вероятностью $\frac{1}{\ln n}$. Конечно, такая модель не всегда адекватно отражает свойства множества простых чисел. Например, недостаточно быстро стремится к нулю вероятность того, что числа n и $n+1$ одновременно— случайные простые. С другой стороны, если говорить о более глобальном поведении простых чисел, предполагается, что оно совпадает с поведением случайной модели. В частности, гипотеза Римана является в этом контексте аналогом Центральной Предельной Теоремы.

3. Нерегулярности в распределении простых чисел

Когда обсуждается распределение простых чисел, в качестве одной из моделей можно рассматривать случайную модель Крамера, в которой натуральное число $n \le x$ является "случайным простым" с вероятностью $\frac{1}{\ln n}$. Конечно, такая модель не всегда адекватно отражает свойства множества простых чисел. Например, недостаточно быстро стремится к нулю вероятность того, что числа n и $n+1$ одновременно— случайные простые. С другой стороны, если говорить о более глобальном поведении простых чисел, предполагается, что оно совпадает с поведением случайной модели. В частности, гипотеза Римана является в этом контексте аналогом Центральной Предельной Теоремы. Кроме того, данная модель привела Крамера к следующей гипотезе о размере промежутков между соседними простыми числами:

Гипотеза 2 (Х. Крамер)

Справедливо соотношение

$$\max_{p_{n+1} \le x} (p_{n+1} - p_n) \asymp \ln^2 x.$$

3. Нерегулярности в распределении простых чисел

С другой стороны, если пользоваться той же интуицией, то теорема Бореля-Кантелли при $\lambda > 2$ приводит к соотношению

$$\pi(x + (\ln x)^\lambda) - \pi(x) \sim (\ln x)^{\lambda-1}.$$

3. Нерегулярности в распределении простых чисел

С другой стороны, если пользоваться той же интуицией, то теорема Бореля-Кантелли при $\lambda > 2$ приводит к соотношению

$$\pi(x + (\ln x)^\lambda) - \pi(x) \sim (\ln x)^{\lambda-1}.$$

Оказывается, данное соотношение нарушается в довольно сильном смысле этого слова. Мы обсудим доказательство такой теоремы:

Теорема 4 (Х. Майер, 1985)

Для всех $\lambda > 1$ выполнено соотношение

$$\limsup_{x\to\infty} \frac{\pi(x + (\ln x)^\lambda) - \pi(x)}{(\ln x)^{\lambda-1}} > 1 > \liminf_{x\to\infty} \frac{\pi(x + (\ln x)^\lambda) - \pi(x)}{(\ln x)^{\lambda-1}}$$

Для доказательства нам потребуются леммы о нулях L–функций, а также о поведении функции Бухштаба.

Для доказательства нам потребуются леммы о нулях $L-$функций, а также о поведении функции Бухштаба. Пусть $C > 0$. Будем говорить, что q является $C-$хорошим модулем, если любой нуль $\beta + i\gamma$ L-функции любого примитивного характера χ по модулю $q_1 \mid q$ удовлетворяет неравенству

$$1 - \beta \geq \frac{C}{\ln(q(|\gamma| + 1))}.$$

3. Нерегулярности в распределении простых чисел

Для доказательства нам потребуются леммы о нулях L−функций, а также о поведении функции Бухштаба. Пусть $C > 0$. Будем говорить, что q является C−хорошим модулем, если любой нуль $\beta + i\gamma$ L-функции любого примитивного характера χ по модулю $q_1 \mid q$ удовлетворяет неравенству

$$1 - \beta \geq \frac{C}{\ln(q(|\gamma| + 1))}.$$

Как мы знаем из теорем о границах нулей (см. лекцию от 18 ноября), для достаточно малых C единственное возможное исключение — это один вещественный нуль L-функции вещественного характера, то есть нуль Зигеля.

Для доказательства нам потребуются леммы о нулях $L-$функций, а также о поведении функции Бухштаба. Пусть $C > 0$. Будем говорить, что q является $C-$хорошим модулем, если любой нуль $\beta + i\gamma$ L-функции любого примитивного характера χ по модулю $q_1 \mid q$ удовлетворяет неравенству

$$1 - \beta \geq \frac{C}{\ln(q(|\gamma| + 1))}.$$

Как мы знаем из теорем о границах нулей (см. лекцию от 18 ноября), для достаточно малых C единственное возможное исключение — это один вещественный нуль L-функции вещественного характера, то есть нуль Зигеля. Покажем, что выполняется следующая лемма

Лемма 2

Существует $c > 0$ такое, что существуют бесконечно большие значения z, для которых модуль $P(z)$ является $c-$хорошим.

В самом деле, пусть c очень мало, а z — очень большое число, такое, что $P(z)$ не является c—хорошим. Тогда существует вещественный нуль вещественной L-функции по модулю, делящему $P(z)$, для которого

$$1 - \beta \leq \frac{c}{\ln P(z)}.$$

В самом деле, пусть c очень мало, а z — очень большое число, такое, что $P(z)$ не является c−хорошим. Тогда существует вещественный нуль вещественной L-функции по модулю, делящему $P(z)$, для которого

$$1-\beta \le \frac{c}{\ln P(z)}.$$

Согласно одной из лемм о вещественных нулях, если β_1 и β_2 — два вещественных нуля по модулям q_1 и q_2, то для некоторого $c_1 > 0$ выполнено

$$\min(\beta_1, \beta_2) \le 1 - \frac{c_1}{\ln q_1 q_2}.$$

В самом деле, пусть c очень мало, а z — очень большое число, такое, что $P(z)$ не является c–хорошим. Тогда существует вещественный нуль вещественной L-функции по модулю, делящему $P(z)$, для которого

$$1-\beta \le \frac{c}{\ln P(z)}.$$

Согласно одной из лемм о вещественных нулях, если β_1 и β_2 — два вещественных нуля по модулям q_1 и q_2, то для некоторого $c_1 > 0$ выполнено

$$\min(\beta_1,\beta_2) \le 1-\frac{c_1}{\ln q_1 q_2}.$$

Выберем $z_1 > z$ так, чтобы было выполнено неравенство

$$1-\frac{c_1}{2\ln P(z_1)} < \beta \le 1-\frac{c_1}{4\ln P(z_1)}.$$

В силу вышенаписанных неравенств, любой другой вещественный нуль по модулю, делящему $P(z_1)$, удовлетворяет

$$\beta_1 \le 1-\frac{c_1}{2\ln P(z_1)}.$$

3. Нерегулярности в распределении простых чисел

Напомним, что если $\Phi(x,y)$ означает количество натуральных $n \le x$, не имеющих простых делителей, меньших y, то при $y = x^{1/u}$ выполнено

$$\Phi(x,y) \sim \frac{\omega(u)x}{\ln y},$$

3. Нерегулярности в распределении простых чисел

Напомним, что если $\Phi(x,y)$ означает количество натуральных $n \le x$, не имеющих простых делителей, меньших y, то при $y = x^{1/u}$ выполнено

$$\Phi(x,y) \sim \frac{\omega(u)x}{\ln y},$$

где $\omega(u)$ — функция, удовлетворяющая соотношениям

$$\omega(u) = \frac{1}{u} \text{ при } 1 \le u \le 2$$

и

$$(u\omega(u))' = \omega(u-1).$$

3. Нерегулярности в распределении простых чисел

Напомним, что если $\Phi(x, y)$ означает количество натуральных $n \le x$, не имеющих простых делителей, меньших y, то при $y = x^{1/u}$ выполнено

$$\Phi(x, y) \sim \frac{\omega(u)x}{\ln y},$$

где $\omega(u)$ — функция, удовлетворяющая соотношениям

$$\omega(u) = \frac{1}{u} \text{ при } 1 \le u \le 2$$

и

$$(u\omega(u))' = \omega(u-1).$$

Нам потребуется такая лемма о её поведении:

Лемма 3

Функция $\omega(u) - e^{-\gamma}$ меняет знак на отрезке $[a, a+1]$ хотя бы один раз для всех $a \ge 1$.

3. Нерегулярности в рапределении простых чисел

Предположим, что

$$\limsup_{x\to\infty} \frac{\pi(x + (\ln x)^{\lambda}) - \pi(x)}{(\ln x)^{\lambda-1}} \leq 1.$$

Выберем $a > \lambda$ такое, что $\omega(a) > e^{-\gamma}$. Фиксируем очень большой параметр D и выберем большое z, для которого $P(z)$ является $c-$хорошим.

3. Нерегулярности в рапределении простых чисел

Предположим, что

$$\limsup_{x\to\infty} \frac{\pi(x+(\ln x)^{\lambda})-\pi(x)}{(\ln x)^{\lambda-1}} \leq 1.$$

Выберем $a > \lambda$ такое, что $\omega(a) > e^{-\gamma}$. Фиксируем очень большой параметр D и выберем большое z, для которого $P(z)$ является $c-$хорошим. Рассмотрим матрицу

$$M = (s + rP(z)),$$

где $1 \leq s \leq z^a$ и $P(z)^{D-1} < r \leq 2P(z)^{D-1}$.

3. Нерегулярности в рапределении простых чисел

Предположим, что

$$\limsup_{x\to\infty} \frac{\pi(x+(\ln x)^{\lambda})-\pi(x)}{(\ln x)^{\lambda-1}} \leq 1.$$

Выберем $a > \lambda$ такое, что $\omega(a) > e^{-\gamma}$. Фиксируем очень большой параметр D и выберем большое z, для которого $P(z)$ является $c-$хорошим. Рассмотрим матрицу

$$M = (s + rP(z)),$$

где $1 \leq s \leq z^a$ и $P(z)^{D-1} < r \leq 2P(z)^{D-1}$. Сосчитаем количество $\pi(M)$ простых элементов в M двумя способами. В каждой строке содержится не более $(1+o(1))z^a(\ln P(z)^D)^{-1}$ простых чисел, поскольку строчки являются сплошными интервалами логарифмической длины. Это означает, что

$$\pi(M) \leq (1+o(1))P(z)^{D-1}z^a(\ln P(z)^D)^{-1}.$$

3. Нерегулярности в распределении простых чисел

С другой стороны, каждый столбец является арифметической прогрессией. Число допустимых столбцов, то есть примитивных арифметических прогрессий, равно $\Phi(z^a, z) \sim \frac{\omega(a)z^a}{\ln z}$. Так как наш модуль — $c-$хорошее число, то количество простых чисел в каждом допустимом столбце равно

$$\pi(2P(z)^D; P(z), s) - \pi(P(z)^D; P(z), s) = \frac{P(z)^D}{\varphi(P(z))\ln(P(z)^D)}(1+O(e^{-cD})).$$

С другой стороны, каждый столбец является арифметической прогрессией. Число допустимых столбцов, то есть примитивных арифметических прогрессий, равно $\Phi(z^a, z) \sim \frac{\omega(a)z^a}{\ln z}$. Так как наш модуль — c—хорошее число, то количество простых чисел в каждом допустимом столбце равно

$$\pi(2P(z)^D; P(z), s) - \pi(P(z)^D; P(z), s) = \frac{P(z)^D}{\varphi(P(z)) \ln(P(z)^D)}(1 + O(e^{-cD})).$$

Так как

$$\varphi(P(z)) = P(z) \prod_{p \leq z} \left(1 - \frac{1}{p}\right) = P(z) \frac{e^{-\gamma} + o(1)}{\ln z},$$

получаем

$$\pi(M) = \frac{\omega(a)z^a}{\ln z} \frac{P(z)^D}{P(z) \ln P(z)^D (e^{-\gamma} + o(1))(\ln z)^{-1}} =$$

$$= \frac{\omega(a)e^{\gamma}z^{a}P(z)^{D-1}}{\ln P(z)^{D}}(1+O(e^{-cD})),$$

что и приводит к противоречию.

$$= \frac{\omega(a)e^{\gamma}z^{a}P(z)^{D-1}}{\ln P(z)^{D}}(1+O(e^{-cD})),$$

что и приводит к противоречию. Случай невыполнения второго неравенства рассматривается аналогично.

Спасибо за внимание!