Решето Эратосфена. Циклические числа.

Александр Калмынин

Распределение простых чисел
25 ноября 2020

1. Решето Эратосфена

В предыдущих лекциях мы обсуждали методы, позволяющие при помощи изучения свойств рядов Дирихле получать различные оценки на суммы с простыми числами.

1. Решето Эратосфена

В предыдущих лекциях мы обсуждали методы, позволяющие при помощи изучения свойств рядов Дирихле получать различные оценки на суммы с простыми числами. Однако, некоторые задачи, связанные с распределением простых чисел определенного вида, не позволяют столь легко применять аналитические методы, и поэтому для их изучения требуются некоторые аргументы более комбинаторного характера.

1. Решето Эратосфена

В предыдущих лекциях мы обсуждали методы, позволяющие при помощи изучения свойств рядов Дирихле получать различные оценки на суммы с простыми числами. Однако, некоторые задачи, связанные с распределением простых чисел определенного вида, не позволяют столь легко применять аналитические методы, и поэтому для их изучения требуются некоторые аргументы более комбинаторного характера. Один из видов таких аргументов— это класс результатов, которые носят общее название "методы решета“, их мы и будем обсуждать на ближайших лекциях.

1. Решето Эратосфена

В предыдущих лекциях мы обсуждали методы, позволяющие при помощи изучения свойств рядов Дирихле получать различные оценки на суммы с простыми числами. Однако, некоторые задачи, связанные с распределением простых чисел определенного вида, не позволяют столь легко применять аналитические методы, и поэтому для их изучения требуются некоторые аргументы более комбинаторного характера. Один из видов таких аргументов— это класс результатов, которые носят общее название "методы решета“, их мы и будем обсуждать на ближайших лекциях.
Название методам решета дал метод построения таблиц простых чисел, открытый Эратосфеном Киренским:

1. Решето Эратосфена

В предыдущих лекциях мы обсуждали методы, позволяющие при помощи изучения свойств рядов Дирихле получать различные оценки на суммы с простыми числами. Однако, некоторые задачи, связанные с распределением простых чисел определенного вида, не позволяют столь легко применять аналитические методы, и поэтому для их изучения требуются некоторые аргументы более комбинаторного характера. Один из видов таких аргументов— это класс результатов, которые носят общее название "методы решета“, их мы и будем обсуждать на ближайших лекциях. Название методам решета дал метод построения таблиц простых чисел, открытый Эратосфеном Киренским:

1	2	3	4	5	6	7	8	9	10	11	12	13	14
15	16	17	18	19	20	21	22	23	24	25	26	27	28
29	30	31	32	33	34	35	36	37	38	39	40	41	42
43	44	45	46	47	48	49	50	51	52	53	54	55	56
57	58	59	60	61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80	81	82	83	84
85	86	87	88	89	90	91	92	93	94	95	96	97	98

1. Решето Эратосфена

В предыдущих лекциях мы обсуждали методы, позволяющие при помощи изучения свойств рядов Дирихле получать различные оценки на суммы с простыми числами. Однако, некоторые задачи, связанные с распределением простых чисел определенного вида, не позволяют столь легко применять аналитические методы, и поэтому для их изучения требуются некоторые аргументы более комбинаторного характера. Один из видов таких аргументов— это класс результатов, которые носят общее название "методы решета“, их мы и будем обсуждать на ближайших лекциях. Название методам решета дал метод построения таблиц простых чисел, открытый Эратосфеном Киренским:

1	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~	11	~~12~~	13	~~14~~
15	~~16~~	17	~~18~~	19	~~20~~	21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~
29	~~30~~	31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~	41	~~42~~
43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~	51	~~52~~	53	~~54~~	55	~~56~~
57	~~58~~	59	~~60~~	61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~	81	~~82~~	83	~~84~~
85	~~86~~	87	~~88~~	89	~~90~~	91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~

1. Решето Эратосфена

В предыдущих лекциях мы обсуждали методы, позволяющие при помощи изучения свойств рядов Дирихле получать различные оценки на суммы с простыми числами. Однако, некоторые задачи, связанные с распределением простых чисел определенного вида, не позволяют столь легко применять аналитические методы, и поэтому для их изучения требуются некоторые аргументы более комбинаторного характера. Один из видов таких аргументов— это класс результатов, которые носят общее название "методы решета“, их мы и будем обсуждать на ближайших лекциях. Название методам решета дал метод построения таблиц простых чисел, открытый Эратосфеном Киренским:

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~
~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~
29	~~30~~	31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~	41	~~42~~
43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~	~~51~~	~~52~~	53	~~54~~	55	~~56~~
~~57~~	~~58~~	59	~~60~~	61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~	~~81~~	~~82~~	83	~~84~~
85	~~86~~	~~87~~	~~88~~	89	~~90~~	91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~

1. Решето Эратосфена

В предыдущих лекциях мы обсуждали методы, позволяющие при помощи изучения свойств рядов Дирихле получать различные оценки на суммы с простыми числами. Однако, некоторые задачи, связанные с распределением простых чисел определенного вида, не позволяют столь легко применять аналитические методы, и поэтому для их изучения требуются некоторые аргументы более комбинаторного характера. Один из видов таких аргументов— это класс результатов, которые носят общее название "методы решета", их мы и будем обсуждать на ближайших лекциях. Название методам решета дал метод построения таблиц простых чисел, открытый Эратосфеном Киренским:

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~
~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~
29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~	41	~~42~~
43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~
~~57~~	~~58~~	59	~~60~~	61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~	~~81~~	~~82~~	83	~~84~~
~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~	91	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~

1. Решето Эратосфена

В предыдущих лекциях мы обсуждали методы, позволяющие при помощи изучения свойств рядов Дирихле получать различные оценки на суммы с простыми числами. Однако, некоторые задачи, связанные с распределением простых чисел определенного вида, не позволяют столь легко применять аналитические методы, и поэтому для их изучения требуются некоторые аргументы более комбинаторного характера. Один из видов таких аргументов— это класс результатов, которые носят общее название "методы решета“, их мы и будем обсуждать на ближайших лекциях. Название методам решета дал метод построения таблиц простых чисел, открытый Эратосфеном Киренским:

1	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~	11	~~12~~	13	~~14~~
~~15~~	~~16~~	17	~~18~~	19	~~20~~	~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~
29	~~30~~	31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~	41	~~42~~
43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~	~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~
~~57~~	~~58~~	59	~~60~~	61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~	~~81~~	~~82~~	83	~~84~~
~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~	~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~

1. Решето Эратосфена

Данный процесс может быть представлен в виде формулы следующим образом:

1. Решето Эратосфена

Данный процесс может быть представлен в виде формулы следующим образом:

$$\pi(x) - \pi(\sqrt{x}) = [x] - \sum_{p \leq \sqrt{x}} \left[\frac{x}{p}\right]$$

1. Решето Эратосфена

Данный процесс может быть представлен в виде формулы следующим образом:

$$\pi(x) - \pi(\sqrt{x}) = [x] - \sum_{p \le \sqrt{x}} \left[\frac{x}{p}\right] + \sum_{p_1 < p_2 \le \sqrt{x}} \left[\frac{x}{p_1 p_2}\right]$$

1. Решето Эратосфена

Данный процесс может быть представлен в виде формулы следующим образом:

$$\pi(x) - \pi(\sqrt{x}) = [x] - \sum_{p \le \sqrt{x}} \left[\frac{x}{p}\right] + \sum_{p_1 < p_2 \le \sqrt{x}} \left[\frac{x}{p_1 p_2}\right] -$$

$$- \sum_{p_1 < p_2 < p_3 \le \sqrt{x}} \left[\frac{x}{p_1 p_2 p_3}\right] + \ldots$$

Данный процесс может быть представлен в виде формулы следующим образом:

$$\pi(x) - \pi(\sqrt{x}) = [x] - \sum_{p \le \sqrt{x}} \left[\frac{x}{p}\right] + \sum_{p_1 < p_2 \le \sqrt{x}} \left[\frac{x}{p_1 p_2}\right] -$$

$$- \sum_{p_1 < p_2 < p_3 \le \sqrt{x}} \left[\frac{x}{p_1 p_2 p_3}\right] + \ldots = \sum_{n | P(\sqrt{x})} \mu(n) \left[\frac{x}{n}\right],$$

Данный процесс может быть представлен в виде формулы следующим образом:

$$\pi(x) - \pi(\sqrt{x}) = [x] - \sum_{p \le \sqrt{x}} \left[\frac{x}{p}\right] + \sum_{p_1 < p_2 \le \sqrt{x}} \left[\frac{x}{p_1 p_2}\right] -$$

$$- \sum_{p_1 < p_2 < p_3 \le \sqrt{x}} \left[\frac{x}{p_1 p_2 p_3}\right] + \ldots = \sum_{n | P(\sqrt{x})} \mu(n) \left[\frac{x}{n}\right],$$

где $P(z) = \prod_{p \le z} p$. Данное рассуждение легко обобщить на случай произвольных просеянных множеств:

1. Решето Эратосфена

Данный процесс может быть представлен в виде формулы следующим образом:

$$\pi(x) - \pi(\sqrt{x}) = [x] - \sum_{p \le \sqrt{x}} \left[\frac{x}{p}\right] + \sum_{p_1 < p_2 \le \sqrt{x}} \left[\frac{x}{p_1 p_2}\right] -$$

$$- \sum_{p_1 < p_2 < p_3 \le \sqrt{x}} \left[\frac{x}{p_1 p_2 p_3}\right] + \ldots = \sum_{n \mid P(\sqrt{x})} \mu(n) \left[\frac{x}{n}\right],$$

где $P(z) = \prod_{p \le z} p$. Данное рассуждение легко обобщить на случай произвольных просеянных множеств:

Теорема 1

Пусть $\mathcal{A}$ — конечное множество целых чисел. Для всех натуральных чисел d определим $\mathcal{A}_d = \mathcal{A} \cap d\mathbb{Z}$. Пусть $z \ge 1$ и $\mathcal{S}(\mathcal{A}, z) = \#\{a \in \mathcal{A} : (a, P(z)) = 1\}$. Тогда

$$\mathcal{S}(\mathcal{A}, z) = \sum_{d \mid P(z)} \mu(d) |\mathcal{A}_d|.$$

1. Решето Эратосфена

Часто для $\mathcal{A}_d$ справедливы приближенные формулы, из которых при помощи Теоремы 1 можно получить более содержательные результаты:

Часто для $\mathcal{A}_d$ справедливы приближенные формулы, из которых при помощи Теоремы 1 можно получить более содержательные результаты:

Следствие 1

Пусть для некоторого $X > 0$ и некоторой мультипликативной функции $g(d)$ справедливо равенство

$$|\mathcal{A}_d| = Xg(d) + r_d.$$

Часто для $\mathcal{A}_d$ справедливы приближенные формулы, из которых при помощи Теоремы 1 можно получить более содержательные результаты:

Следствие 1

Пусть для некоторого $X > 0$ и некоторой мультипликативной функции $g(d)$ справедливо равенство

$$|\mathcal{A}_d| = Xg(d) + r_d.$$

Тогда

$$\mathcal{S}(\mathcal{A}, z) = XV(z) + O\left(\sum_{d|P(z)} |r_d|\right),$$

где

$$V(z) = \prod_{p \le z} (1 - g(p)).$$

Последнее соотношение получается из равенства

$$\sum_{d|N}\mu(d)g(d)=\prod_{p|N}(1-g(p)).$$

Последнее соотношение получается из равенства

$$\sum_{d|N} \mu(d)g(d) = \prod_{p|N}(1 - g(p)).$$

Выбирая большое $x > 0$, $z = \ln x$, $\mathcal{A} = \mathbb{N} \cap [1, x]$, получаем

$$|\mathcal{A}_d| = \left[\frac{x}{d}\right] = \frac{x}{d} + O(1),$$

то есть $X = x$, $g(d) = \frac{1}{d}$ и $r_d = O(1)$, откуда, в частности

$$\pi(x) \leq \pi(z) + \mathcal{S}(\mathcal{A}, z) = \pi(z) + xV(z) + O(\tau(P(z))) \leq$$

$$\leq z + x\prod_{p\leq z}\left(1 - \frac{1}{p}\right) + O(2^{\pi(z)}) \ll 2^z + \frac{x}{\ln z} \ll \frac{x}{\ln \ln x}.$$

Последнее соотношение получается из равенства

$$\sum_{d|N} \mu(d)g(d) = \prod_{p|N} (1 - g(p)).$$

Выбирая большое $x > 0$, $z = \ln x$, $\mathcal{A} = \mathbb{N} \cap [1, x]$, получаем

$$|\mathcal{A}_d| = \left[\frac{x}{d}\right] = \frac{x}{d} + O(1),$$

то есть $X = x$, $g(d) = \frac{1}{d}$ и $r_d = O(1)$, откуда, в частности

$$\pi(x) \leq \pi(z) + \mathcal{S}(\mathcal{A}, z) = \pi(z) + xV(z) + O(\tau(P(z))) \leq$$

$$\leq z + x \prod_{p \leq z} \left(1 - \frac{1}{p}\right) + O(2^{\pi(z)}) \ll 2^z + \frac{x}{\ln z} \ll \frac{x}{\ln \ln x}.$$

Получившаяся оценка существенно слабее асимптотически точной формулы для $\pi(x)$, однако методы решета начинают быть полезны в других ситуациях.

2. Проблемы Ландау

Примеры задач, в которых методы решета раскрываются в полную мощь, происходят из вопросов о суммах вида

$$\sum_{p \leq x} f(p),$$

где $f(p)$ — некоторая функция, не являющаяся ограничением какой-либо простой для изучения мультипликативной функции.

Примеры задач, в которых методы решета раскрываются в полную мощь, происходят из вопросов о суммах вида

$$\sum_{p\leq x} f(p),$$

где $f(p)$ — некоторая функция, не являющаяся ограничением какой-либо простой для изучения мультипликативной функции. Самые знаменитые в теории простых чисел задачи такого типа были объединены Эдмундом Ландау в список из четырех задач 1912 году на Международном конгрессе математиков:

2. Проблемы Ландау

Примеры задач, в которых методы решета раскрываются в полную мощь, происходят из вопросов о суммах вида

$$\sum_{p \le x} f(p),$$

где $f(p)$ — некоторая функция, не являющаяся ограничением какой-либо простой для изучения мультипликативной функции. Самые знаменитые в теории простых чисел задачи такого типа были объединены Эдмундом Ландау в список из четырех задач 1912 году на Международном конгрессе математиков:

Гипотеза 1

- *Для всякого чётного $2N > 2$ существуют простые числа p и q такие, что $2N = p + q$.*

2. Проблемы Ландау

Примеры задач, в которых методы решета раскрываются в полную мощь, происходят из вопросов о суммах вида

$$\sum_{p \le x} f(p),$$

где $f(p)$ — некоторая функция, не являющаяся ограничением какой-либо простой для изучения мультипликативной функции. Самые знаменитые в теории простых чисел задачи такого типа были объединены Эдмундом Ландау в список из четырех задач 1912 году на Международном конгрессе математиков:

Гипотеза 1

- *Для всякого чётного $2N > 2$ существуют простые числа p и q такие, что $2N = p + q$.*
- *Существует бесконечно много простых p, таких, что $p + 2$ также простое.*

2. Проблемы Ландау

Примеры задач, в которых методы решета раскрываются в полную мощь, происходят из вопросов о суммах вида

$$\sum_{p \le x} f(p),$$

где $f(p)$ — некоторая функция, не являющаяся ограничением какой-либо простой для изучения мультипликативной функции. Самые знаменитые в теории простых чисел задачи такого типа были объединены Эдмундом Ландау в список из четырех задач 1912 году на Международном конгрессе математиков:

Гипотеза 1

- *Для всякого чётного $2N > 2$ существуют простые числа p и q такие, что $2N = p + q$.*
- *Существует бесконечно много простых p, таких, что $p + 2$ также простое.*
- *Между N^2 и $(N + 1)^2$ всегда есть простое число.*

2. Проблемы Ландау

Примеры задач, в которых методы решета раскрываются в полную мощь, происходят из вопросов о суммах вида

$$\sum_{p\le x} f(p),$$

где $f(p)$ — некоторая функция, не являющаяся ограничением какой-либо простой для изучения мультипликативной функции. Самые знаменитые в теории простых чисел задачи такого типа были объединены Эдмундом Ландау в список из четырех задач 1912 году на Международном конгрессе математиков:

Гипотеза 1

- *Для всякого чётного $2N > 2$ существуют простые числа p и q такие, что $2N = p + q$.*
- *Существует бесконечно много простых p, таких, что $p + 2$ также простое.*
- *Между N^2 и $(N+1)^2$ всегда есть простое число.*
- *Существует бесконечно много N таких, что $N^2 + 1$ — простое число.*

2. Проблемы Ландау

Попробуем приложить полученные нами в первом разделе результаты к задаче о числах-близнецах.

2. Проблемы Ландау

Попробуем приложить полученные нами в первом разделе результаты к задаче о числах-близнецах. Найдем верхнюю оценку для величины $\pi_2(x) = \#\{p \leq x : p + 2$ — простое число$\}$. Для этого будем решать общую задачу оценки для $\mathcal{S}(\mathcal{A}, z)$, где $\mathcal{A} = \#\{p + 2 : p \leq x$ — простое число$\}$ и z — параметр, который мы выберем позже.

2. Проблемы Ландау

Попробуем приложить полученные нами в первом разделе результаты к задаче о числах-близнецах. Найдем верхнюю оценку для величины $\pi_2(x) = \#\{p \leq x : p+2$ — простое число$\}$. Для этого будем решать общую задачу оценки для $\mathcal{S}(\mathcal{A}, z)$, где $\mathcal{A} = \#\{p+2 : p \leq x$ — простое число$\}$ и z — параметр, который мы выберем позже. Согласно теореме Зигеля-Вальфиша, для всех нечётных $d \leq \ln x$ справедливо равенство

$$|\mathcal{A}_d| = \pi(x; d, -2) = \frac{Li(x)}{\varphi(d)} + O(xe^{-c\sqrt{\ln x}}).$$

2. Проблемы Ландау

Попробуем приложить полученные нами в первом разделе результаты к задаче о числах-близнецах. Найдем верхнюю оценку для величины $\pi_2(x) = \#\{p \leq x : p+2$ — простое число$\}$. Для этого будем решать общую задачу оценки для $\mathcal{S}(\mathcal{A}, z)$, где $\mathcal{A} = \#\{p+2 : p \leq x$ — простое число$\}$ и z — параметр, который мы выберем позже. Согласно теореме Зигеля-Вальфиша, для всех нечётных $d \leq \ln x$ справедливо равенство

$$|\mathcal{A}_d| = \pi(x; d, -2) = \frac{Li(x)}{\varphi(d)} + O(xe^{-c\sqrt{\ln x}}).$$

Для чётных же d выполнено соотношение

$$|\mathcal{A}_d| = |\{2\}| = 1.$$

Попробуем приложить полученные нами в первом разделе результаты к задаче о числах-близнецах. Найдем верхнюю оценку для величины $\pi_2(x) = \#\{p \le x : p + 2$ — простое число$\}$. Для этого будем решать общую задачу оценки для $\mathcal{S}(\mathcal{A}, z)$, где $\mathcal{A} = \#\{p + 2 : p \le x$ — простое число$\}$ и z — параметр, который мы выберем позже. Согласно теореме Зигеля-Вальфиша, для всех нечётных $d \le \ln x$ справедливо равенство

$$|\mathcal{A}_d| = \pi(x; d, -2) = \frac{Li(x)}{\varphi(d)} + O(xe^{-c\sqrt{\ln x}}).$$

Для чётных же d выполнено соотношение

$$|\mathcal{A}_d| = |\{2\}| = 1.$$

Таким образом, для всех $d \le \ln x$ выполнено равенство

$$|\mathcal{A}_d| = Xg(d) + r_d,$$

2. Проблемы Ландау

Попробуем приложить полученные нами в первом разделе результаты к задаче о числах-близнецах. Найдем верхнюю оценку для величины $\pi_2(x) = \#\{p \leq x : p+2$ — простое число$\}$. Для этого будем решать общую задачу оценки для $\mathcal{S}(\mathcal{A}, z)$, где $\mathcal{A} = \#\{p+2 : p \leq x$ — простое число$\}$ и z — параметр, который мы выберем позже. Согласно теореме Зигеля-Вальфиша, для всех нечётных $d \leq \ln x$ справедливо равенство

$$|\mathcal{A}_d| = \pi(x; d, -2) = \frac{Li(x)}{\varphi(d)} + O(xe^{-c\sqrt{\ln x}}).$$

Для чётных же d выполнено соотношение

$$|\mathcal{A}_d| = |\{2\}| = 1.$$

Таким образом, для всех $d \leq \ln x$ выполнено равенство

$$|\mathcal{A}_d| = Xg(d) + r_d,$$

где $X = Li(x)$, $g(d) = \frac{1}{\varphi(d)}$ для нечетных d, $g(d) = 0$ для чётных d и $r_d \ll xe^{-c\sqrt{\ln x}}$.

Таким образом, из Следствия 1 при $P(z) \le \ln x$ получаем

$$\pi_2(x) \le \pi(z+2) + \mathcal{S}(\mathcal{A}, z) \le \pi(z+2) + Li(x)V(z) + O(\tau(P(z))xe^{-c\sqrt{\ln x}}).$$

Таким образом, из Следствия 1 при $P(z) \leq \ln x$ получаем

$$\pi_2(x) \leq \pi(z+2)+\mathcal{S}(\mathcal{A}, z) \leq \pi(z+2)+Li(x)V(z)+O(\tau(P(z))xe^{-c\sqrt{\ln x}}).$$

Ограничение на $P(z)$ приводит к соотношению

$$\ln\ln x \geq \ln P(z) = \theta(z) = z + o(z),$$

согласно асимптотическому закону распределения простых чисел.

Таким образом, из Следствия 1 при $P(z) \le \ln x$ получаем

$$\pi_2(x) \le \pi(z+2) + \mathcal{S}(\mathcal{A}, z) \le \pi(z+2) + Li(x)V(z) + O(\tau(P(z))xe^{-c\sqrt{\ln x}}).$$

Ограничение на $P(z)$ приводит к соотношению

$$\ln\ln x \ge \ln P(z) = \theta(z) = z + o(z),$$

согласно асимптотическому закону распределения простых чисел. Таким образом, достаточно выбрать $z = \ln\ln x/2$. Отсюда получим

$$\pi(z+2) \le z + 2 \ll \ln\ln x$$

$$\tau(P(z))xe^{-c\sqrt{\ln x}} \ll x \ln x e^{-c\sqrt{\ln x}} \ll xe^{-c/2\sqrt{\ln x}}$$

2. Проблемы Ландау

Таким образом, из Следствия 1 при $P(z) \leq \ln x$ получаем

$$\pi_2(x) \leq \pi(z+2) + \mathcal{S}(\mathcal{A}, z) \leq \pi(z+2) + Li(x)V(z) + O(\tau(P(z))xe^{-c\sqrt{\ln x}}).$$

Ограничение на $P(z)$ приводит к соотношению

$$\ln\ln x \geq \ln P(z) = \theta(z) = z + o(z),$$

согласно асимптотическому закону распределения простых чисел. Таким образом, достаточно выбрать $z = \ln\ln x/2$. Отсюда получим

$$\pi(z+2) \leq z + 2 \ll \ln\ln x$$

$$\tau(P(z))xe^{-c\sqrt{\ln x}} \ll x\ln xe^{-c\sqrt{\ln x}} \ll xe^{-c/2\sqrt{\ln x}}$$

и, наконец,

$$V(z) = \prod_{2<p\leq z}\left(1 - \frac{1}{p-1}\right) \ll \frac{1}{\ln z} \asymp \frac{1}{\ln\ln\ln x}.$$

Таким образом, мы доказали такую оценку:

Теорема 2

$$\pi_2(x) \ll \frac{\pi(x)}{\ln\ln\ln x}.$$

В частности, простые-близнецы имеют относительную плотность 0 во множестве простых чисел.

Таким образом, мы доказали такую оценку:

Теорема 2

$$\pi_2(x) \ll \frac{\pi(x)}{\ln\ln\ln x}.$$

В частности, простые-близнецы имеют относительную плотность 0 во множестве простых чисел.

В дальнейшем мы обсудим более эффективные стратегии получения оценок для $\pi_2(x)$, а также нижние оценки для похожих величин.

Таким образом, мы доказали такую оценку:

Теорема 2

$$\pi_2(x) \ll \frac{\pi(x)}{\ln\ln\ln x}.$$

В частности, простые-близнецы имеют относительную плотность 0 во множестве простых чисел.

В дальнейшем мы обсудим более эффективные стратегии получения оценок для $\pi_2(x)$, а также нижние оценки для похожих величин. Гипотетическая асимптотика для $\pi_2(x)$ выглядит так:

Гипотеза 2

При $x \to +\infty$

$$\pi_2(x) \sim 2C_2 \frac{x}{(\ln x)^2},$$

где $C_2 = \prod_{p\geq 3}\left(1 - \frac{1}{(p-1)^2}\right) \approx 0.66016$ — *константа чисел-близнецов.*

3. Циклические числа

В этом разделе мы обсудим небольшую модификацию решета Эратосфена, которая позволит нам подсчитать количество $Z(x)$ циклических чисел, не превосходящих x.

3. Циклические числа

В этом разделе мы обсудим небольшую модификацию решета Эратосфена, которая позволит нам подсчитать количество $Z(x)$ циклических чисел, не превосходящих x. Циклическим называется такое n, что $(n, \varphi(n)) = 1$. Например, все простые числа цикличны, а все квадраты простых — нет. Кроме того, можно показать, что число n является циклическим тогда и только тогда, когда всякая группа порядка n является циклической.

3. Циклические числа

В этом разделе мы обсудим небольшую модификацию решета Эратосфена, которая позволит нам подсчитать количество $Z(x)$ циклических чисел, не превосходящих x. Циклическим называется такое n, что $(n, \varphi(n)) = 1$. Например, все простые числа цикличны, а все квадраты простых — нет. Кроме того, можно показать, что число n является циклическим тогда и только тогда, когда всякая группа порядка n является циклической. Мы докажем такую асимптотическую формулу для $Z(x)$:

Теорема 3 (Эрдёш, 1948)

При $x \to +\infty$ выполнено равенство

$$Z(x) = \frac{(e^{-\gamma} + o(1))x}{\ln \ln \ln x}.$$

3. Циклические числа

В этом разделе мы обсудим небольшую модификацию решета Эратосфена, которая позволит нам подсчитать количество $Z(x)$ циклических чисел, не превосходящих x. Циклическим называется такое n, что $(n, \varphi(n)) = 1$. Например, все простые числа цикличны, а все квадраты простых — нет. Кроме того, можно показать, что число n является циклическим тогда и только тогда, когда всякая группа порядка n является циклической. Мы докажем такую асимптотическую формулу для $Z(x)$:

Теорема 3 (Эрдёш, 1948)

При $x \to +\infty$ выполнено равенство

$$Z(x) = \frac{(e^{-\gamma} + o(1))x}{\ln \ln \ln x}.$$

Для начала нам потребуются две вспомогательные леммы:

Лемма 1

При $x \to +\infty$

$$\prod_{p \le x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma} + o(1)}{\ln x}.$$

Лемма 1

При $x \to +\infty$

$$\prod_{p \le x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma} + o(1)}{\ln x}.$$

Лемма 2

Пусть $y = x^{\frac{1}{9 \ln \ln x}}$ *и* $\mathcal{P} \subset [1, y]$ *— некоторое множество простых чисел. Если* $S(\mathcal{P}) = \sum_{p \in \mathcal{P}} \frac{1}{p}$, *то*

$$A_{\mathcal{P}}(x) := \#\{n \le x : \forall p \in \mathcal{P}\ (p, n) = 1\} \ll x e^{-S(\mathcal{P})}.$$

3. Циклические числа

Лемма 1

При $x \to +\infty$

$$\prod_{p \le x}\left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma} + o(1)}{\ln x}.$$

Лемма 2

Пусть $y = x^{\frac{1}{9 \ln \ln x}}$ *и* $\mathcal{P} \subset [1, y]$ *— некоторое множество простых чисел. Если* $S(\mathcal{P}) = \sum\limits_{p \in \mathcal{P}} \frac{1}{p}$, *то*

$$A_{\mathcal{P}}(x) := \#\{n \le x : \forall p \in \mathcal{P}\ (p, n) = 1\} \ll x e^{-S(\mathcal{P})}.$$

Для доказательства Леммы 2 заметим, что если в доказательстве Теоремы 1 не выписывать полную формулу, а остановиться после чётного числа шагов, то получится оценка сверху.

3. Циклические числа

Возьмём теперь $m = [4 \ln \ln x] + 1$ и сделаем $2m$ шагов включений-исключений. Получим

3. Циклические числа

Возьмём теперь $m = [4 \ln\ln x] + 1$ и сделаем $2m$ шагов включений-исключений. Получим

$$A_{\mathcal{P}}(x) \leq [x] - \sum_{p \in \mathcal{P}} \left[\frac{x}{p}\right] + \ldots + \sum_{p_1 < p_2 < \ldots < p_{2m}, p_i \in \mathcal{P}} \left[\frac{x}{p_1 \ldots p_{2m}}\right].$$

Возьмём теперь $m = [4\ln\ln x] + 1$ и сделаем $2m$ шагов включений-исключений. Получим

$$A_{\mathcal{P}}(x) \leq [x] - \sum_{p\in\mathcal{P}} \left[\frac{x}{p}\right] + \ldots + \sum_{p_1<p_2<\ldots<p_{2m}, p_i\in\mathcal{P}} \left[\frac{x}{p_1\ldots p_{2m}}\right].$$

Опуская все знаки целой части, получаем

$$A_{\mathcal{P}}(x) = x\mathfrak{S} + O(y^{2m}),$$

3. Циклические числа

Возьмём теперь $m = [4 \ln \ln x] + 1$ и сделаем $2m$ шагов включений-исключений. Получим

$$A_{\mathcal{P}}(x) \leq [x] - \sum_{p \in \mathcal{P}} \left[\frac{x}{p} \right] + \ldots + \sum_{p_1 < p_2 < \ldots < p_{2m}, p_i \in \mathcal{P}} \left[\frac{x}{p_1 \ldots p_{2m}} \right].$$

Опуская все знаки целой части, получаем

$$A_{\mathcal{P}}(x) = x\mathfrak{S} + O(y^{2m}),$$

где

$$\mathfrak{S} = 1 - \sum_{p \in \mathcal{P}} \frac{1}{p} + \ldots + \sum_{p_1 < p_2 < \ldots < p_{2m}, p_i \in \mathcal{P}} \frac{1}{p_1 \ldots p_{2m}}.$$

3. Циклические числа

Возьмём теперь $m = [4 \ln\ln x] + 1$ и сделаем $2m$ шагов включений-исключений. Получим

$$A_{\mathcal{P}}(x) \le [x] - \sum_{p \in \mathcal{P}} \left[\frac{x}{p}\right] + \ldots + \sum_{p_1 < p_2 < \ldots < p_{2m}, p_i \in \mathcal{P}} \left[\frac{x}{p_1 \ldots p_{2m}}\right].$$

Опуская все знаки целой части, получаем

$$A_{\mathcal{P}}(x) = x\mathfrak{S} + O(y^{2m}),$$

где

$$\mathfrak{S} = 1 - \sum_{p \in \mathcal{P}} \frac{1}{p} + \ldots + \sum_{p_1 < p_2 < \ldots < p_{2m}, p_i \in \mathcal{P}} \frac{1}{p_1 \ldots p_{2m}}.$$

Попробуем теперь приблизить нашу конечную сумму $\mathfrak{S}$ полной суммой

$$V = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right) = 1 - \sum_{p \in \mathcal{P}} \frac{1}{p} + \ldots + \sum_{p_1 < p_2 < \ldots < p_{2m}, p_i \in \mathcal{P}} \frac{1}{p_1 \ldots p_{2m}} - \ldots$$

3. Циклические числа

Согласно выписанному разложению, имеет место неравенство

$$|\mathfrak{S} - V| \leq \sum_{k>2m} \sum_{p_1<p_2<\ldots<p_k, p_i \in \mathcal{P}} \frac{1}{p_1 \ldots p_k}.$$

Согласно выписанному разложению, имеет место неравенство

$$|\mathfrak{S} - V| \leq \sum_{k>2m} \sum_{p_1<p_2<\ldots<p_k, p_i\in\mathcal{P}} \frac{1}{p_1\ldots p_k}.$$

Заметим, что каждое слагаемое можно оценить так:

$$\sum_{p_1<p_2<\ldots<p_k, p_i\in\mathcal{P}} \frac{1}{p_1\ldots p_k} \leq \frac{1}{k!}\left(\sum_{p\in\mathcal{P}} \frac{1}{p}\right)^k = \frac{1}{k!}S(\mathcal{P})^k.$$

3. Циклические числа

Согласно выписанному разложению, имеет место неравенство

$$|\mathfrak{S} - V| \le \sum_{k>2m} \sum_{p_1<p_2<\ldots<p_k, p_i\in\mathcal{P}} \frac{1}{p_1\ldots p_k}.$$

Заметим, что каждое слагаемое можно оценить так:

$$\sum_{p_1<p_2<\ldots<p_k, p_i\in\mathcal{P}} \frac{1}{p_1\ldots p_k} \le \frac{1}{k!}\left(\sum_{p\in\mathcal{P}} \frac{1}{p}\right)^k = \frac{1}{k!}S(\mathcal{P})^k.$$

Далее, поскольку

$$S(\mathcal{P}) = \sum_{p\in\mathcal{P}} \frac{1}{p} \le \sum_{p\le y} \frac{1}{p} = \ln\ln y + O(1) = \ln\ln x - \ln(9\ln\ln x) + O(1) \le \ln\ln x,$$

то

3. Циклические числа

Согласно выписанному разложению, имеет место неравенство

$$|\mathfrak{S} - V| \leq \sum_{k>2m} \sum_{p_1<p_2<\ldots<p_k, p_i\in\mathcal{P}} \frac{1}{p_1\ldots p_k}.$$

Заметим, что каждое слагаемое можно оценить так:

$$\sum_{p_1<p_2<\ldots<p_k, p_i\in\mathcal{P}} \frac{1}{p_1\ldots p_k} \leq \frac{1}{k!}\left(\sum_{p\in\mathcal{P}} \frac{1}{p}\right)^k = \frac{1}{k!}S(\mathcal{P})^k.$$

Далее, поскольку

$$S(\mathcal{P}) = \sum_{p\in\mathcal{P}} \frac{1}{p} \leq \sum_{p\leq y} \frac{1}{p} = \ln\ln y + O(1) = \ln\ln x - \ln(9\ln\ln x) + O(1) \leq \ln\ln x,$$

то

$$\frac{1}{k!}S(\mathcal{P})^k \leq \frac{1}{k!}(m/4)^k \leq \frac{1}{4^{k-2m}}\frac{(m/4)^{2m}}{(2m)!}.$$

3. Циклические числа

Заметим, что

$$\frac{(m/4)^{2m}}{(2m)!} \le \frac{(2m)^{2m}}{(2m)!}8^{-2m} \le \left(\frac{e}{8}\right)^{2m} \le e^{-2m}.$$

Заметим, что

$$\frac{(m/4)^{2m}}{(2m)!} \le \frac{(2m)^{2m}}{(2m)!} 8^{-2m} \le \left(\frac{e}{8}\right)^{2m} \le e^{-2m}.$$

Суммируя предыдущее неравенство по всем k, получаем

$$|\mathfrak{S} - V| \le e^{-2m} \le \frac{1}{(\ln x)^8}.$$

3. Циклические числа

Заметим, что

$$\frac{(m/4)^{2m}}{(2m)!} \le \frac{(2m)^{2m}}{(2m)!} 8^{-2m} \le \left(\frac{e}{8}\right)^{2m} \le e^{-2m}.$$

Суммируя предыдущее неравенство по всем k, получаем

$$|\mathfrak{S} - V| \le e^{-2m} \le \frac{1}{(\ln x)^8}.$$

Далее, поскольку

$$V = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right) \ge \prod_{p \le y} \left(1 - \frac{1}{p}\right) \gg \frac{1}{\ln y} \gg \frac{1}{\ln x},$$

то выводим $\mathfrak{S} = V(1 + o(1))$.

Заметим, что

$$\frac{(m/4)^{2m}}{(2m)!} \le \frac{(2m)^{2m}}{(2m)!} 8^{-2m} \le \left(\frac{e}{8}\right)^{2m} \le e^{-2m}.$$

Суммируя предыдущее неравенство по всем k, получаем

$$|\mathfrak{S} - V| \le e^{-2m} \le \frac{1}{(\ln x)^8}.$$

Далее, поскольку

$$V = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p}\right) \ge \prod_{p \le y} \left(1 - \frac{1}{p}\right) \gg \frac{1}{\ln y} \gg \frac{1}{\ln x},$$

то выводим $\mathfrak{S} = V(1 + o(1))$. Так как кроме того

$$y^{2m} = x^{\frac{2[4 \ln \ln x] + 2}{9 \ln \ln x}} \ll x^{9/10},$$

окончательно приходим к оценке

$$A_{\mathcal{P}} \ll xV.$$

окончательно приходим к оценке

$$A_{\mathcal{P}} \ll xV.$$

Заметим теперь, что

$$\ln V = \sum_{p\in\mathcal{P}} \ln\left(1-\frac{1}{p}\right) = -\sum_{p\in\mathcal{P}}\left(\frac{1}{p}+O\left(\frac{1}{p^2}\right)\right) = -S(\mathcal{P})+O(1),$$

откуда и получаем требуемый результат.

окончательно приходим к оценке

$$A_{\mathcal{P}} \ll xV.$$

Заметим теперь, что

$$\ln V = \sum_{p \in \mathcal{P}} \ln\left(1 - \frac{1}{p}\right) = -\sum_{p \in \mathcal{P}} \left(\frac{1}{p} + O\left(\frac{1}{p^2}\right)\right) = -S(\mathcal{P}) + O(1),$$

откуда и получаем требуемый результат. Приступим теперь к доказательству Теоремы 3. Зафиксируем $0 < \varepsilon < 1/2$ и обозначим через $Z_p(x)$ число циклических $n \leq x$, наименьший простой делитель которых равен p. Представим $Z(x)$ в следующем виде:

$$Z(x) = \sum_{p \leq x} Z_p(x) = Z_-(x) + Z_0(x) + Z_+(x).$$

окончательно приходим к оценке

$$A_{\mathcal{P}} \ll xV.$$

Заметим теперь, что

$$\ln V = \sum_{p\in\mathcal{P}} \ln\left(1-\frac{1}{p}\right) = -\sum_{p\in\mathcal{P}}\left(\frac{1}{p}+O\left(\frac{1}{p^2}\right)\right) = -S(\mathcal{P})+O(1),$$

откуда и получаем требуемый результат. Приступим теперь к доказательству Теоремы 3. Зафиксируем $0<\varepsilon<1/2$ и обозначим через $Z_p(x)$ число циклических $n\le x$, наименьший простой делитель которых равен p. Представим $Z(x)$ в следующем виде:

$$Z(x) = \sum_{p\le x} Z_p(x) = Z_-(x)+Z_0(x)+Z_+(x).$$

Суммирование в Z_-, Z_0 и Z_+ ведется по $p\le(\ln\ln x)^{1-\varepsilon}$, $(\ln\ln x)^{1-\varepsilon}<p<(\ln\ln x)^{1+\varepsilon}$ и $p\ge(\ln\ln x)^{1+\varepsilon}$ соответственно.

Оценим сначала $Z_-(x)$. Для этого оценим каждое слагаемое по отдельности.

3. Циклические числа

Оценим сначала $Z_-(x)$. Для этого оценим каждое слагаемое по отдельности. Пусть $p \le (\ln\ln x)^{1-\varepsilon}$. Тогда $Z_p(x)$ не больше, чем количество $n \le x$, не делящихся ни на одно простое $q \le y = x^{1/9 \ln\ln x}$ с условием $q \equiv 1 \pmod p$.

3. Циклические числа

Оценим сначала $Z_{-}(x)$. Для этого оценим каждое слагаемое по отдельности. Пусть $p \le (\ln\ln x)^{1-\varepsilon}$. Тогда $Z_p(x)$ не больше, чем количество $n \le x$, не делящихся ни на одно простое $q \le y = x^{1/9 \ln\ln x}$ с условием $q \equiv 1 \pmod p$. Следовательно, согласно Лемме 2, имеем

$$Z_p(x) \ll x \exp\left(- \sum_{\substack{q \le y \\ q \equiv 1 \pmod p}} \frac{1}{q} \right).$$

3. Циклические числа

Оценим сначала $Z_-(x)$. Для этого оценим каждое слагаемое по отдельности. Пусть $p \le (\ln\ln x)^{1-\varepsilon}$. Тогда $Z_p(x)$ не больше, чем количество $n \le x$, не делящихся ни на одно простое $q \le y = x^{1/9\ln\ln x}$ с условием $q \equiv 1 \pmod p$. Следовательно, согласно Лемме 2, имеем

$$Z_p(x) \ll x \exp\left(-\sum_{\substack{q \le y \\ q \equiv 1 \pmod p}} \frac{1}{q}\right).$$

В силу теоремы Зигеля-Вальфиша,

$$\sum_{\substack{q \le y \\ q \equiv 1 \pmod p}} \frac{1}{q} \gg \frac{\ln\ln y}{p} \gg (\ln\ln x)^{\varepsilon},$$

Оценим сначала $Z_-(x)$. Для этого оценим каждое слагаемое по отдельности. Пусть $p \le (\ln\ln x)^{1-\varepsilon}$. Тогда $Z_p(x)$ не больше, чем количество $n \le x$, не делящихся ни на одно простое $q \le y = x^{1/9\ln\ln x}$ с условием $q \equiv 1 \pmod p$. Следовательно, согласно Лемме 2, имеем

$$Z_p(x) \ll x\exp\left(-\sum_{\substack{q\le y\\ q\equiv 1 \pmod p}} \frac{1}{q}\right).$$

В силу теоремы Зигеля-Вальфиша,

$$\sum_{\substack{q\le y\\ q\equiv 1 \pmod p}} \frac{1}{q} \gg \frac{\ln\ln y}{p} \gg (\ln\ln x)^{\varepsilon},$$

откуда

$$Z_p(x) \ll \frac{x}{(\ln\ln x)^2}$$

при $p \le (\ln\ln x)^{1-\varepsilon}$ и, следовательно,

3. Циклические числа

$$Z_-(x) \ll \ln\ln x \cdot \frac{x}{(\ln\ln x)^2} \ll \frac{x}{\ln\ln x} = o\left(\frac{x}{\ln\ln\ln x}\right).$$

$$Z_-(x) \ll \ln\ln x \cdot \frac{x}{(\ln\ln x)^2} \ll \frac{x}{\ln\ln x} = o\left(\frac{x}{\ln\ln\ln x}\right).$$

Разберемся теперь со слагаемым $Z_0(x)$. Пусть $r \le (\ln\ln x)^{1+\varepsilon}$. Обозначим через $Y_r(x)$ число $m \le x$, не делящихся ни на одно простое $p \le r$. Согласно Теореме 1, справедливо равенство

$$Z_-(x) \ll \ln\ln x \cdot \frac{x}{(\ln\ln x)^2} \ll \frac{x}{\ln\ln x} = o\left(\frac{x}{\ln\ln\ln x}\right).$$

Разберемся теперь со слагаемым $Z_0(x)$. Пусть $r \le (\ln\ln x)^{1+\varepsilon}$. Обозначим через $Y_r(x)$ число $m \le x$, не делящихся ни на одно простое $p \le r$. Согласно Теореме 1, справедливо равенство

$$Y_r(x) = \sum_{d|P(r)} \mu(d)\left[\frac{x}{d}\right] = x\prod_{p\le r}\left(1 - \frac{1}{p}\right) + O(2^r) = \frac{(e^{-\gamma} + o(1))x}{\ln r}.$$

Следовательно, для каждого простого $p \le (\ln\ln x)^{1+\varepsilon}$ справедлива такая оценка для числа $T_p(x)$ бесквадратных чисел $m \le x$, наименьший простой делитель которых в точности равен p:

$$Z_-(x) \ll \ln\ln x \cdot \frac{x}{(\ln\ln x)^2} \ll \frac{x}{\ln\ln x} = o\left(\frac{x}{\ln\ln\ln x}\right).$$

Разберемся теперь со слагаемым $Z_0(x)$. Пусть $r \leq (\ln\ln x)^{1+\varepsilon}$. Обозначим через $Y_r(x)$ число $m \leq x$, не делящихся ни на одно простое $p \leq r$. Согласно Теореме 1, справедливо равенство

$$Y_r(x) = \sum_{d|P(r)} \mu(d)\left[\frac{x}{d}\right] = x\prod_{p\leq r}\left(1-\frac{1}{p}\right) + O(2^r) = \frac{(e^{-\gamma}+o(1))x}{\ln r}.$$

Следовательно, для каждого простого $p \leq (\ln\ln x)^{1+\varepsilon}$ справедлива такая оценка для числа $T_p(x)$ бесквадратных чисел $m \leq x$, наименьший простой делитель которых в точности равен p:

$$T_p(x) = Y_p\left(\frac{x}{p}\right) \ll \frac{x}{p\ln p}.$$

Из этого для промежуточной суммы выводим оценку

$$Z_0(x) \leq \sum_{(\ln\ln x)^{1-\varepsilon} \leq p \leq (\ln\ln x)^{1+\varepsilon}} T_p(x) \ll \frac{x}{\ln\ln\ln x} \sum \frac{1}{p} \ll \frac{\varepsilon x}{\ln\ln\ln x}.$$

3. Циклические числа

Из этого для промежуточной суммы выводим оценку

$$Z_0(x) \le \sum_{(\ln\ln x)^{1-\varepsilon} \le p \le (\ln\ln x)^{1+\varepsilon}} T_p(x) \ll \frac{x}{\ln\ln\ln x} \sum \frac{1}{p} \ll \frac{\varepsilon x}{\ln\ln\ln x}.$$

Осталось только получить формулу для суммы $Z_+(x)$ по большим простым числам. Заметим, что в ней учитываются только циклические n, у которых наименьший простой делитель больше $s = (\ln\ln x)^{1+\varepsilon}$, откуда

$$Z_+(x) \le Y_s(x) = \frac{(e^{-\gamma} + o(1))x}{\ln s} = \frac{(e^{-\gamma} + o(1))x}{(1+\varepsilon)\ln\ln\ln x}.$$

Из этого для промежуточной суммы выводим оценку

$$Z_0(x) \leq \sum_{(\ln\ln x)^{1-\varepsilon} \leq p \leq (\ln\ln x)^{1+\varepsilon}} T_p(x) \ll \frac{x}{\ln\ln\ln x} \sum \frac{1}{p} \ll \frac{\varepsilon x}{\ln\ln\ln x}.$$

Осталось только получить формулу для суммы $Z_+(x)$ по большим простым числам. Заметим, что в ней учитываются только циклические n, у которых наименьший простой делитель больше $s = (\ln\ln x)^{1+\varepsilon}$, откуда

$$Z_+(x) \leq Y_s(x) = \frac{(e^{-\gamma} + o(1))x}{\ln s} = \frac{(e^{-\gamma} + o(1))x}{(1+\varepsilon)\ln\ln\ln x}.$$

Далее, так как для того, чтобы число n было циклическим, достаточно, чтобы оно не делилось на квадраты и выражения вида pq, где p и q — простые и $q-1$ делится на p, то

$$Z_+(x) \geq Y_s(x) - \sum_{r>s} \frac{x}{r^2} - \sum_{\substack{p>s,\, q\leq x \\ q\equiv 1 \pmod p}} \frac{x}{pq}.$$

3. Циклические числа

Первое вычитаемое оценивается просто:

$$\sum_{r>s} \frac{x}{r^2} \ll \frac{x}{s} = o\left(\frac{x}{\ln\ln\ln x}\right).$$

3. Циклические числа

Первое вычитаемое оценивается просто:

$$\sum_{r>s} \frac{x}{r^2} \ll \frac{x}{s} = o\left(\frac{x}{\ln\ln\ln x}\right).$$

Что же касается второй суммы, то здесь мы воспользуемся такой теоремой, которую пока будем использовать без доказательства:

Теорема (Неравенство Бруна-Титчмарша)

Если $x > q^2$, *то*

$$\pi(x; q, a) \ll \frac{x}{\varphi(q)\ln x}$$

для всех $(a, q) = 1$.

3. Циклические числа

Первое вычитаемое оценивается просто:

$$\sum_{r>s} \frac{x}{r^2} \ll \frac{x}{s} = o\left(\frac{x}{\ln\ln\ln x}\right).$$

Что же касается второй суммы, то здесь мы воспользуемся такой теоремой, которую пока будем использовать без доказательства:

Теорема (Неравенство Бруна-Титчмарша)

Если $x > q^2$, *то*

$$\pi(x; q, a) \ll \frac{x}{\varphi(q)\ln x}$$

для всех $(a, q) = 1$.

Разбив сумму по q на два слагаемых с $q < p^2$ и $q > p^2$, получим

$$\sum_{\substack{q \le x \\ q \equiv 1 \pmod p}} \frac{1}{q} \ll \frac{\ln\ln x + \ln p}{p}.$$

3. Циклические числа

Следовательно,

$$\sum_{\substack{p>s, q\le x \\ q\equiv 1 \pmod p}} \frac{x}{pq} \ll x \sum_{p>s} \frac{\ln\ln x + \ln p}{p^2} \ll \frac{x \ln\ln x}{s} = \frac{x}{(\ln\ln x)^{\varepsilon}} = o\left(\frac{x}{\ln\ln\ln x}\right)$$

Следовательно,

$$\sum_{\substack{p>s,q\le x\\ q\equiv 1 \pmod p}} \frac{x}{pq} \ll x\sum_{p>s}\frac{\ln\ln x+\ln p}{p^2} \ll \frac{x\ln\ln x}{s} = \frac{x}{(\ln\ln x)^{\varepsilon}} = o\left(\frac{x}{\ln\ln\ln x}\right)$$

Итого

$$Z_-(x) = o\left(\frac{x}{\ln\ln\ln x}\right)$$

Следовательно,

$$\sum_{\substack{p>s, q\le x\\ q\equiv 1 \pmod p}} \frac{x}{pq} \ll x\sum_{p>s}\frac{\ln\ln x+\ln p}{p^2} \ll \frac{x\ln\ln x}{s} = \frac{x}{(\ln\ln x)^{\varepsilon}} = o\left(\frac{x}{\ln\ln\ln x}\right)$$

Итого

$$Z_-(x) = o\left(\frac{x}{\ln\ln\ln x}\right)$$

$$Z_0(x) \ll \frac{\varepsilon x}{\ln\ln\ln x}$$

Следовательно,

$$\sum_{\substack{p>s, q\le x \\ q\equiv 1 \pmod p}} \frac{x}{pq} \ll x\sum_{p>s}\frac{\ln\ln x+\ln p}{p^2} \ll \frac{x\ln\ln x}{s} = \frac{x}{(\ln\ln x)^{\varepsilon}} = o\left(\frac{x}{\ln\ln\ln x}\right)$$

Итого

$$Z_-(x) = o\left(\frac{x}{\ln\ln\ln x}\right)$$

$$Z_0(x) \ll \frac{\varepsilon x}{\ln\ln\ln x}$$

$$Z_+(x) = \frac{(e^{-\gamma}+O(\varepsilon))x}{\ln\ln\ln x}.$$

Складывая и выбирая ε произвольно малым, получаем требуемое.

Спасибо за внимание!