# М. Королёв, Краткое введение в методы решета.

(расширенный конспект мини-курса, прочитанного на ЛШСМ-2022)

## Введение

Настоящий миникурс посвящен краткому введению в методы решета — одному из самых мощных методов современной теории чисел. С его помощью получены, в частности, недавние результаты о малых расстояниях между соседними простыми числами, среди авторов которых — Я. Пинтц, Д. Голдстон, К. Йылдырым, Й. Мотохаши, нынешний лауреат филдсовской медали Дж. Мейнард и другие ученые.

## Глава 1. Решето Эратосфена

Для начала вспомним известное нам со школьных лет решето Эратосфена. Так называется процедура, позволяющая за сравнительно малое время построить таблицу всех простых чисел, не превосходящих заданной границы $N$. Она основана на следующем простом наблюдении: если $n$ — составное число, то его наименьший простой делитель не превосходит $\sqrt{n}$.

Поясним, как работает решето Эратосфена на конкретном примере. Именно, рассмотрим таблицу всех натуральных чисел от 2 до $N = 64$. На первом шаге вычеркнем из нее все числа, кратные 2 (кроме самой двойки), на втором шаге — все числа, делящиеся на 3 (кроме тройки), и то же проделаем для всех простых чисел, не превосходящих $\sqrt{N} = 8$, т.е. для 5 и 7. Все числа, оставшиеся невычеркнутыми, — простые:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | 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~~ |

Попробуем найти аналитическую форму этой процедуры — перевести её на язык формул. Для этого определим функцию Мёбиуса $\mu(n)$ равенствами:

$$\mu(n) = \begin{cases} 1, \text{ если } n=1, \\ 0, \text{ если } n \text{ делится на квадрат простого числа}, \\ (-1)^k, \text{ если } n = p_1 \cdots p_k, \text{ где } p_j \text{ — различные простые числа} \end{cases}$$

Несложно проверить, что $\mu(2) = \mu(3) = \mu(5) = \mu(7) = -1$, $\mu(4) = \mu(8) = \mu(9) = 0$, $\mu(6) = \mu(10) = 1$ и т.д.

<u>Задача 1</u>. Пусть $s > 1$. Определим дзета-функцию Римана $\zeta(s)$ суммою ряда $\sum_{n=1}^{+\infty} \frac{1}{n^s}$. Доказать, что

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s}.$$

<u>Указание</u>: докажите сперва тождество Эйлера

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

где $p$ пробегает подряд идущие простые числа.

Пусть $f(n)$ — произвольная арифметическая функция. Символом $\sum_{d|n} f(d)$ будем обозначать сумму значений $f$ по всем делителям числа $n$ (включая единицу и само число $n$).

<u>Задача 2</u>. Чему равны суммы $\sum_{d|30} d$ и $\sum_{d|30} \frac{1}{d}$? Как, зная одну, сразу найти вторую?

Арифметическую функцию $f$ назовём мультипликативной, если $f$ не равна нулю тождественно, и для любых взаимно-простых чисел $m, n$ удовлетворяет равенству $f(mn) = f(m)f(n)$.

<u>Задача 3</u> Покажите, что функция Мёбиуса мультипликативна.

<u>Задача 4</u>. Пусть $f$ мультипликативна. Тогда функция $F$, определённая для всякого $n$ равенством $F(n) = \sum_{d|n} f(d)$, тоже мультипликативна.

Теорема 1 (основное свойство функции Мёбиуса). Справедливо равенство:

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если } n=1, \\ 0, & \text{в остальных случаях.} \end{cases}$$

Док-во Из результатов задач 3 и 4 следует, что утверждение достаточно проверить для $n = p^k$, где $p$ – простое, $k \geq 1$. Но для такого $n$ сумма из условия равна $\mu(1) + \mu(p) = 1 - 1 = 0$. Теорема доказана.

Полезно (для дальнейшего) привести ещё одно доказательство Теоремы 1 — комбинаторное. Т.к. в случае $n=1$ утверждение очевидно, можно считать, что $n>1$, и что $p_1^{k_1}\dots p_r^{k_r}$ – каноническое разложение $n$. В силу определения функции Мёбиуса ненулевой вклад в сумму по $d$ вносят лишь бесквадратные делители $n$, т.е. числа вида $p_1^{\alpha_1}\dots p_r^{\alpha_r}$, где каждый из показателей $\alpha_i$ принимает два значения: 0 и 1.

Общее число таких делителей совпадает с числом всевозможных наборов длины $r$ из нулей и единиц, т.е. $2^r$. Количество делителей, имеющих в каноническом разложении ровно $s \geq 0$ сомножителей, совпадает, очевидно, с $C_r^s$, причём вклад от каждого из них в исходную сумму равен $(-1)^s$. Следовательно,

$$\sum_{d|n} \mu(d) = \sum_{s=0}^{r} (-1)^s C_r^s = (1-1)^r = 0,$$ что и требовалось.

Для дальнейшего нам потребуется следующий вспомогательный результат

Лемма 1 Пусть $x \geq 2$. Тогда $\prod_{p \leq x} \left(1 - \frac{1}{p}\right) < \frac{1}{\ln x}$.

Док-во Положим $P = \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1}$ и докажем, что $P > \ln x$. Обращая каждый из сомножителей в геометрическую прогрессию, получим:

$$P = \prod_{p\le x}\left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\dots+\frac{1}{p^k}+\dots\right) = 1+\sum \frac{1}{p_1^{k_1}\dots p_r^{k_r}},$$

где $r\ge 1$, $p_1,\dots,p_r$ – всевозможные различные простые числа, не превосходящие $x$. В силу основной теоремы арифметики, в последней сумме встретятся все дроби $1/n$, $2\le n\le x$. Следовательно,

$$P > \sum_{1\le n\le x}\frac{1}{n} > \ln x.$$

<u>Замечание</u>. При $x\to+\infty$ справедлива следующая асимптотическая формула (формула Мертенса):

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

(см. оборот)

где $\gamma$ – постоянная Эйлера.

Определим $\pi(x)$ как количество простых чисел, не превосходящих $x$, так что, например, $\pi(1)=0$, $\pi(2)=1$, $\pi(3)=2$, $\pi(10)=4$ и т.д. Как ведет себя $\pi(x)$ с ростом $x$?

Из классической теоремы Евклида следует, что $\pi(x)\to+\infty$ при $x\to+\infty$. Можно ли оценить $\pi(x)$ сверху? Так как все простые, за исключением двойки, – нечетные, то

$$\pi(x) \le \left[\frac{x-1}{2}\right]+1 \le \frac{x+1}{2},$$

но такая оценка слишком груба. Чтобы уточнить её, используем конструкцию Эратосфена. Пусть $x\ge 4$, и пусть $P = \prod_{p\le\sqrt{x}} p$. Как мы уже видели, если $\sqrt{x}<n\le x$ и $(n,P)=1$, то $n$ – простое. Если же $n\le\sqrt{x}$, то $(n,P)>1$ за единственным исключением $n=1$. Следовательно, количество всех $n$,

$1 \le n \le x$, удовлетворяющих условию $(n, P) = 1$, равно количеству всех простых на промежутке $(\sqrt{x}, x)$ плюс единица (вклад от $n = 1$), т.е.

$$\pi(x) - \pi(\sqrt{x}) + 1 = \sum_{\substack{1 \le n \le x \\ (n,P)=1}} 1 .$$

Но условие $(n, P) = 1$ можно записать, пользуясь основным свойством функции Мёбиуса. Получим:

$$\pi(x) = \pi(\sqrt{x}) - 1 + \sum_{1 \le n \le x} \sum_{d|(n,P)} \mu(d),$$

Но сумма в правой части приводится к виду

$$\sum_{d|P} \mu(d) \sum_{\substack{1 \le n \le x \\ d|n}} 1 = \sum_{d|P} \mu(d) \left[\frac{x}{d}\right],$$

где $[a]$ – целая часть числа $a$. Так нами доказана

<u>Теорема 2</u> (формула Лежандра):

$$\pi(x) = \pi(\sqrt{x}) + \sum_{d|P} \mu(d) \left[\frac{x}{d}\right] - 1 .$$

Её красота обманчива: чтобы проводить с её помощью вычисления, нужно знать все делители числа $P$ или, что то же, каноническое разложение $P$ на простые сомножители. Но кое-какую пользу из неё мы все же извлечём.

Попытаемся сперва избавиться от знака целой части по формуле $[a] = a - \{a\}$, где $\{a\}$ – дробная доля $a$ (очевидно, $0 \le \{a\} < 1$). Получим:

$$\sum_{d|P} \mu(d) \left[\frac{x}{d}\right] = \sum_{d|P} \mu(d) \left(\frac{x}{d} - \left\{\frac{x}{d}\right\}\right) = xW - R, \text{ где}$$

$$W = \sum_{d|P} \frac{\mu(d)}{d}, \quad R = \sum_{d|P} \mu(d) \left\{\frac{x}{d}\right\}.$$

В силу задачи 4 $W = W(P)$ есть мультипликативная функция $P$, так что

$$W(P) = \prod_{p \le \sqrt{x}} W(p) = \prod_{p \le \sqrt{x}} \left(1 - \frac{1}{p}\right).$$

По лемме 1, $W(P) < \frac{1}{\ln\sqrt{x}} = \frac{2}{\ln x}$, откуда

$$\pi(x) < \frac{2x}{\ln x} + \pi(\sqrt{x}) - 1 + R \leq \frac{2x}{\ln x} + \sqrt{x} + |R|.$$

Переходя к оценке $R$, мы не можем предложить ничего лучшего, чем неравенство

$$|R| \leq \sum_{d|P} 1 = 2^{\pi(\sqrt{x})}.$$

Хотя мы не знаем порядка роста $\pi(x)$, интуитивно ясно, что такая оценка слишком груба: величина $2^{\pi(\sqrt{x})}$ оказывается много больше, чем слагаемое $2x/\ln x$, и наше рассуждение заходит в тупик.

Однако не будем спешить. Иногда полезно немного "пошевелить" уже известную конструкцию и извлечь из неё содержательную информацию.

Заменим величину $\sqrt{x}$ некоторым числом $z$, $2 < z < \sqrt{x}$, а величину $P$ — произведением $\prod_{p \leq z} p$ (которое для простоты будем обозначать той же буквой $P$).

Предположим теперь, что целое $n$ с условием $z < n \leq x$ взаимно-просто с $P$. Это означает, что все простые делители числа $n$ больше $z$. Но ясно, что все простые числа $p$, $z < p \leq x$, обладают таким свойством. Следовательно,

$$\pi(x) - \pi(z) + 1 \leq \sum_{\substack{1 \leq n \leq x \\ (n, P) = 1}} 1$$

Появившийся теперь знак неравенства отражает тот факт, что указанным свойством — взаимной простотой с $P$ — обладают не только простые числа $p$, $z < p \leq x$, но и куча составных.

Стало быть,

$$\pi(x) \le z + \sum_{1\le n\le x} \sum_{d|(n,P)} \mu(d) = z + \sum_{d|P} \mu(d) \sum_{\substack{1\le n\le x\\ n\equiv 0 (\mathrm{mod}\, d)}} 1 =$$

$$= z + \sum_{d|P} \mu(d)\left[\frac{x}{d}\right] = z + x\sum_{d|P}\frac{\mu(d)}{d} - \sum_{d|P}\mu(d)\left\{\frac{x}{d}\right\} =$$

$$= xW + z - R.$$

Далее, $W = \prod_{p\le z}\left(1-\frac{1}{p}\right) < \frac{1}{\ln z}$, $|R| \le 2^{\pi(z)} < 2^{z-1}$.

Следовательно,

$$\pi(x) \le \frac{x}{\ln z} + z + 2^{z-1} \le \frac{x}{\ln z} + 2^z.$$

Возьмем теперь $z = \ln x$. Тогда $2^z = x^{\ln 2} < x^{7/10}$, и окончательно

$$\pi(x) \le \frac{x}{\ln\ln x} + x^{7/10}.$$

Тем самым доказана

<u>Теорема 3</u>. Если $x$ достаточно велико, то

$$\pi(x) < \frac{2x}{\ln\ln x}.$$

Оценка теоремы 3 уже содержательна. Из неё, в частности, следует, что $\frac{\pi(x)}{x} \to 0$ при $x \to +\infty$, т.е. что простых чисел в натуральном ряду "гораздо меньше", чем членов любой арифметической прогрессии. Насколько точна оценка теоремы 3? Известно, что

$$\pi(x) = (1+\bar{o}(1))\frac{x}{\ln x}$$

и, в частности,

$$\pi(x) \le (1+\varepsilon)\frac{x}{\ln x}$$

при любом сколь угодно малом $\varepsilon$ и если $x \ge x_0(\varepsilon)$. Поэтому найденная нами оценка остаётся достаточно грубой. Можно ли выжать еще что-то из нашей конструкции? Оказывается, можно, но для этого её нужно подвергнуть ещё одной модификации.

## Глава 2. Простейшее решето Бруна

Основная идея такой модификации, принадлежащая норвежскому математику Вигго Бруну (1885-1978) состоит в замене функции Мебиуса $\mu(d)$ некоторой другой арифметической функцией $\lambda_d$, "носитель" которой (т.е. множество тех натуральных чисел $d$, для которых $\lambda_d \neq 0$) помещается в сравнительно коротком отрезке.

Заметим, что в этом-то и коренилась главная проблема, из-за которой оценка Теоремы 3 оказалась очень слабенькой: количество чисел $d$ – делителей $P$ – было очень большим.

Чтобы изложить идею Бруна, удобно рассмотреть более общую задачу. Пусть $A$ – некоторое конечное множество натуральных чисел, и пусть $a_n$, $n \in A$, – некоторая последовательность неотрицательных чисел. Пусть, наконец, $z > 2$ и $P = P(z) = \prod_{p \le z} p$. Требуется оценить сверху сумму величин $a_n$ по всем $n$, взаимно простым с $P(z)$ (эту сумму удобно обозначать через $S(A;z)$). Заметим, что задача оценки $\pi(x)$ отвечает случаю, когда $a_n = 1$ для всех $n \le x$, а $z = \sqrt{x}$. Тогда

$$S(A;z) = \sum_{(n,P(z))=1} a_n = \sum_n a_n \sum_{d|(n,P)} \mu(d).$$

Здесь мы свернем со старого пути. Предположим, что имеется функция $\lambda_d$ такая, что для любого $m \ge 1$ выполнено неравенство

$$\sum_{d|m} \mu(d) \le \sum_{d|m} \lambda_d.$$

Тогда, пользуясь тем, что все числа $a_n$ – неотрицательны, будем иметь:

$$S(A;z) \le \sum_n a_n \sum_{d|(n,P)} \lambda_d = \sum_{d|P} \lambda_d \sum_{n \equiv 0 (\mathrm{mod}\, d)} a_n.$$

Теперь выкладки подсказывают нам новые обозначения. Пусть $A_d$ — совокупность всех элементов последовательности $a_n$, $n \in A$, номера которых кратны $d$. Символом $|A_d|$ станем обозначать сумму величин $a_n$ по всем $n \in A_d$.

(Эти обозначения вполне естественны. Если $a_n = 1$ при $n \in A$, и $a_n = 0$ в противном случае, то $A_d$ — это совокупность чисел из $A$, делящихся на $d$, и $|A_d|$ — их количество, совпадающее в данном случае с суммой $a_n$ по всем $n \equiv 0 \pmod d$).

Итак, имеем: $S(A;z) \leq \sum_{d|P} \lambda_d |A_d|$.

Чтобы двигаться дальше, нужно что-то потребовать от величин $|A_d|$. В большинстве случаев оказывается, что $|A_d| = Xg(d) + r_d$, где $g(d)$ — некоторая мультипликативная функция, удовлетворяющая неравенствам $0 \leq g(d) < 1$ для всех бесквадратных $d > 1$, $r_d$ — некоторая величина, которая "в среднем" невелика. Смысл величины $X$ откроется, если положить $d = 1$: $X$ есть хорошее приближение к величине $|A_1| = |A| = \sum_n a_n$. Соответственно,

$$S(A;z) \leq \sum_{d|P} \lambda_d \left( Xg(d) + r_d \right) =$$

$$= X \sum_{d|P} g(d)\lambda_d + \sum_{d|P} \lambda_d r_d = XW + R.$$

Прелесть такого подхода состоит в том, что $\lambda_d$ можно выбрать так, что в сумме $R$ будет не слишком много ненулевых слагаемых.

Чтобы предъявить пример функции $\lambda_d$, обозначим через $\omega(n)$ количество простых делителей числа $n$ без учета их кратности: $\omega(1)=0$, $\omega(2)=\omega(3)=\omega(4)=\omega(5)=1$, $\omega(6)=2$, $\omega(7)=\omega(8)=\omega(9)=1$, $\omega(10)=2$ и т.д. Далее, зададимся четным числом $r \geq 2$ и положим для бесквадратного $d$

$$\lambda_d = \begin{cases} \mu(d), & \text{если } \omega(d) \leq r, \\ 0, & \text{в противном случае} \end{cases}$$

Покажем, что $\lambda_d$ обладает требуемым свойством, т.е. что

$$\sum_{d|m} \mu(d) \leq \sum_{d|m} \lambda_d$$

для любого $m \geq 1$. Пусть сперва $\omega(m) \leq r$. Тогда $\lambda_d = \mu(d)$ для любого делителя числа $m$, и утверждение очевидно. Пусть теперь $\omega(m) = s \geq r+1$. Тогда

$$\sum_{d|m} \lambda_d = \sum_{\substack{d|m \\ \omega(m) \leq r}} \mu(d) = \sum_{k=0}^{r} \sum_{\substack{d|m \\ \omega(d)=k}} \mu(d) = \sum_{k=0}^{r} (-1)^k \sum_{\substack{d|m \\ \omega(d)=k}} 1$$

$$= \sum_{k=0}^{r} (-1)^k C_s^k.$$

Замечая, что $C_s^k = C_{s-1}^{k-1} + C_s^{k-1}$ при $1 \leq k \leq s-1$, получим:

$$\sum_{k=0}^{r} (-1)^k C_s^k = C_s^0 - C_s^1 + C_s^2 - \dots + (-1)^{r-1} C_s^{r-1} + (-1)^r C_s^r =$$

$$= C_{s-1}^0 - (C_{s-1}^0 + C_{s-1}^1) + (C_{s-1}^1 + C_{s-1}^2) - \dots + (-1)^{r-1} (C_{s-1}^{r-2} + C_{s-1}^{r-1}) +$$

$$+ (-1)^r (C_{s-1}^{r-1} + C_{s-1}^r) = (-1)^r C_{s-1}^r = C_{s-1}^r > 0,$$ так что

$$\sum_{d|m} \lambda_d > \sum_{d|m} \mu(d).$$

<u>Задача 6</u>. Пусть $r \geq 1$ — нечетное число. Докажите, что функция

$$\bar{\lambda}_d = \begin{cases} \mu(d), & \omega(d) \leq r, \\ 0, & \text{в противном случае}, \end{cases}$$

при любом $m$ удовлетворяет неравенству $\sum_{d|m} \bar{\lambda}_d \leq \sum_{d|m} \mu(d)$.

Посмотрим, что дает такой выбор для верхней оценки $\pi(x)$. В этом случае

$$|A_d| = \sum_{\substack{1\le n\le x \\ n\equiv 0 \pmod d}} 1 = \left[\frac{x}{d}\right] = \frac{x}{d} - \left\{\frac{x}{d}\right\},$$

так что можно положить $X = x$, $g(d) = \frac{1}{d}$, $r_d = -\left\{\frac{x}{d}\right\}$.

Далее,

$$\pi(x) - \pi(z) + 1 \le S(A, z) \le xW + R, \text{ где}$$

$$W = \sum_{d|P} \frac{\lambda_d}{d}, \quad |R| \le \sum_{d|P} |\lambda_d|.$$

Сразу заметим: все делители $d$ числа $P$, для которых $\lambda_d \ne 0$, подчинены условию $\omega(d) \le \tau$. Поэтому для каждого из них справедливо неравенство: $d \le z^{\omega(d)} \le z^{\tau}$.

Таким образом $|R| \le z^{\tau}$.

Чуть сложнее обстоит дело с величиной $W$. Прежде всего, представим ее в виде разности

$$W = \Bigg( \sum_{d|P} - \sum_{\substack{d|P \\ \omega(d)>\tau}} \Bigg) \frac{\mu(d)}{d} = W_1 - W_2.$$

Сумма $W_1$ уже оценивалась выше:

$$W_1 = \prod_{p\le z} \left(1 - \frac{1}{p}\right) \le \frac{1}{\ln z}.$$

Далее, группируя в $W_2$ слагаемые с одинаковым значением $\omega(d)$, будем иметь:

$$|W_2| \le \sum_{\substack{d|P \\ \omega(d)=\tau+1}} \frac{1}{d} + \sum_{\substack{d|P \\ \omega(d)=\tau+2}} \frac{1}{d} + \dots + \sum_{\substack{d|P \\ \omega(d)=s}} \frac{1}{d} + \dots = w_{\tau+1} + w_{\tau+2} + \dots + w_s + \dots$$

Но несложно проверить (сделайте это!), что

$$w_s \le \frac{1}{s!} \Bigg( \sum_{p\le z} \frac{1}{p} \Bigg)^s = \frac{\sigma^s}{s!},$$

где смысл обозначения $\sigma$ очевиден.

<u>Задача 7</u> Докажите, что $\sigma < \ln\ln z + c$, где $c$ - некоторая постоянная.

Указание. Воспользовавшись формулой

$$n! = \prod_{p\le n} p^{\alpha_p(n)}, \quad \alpha_p(n) = \left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots,$$

докажите сначала, что $\sum\limits_{p\le n} \frac{\ln p}{p} \ge \ln n - c_1$, где $c_1$ – некоторая постоянная.

Так как $z \le \sqrt{x}$, то $\sigma \le \ln\ln\sqrt{x} + c = \ln\ln x + c_1 = w$, где $c_1 = c - \ln 2$. Согласно формуле Стирлинга,

$$s! > \sqrt{2\pi s}\left(\frac{s}{e}\right)^s > \left(\frac{s}{e}\right)^s, \text{ так что}$$

$$W_2 < \sum_{s=\tau+1}^{\infty} \frac{w^s}{s!} < \sum_{s=\tau+1}^{\infty}\left(\frac{ew}{s}\right)^s < \sum_{s=\tau+1}^{\infty}\left(\frac{ew}{\tau}\right)^s.$$

Выберем теперь значение $\tau$ в виде $2([ew]+1)$.
Тогда $\frac{ew}{\tau} \le \frac{1}{2}$ и $W_2 < \sum\limits_{s=\tau+1}^{\infty} 2^{-s} = 2^{-\tau} \le$

$$\le 2^{-2ew} = 2^{-2e(\ln\ln x + c_1)} < c_2(\ln x)^{-\frac{15}{4}}, \text{ где } c_2 = 2^{-2ec_1}.$$

Итак, $W \le \frac{1}{\ln z} + c_2(\ln x)^{-\frac{15}{4}} < \frac{2}{\ln z}$,

$$\pi(x) \le \pi(z) - 1 + xW + |R| \le \frac{2x}{\ln z} + z + z^\tau < \frac{2x}{\ln z} + 2z^\tau,$$

Все, что нам осталось – это выбрать параметр $z$. С одной стороны, $z$ не может быть слишком маленьким: первое слагаемое окажется большим, и ничего нового по сравнению с Теоремой 3 мы не получим. С другой стороны, $z$ не должно быть и очень большим, так как второе слагаемое может перевесить первое. Положим $z = \exp\left(\frac{\ln x}{6\ln\ln x}\right)$.

Тогда $z^\tau = \exp\left(\frac{\tau}{6}\cdot\frac{\ln x}{\ln\ln x}\right) < \exp\left(\frac{1}{6}(2e\ln\ln x + 2ec_1 + 1)\frac{\ln x}{\ln\ln x}\right)$

$= \exp\left(\frac{e}{3}\ln x + c_3\frac{\ln x}{\ln\ln x}\right)$, где $c_3 = \frac{1}{6}(2ec_1+1)$.

Так как $\frac{e}{3} = 0.90\ldots$, то при достаточно большом $x$ получим: $z^\tau < x^{8/9}$, $\pi(x) < \frac{12x}{\ln x}(\ln\ln x) + 2x^{8/9} < \frac{14x}{\ln x}\ln\ln x$, Как уже говорилось, $\pi(x) = (1+\bar{o}(1))\dfrac{x}{\ln x}$, так что полученная оценка не очень впечатляет. Однако метод Бруна можно применять к задачам, в которых точный ответ неизвестен. Одной из таких задач является гипотеза о простых близнецах.

Простые близнецы — это пары простых чисел, отличающихся на двойку, т.е. пары $p, p+2$, где оба числа — простые, например 3 и 5, 5 и 7, 11 и 13, 17 и 19, 29 и 31 и т.д. Упомянутая гипотеза утверждает, что множество таких пар бесконечно. Она до сих пор не доказана.

Введем функцию $\pi_2(x)$, равную количеству таких пар с условием $p \le x$. Хотя мы не знаем, ограничена $\pi_2(x)$ сверху или нет, метод Бруна позволяет получить верхнюю оценку $\pi_2(x)$, следствием которой будет весьма нетривиальный факт — сходимость ряда, составленного из обратных к простым близнецам:

$$\sum_{p,\, p+2 \text{ — простые}} \left(\frac{1}{p} + \frac{1}{p+2}\right) < +\infty.$$

<u>Теорема 4</u> Для достаточно больших $x$ справедлива оценка: $\pi_2(x) < cx\left(\dfrac{\ln\ln x}{\ln x}\right)^2$, где $c>0$ — некоторая постоянная.

<u>Д-во</u>. Пусть $2 < z \le \sqrt{x}$ и $P = P(z) = \prod_{p \le z} p$. Положим

$$a_n = \begin{cases} 1, & \text{если } n = m(m+2) \text{ для некоторого } m,\ 1 \le m \le x, \\ 0, & \text{иначе.} \end{cases}$$

Все произведения $p(p+2)$, отвечающие простым близнецам с условием $z < p \le x$, находятся среди чисел $n = m(m+2)$, взаимно простых с $P(z)$. Следовательно,

$$\pi_2(x) - \pi_2(z) \le S(A,z) \le \sum_{d \mid P} \lambda_d |A_d|.$$

В отличие от предыдущей задачи нахождение $|A_d|$ потребует некоторых усилий. Величина $|A_d|$ равна количеству тех $m$, $1 \le m \le x$, которые делятся на $d$ или, что то же, ~~числу~~ решений сравнения

$$\begin{cases} m(m+2) \equiv 0 \pmod{d}, \\ 1 \le m \le x. \end{cases}$$

Ясно, что если $m_0$ — решение, то число $m_0 + d$ — также решение, и обратно. Поэтому достаточно найти число решений этого сравнения с условием $1 \le m \le d$. Обозначим его через $\nu(d)$.
Предположим сперва, что $d$ — простое. Если $d = 2$, то сравнение принимает вид $m^2 \equiv 0 \pmod{2}$ и имеет, очевидно, единственное решение $m \equiv 0 \pmod{2}$. Если $d > 2$, то вычеты $m \equiv 0 \pmod{d}$ и $m \equiv d-2 \pmod{d}$ будут решениями. Других решений нет: это следует из теоремы Лагранжа. Итак, для простого $d$ имеем:

$$\nu(d) = \begin{cases} 1, & \text{если } d = 2, \\ 2, & \text{если } d > 2. \end{cases}$$

Пусть теперь $d = p_1 \ldots p_k$ — произвольное бесквадратное число. Ясно, что всякое решение исходного сравнения удовлетворяет системе

$$\begin{cases} m(m+2) \equiv 0 \pmod{p_1}, \\ \ldots \\ m(m+2) \equiv 0 \pmod{p_k}. \end{cases}$$

Пусть $m_1, \ldots, m_k$ — произвольные решения первого, …, $k$-го сравнений системы. В силу китайской теоремы об остатках, существует единственный вычет $m_0$ по модулю $d = p_1 \ldots p_k$ такой, что $m_0 \equiv m_1 \pmod{p_1}, \ldots, m_0 \equiv m_k \pmod{p_k}$.
Иными словами, всякий набор $(m_1, \ldots, m_k)$ порождает решение сравнения по модулю $d$. Верно, очевидно, и обратное. Общее количество

различных наборов равно произведению $\nu(p_1)\ldots\nu(p_k)$. Если все числа $p_1,\ldots,p_k$ - нечетные, то $\nu(d)=2^k=2^{\omega(d)}$. Если среди $p_1,\ldots,p_k$ встречается двойка, то $\nu(d)=2^{k-1}=2^{\omega(d)-1}$. Определяя функцию $\omega_a(d)$ как количество простых делителей $d$, не делящих целое число $a$, получим:

$$\nu(d) = 2^{\omega_2(d)}.$$

Переходя к сравнению с условием $1\le n\le x$, число $\nu(d)$ надо домножить на количество отрезков длины $d$, которые полностью укладываются в отрезок $1\le n\le x$. Оставшийся отрезок (если он меньше) содержит не более $\nu(d)$ решений. Следовательно,

$$|A_d| = \nu(d)\left[\frac{x}{d}\right] + \theta_1\nu(d), \quad \text{где } 0\le\theta_1\le 1.$$

Преобразуя это выражение, найдем:

$$|A_d| = xg(d) + r_d, \text{ где } g(d)=\frac{\nu(d)}{d}, \ |r_d|\le\nu(d).$$

Соответственно, $S(A;z)\le xW+R$, где

$$W=\sum_{d|P}\frac{\nu(d)}{d}\lambda_d, \quad |R|\le\sum_{d|P}\nu(d)|\lambda_d|.$$

Как и выше, при оценке $|R|$ воспользуемся тем, что $\lambda_d\ne 0$ лишь в случае $\omega(d)\le r$. Для таких $d$ имеем $\nu(d)\le 2^{\omega(d)}\le 2^r$, так что $|R|\le 2^r\sum_{\substack{\omega(d)\le r\\ d|P}}1\le(2z)^r$. Сумма $W$ оценивается подобно тому, как это делалось выше. Прежде всего,

$$W=\sum_{\substack{d|P\\ \omega(d)\le r}}\frac{\nu(d)\mu(d)}{d} = \Bigg(\sum_{d|P} - \sum_{\substack{d|P\\ \omega(d)>r}}\Bigg)\frac{\nu(d)\mu(d)}{d} = W_1 - W_2.$$

Пользуясь леммой 1, получаем:

$$W_1 = \prod_{p\le z}\left(1-\frac{\nu(p)}{p}\right) = \left(1-\frac12\right)\prod_{2<p\le z}\left(1-\frac{2}{p}\right) < \frac12\prod_{2<p\le z}\left(1-\frac2p+\frac1{p^2}\right) =$$

$$= \frac12\prod_{2<p\le z}\left(1-\frac1p\right)^2 = 2\prod_{p\le z}\left(1-\frac1p\right)^2 < \frac{2}{(\ln z)^2}.$$

Далее, $|W_2| \le w_{\tau+1}+w_{\tau+2}+\dots+w_s+\dots$, где

$$w_s = \sum_{\substack{d\mid P\\ \omega(d)=s}}\frac{\nu(d)}{d} \le \sum_{\substack{d\mid P\\ \omega(d)=s}} \frac{2^{\omega(d)}}{d} = 2^s\sum_{\substack{d\mid P\\ \omega(d)=s}} \frac1d \le \frac{2^s\cdot\sigma^s}{s!} <$$

$< \dfrac{(2w)^s}{s!}$, где $w = \ln\ln x + c_1$.

Вновь пользуясь формулой Стирлинга и полагая $\tau = 4([ew]+1)$, находим:

$$W_2 < \sum_{s=\tau+1}^{+\infty}\left(\frac{2ew}{\tau}\right)^{\tau} < c_2(\ln x)^{-\frac{15}{4}},$$

$$W < \frac{2}{(\ln z)^2} + c_2(\ln x)^{-\frac{15}{4}} < \frac{3}{(\ln z)^2}.$$

Итак,

$$\pi_2(x) \le \pi_2(z) + xW + |R| \le \frac{3x}{(\ln z)^2} + (2z)^{\tau} + z < \frac{3x}{(\ln z)^2}+2(2z)^{\tau}.$$

Положив, наконец, $z=\exp\left(\frac1{12}\frac{\ln x}{\ln\ln x}\right)$, находим:

$$\pi_2(x) < 3\cdot 12^2 x\left(\frac{\ln\ln x}{\ln x}\right)^2 + x^{14/15} < 433x\left(\frac{\ln\ln x}{\ln x}\right)^2,$$

что и требовалось.

Выведем теперь следующее

<u>Следствие</u> Ряд $\displaystyle\sum_{p,\,p+2\text{ — простые}}\left(\frac1p+\frac1{p+2}\right)$ — сходится.

<u>Док-во</u> Положим $\displaystyle S(x) = \sum_{\substack{x<p\le 2x\\ p+2\text{ — простое}}}\left(\frac1p+\frac1{p+2}\right)$. Очевидно, $S_1(x)<S(x)<2S_1(x)$, где

$\displaystyle S_1(x)=\sum_{\substack{x<p\le 2x\\ p+2\text{ — простое}}} \frac1p$. Считая $x\ge x_0$ (где $x_0$ — достаточно велико), будем иметь:

$$S_1(x) \le \frac1x(\pi_2(2x)-\pi_2(x)) \le \frac{\pi_2(2x)}{x} \le \frac1x\cdot 433\cdot 2x\left(\frac{\ln\ln 2x}{\ln 2x}\right)^2 =$$

$= 866 \left( \frac{\ln\ln(2x)}{\ln(2x)} \right)^2$. Определяя $k_0$ из условий $x_0 < 2^{k_0} \le 2x_0$, получим:

$$\sum_{\substack{p,\, p+2 - \text{простые} \\ p > 2x_0}} \frac{1}{p} \le \sum_{k=k_0}^{+\infty} S_1(2^k) \le 866 \sum_{k=k_0}^{+\infty} \left( \frac{\ln\ln(2^{k+1})}{\ln(2^{k+1})} \right)^2 =$$

$$\le 866 \sum_{k=k_0}^{+\infty} \left( \frac{\ln(k+1)}{(k+1)\ln 2} \right)^2 < +\infty,$$ откуда следует искомое утверждение.

<u>Глава 3</u> Модификация решета Бруна

Впоследствии в метод Бруна были внесены различные усовершенствования. Одно из них, предложенное самим Бруном, состоит в следующем.

Выше при построении мажоранты $\lambda_d$ мы ограничились делителями $d$ числа $P$, у которых $\omega(d) \le k$, где $k$ - четное число. Все простые делители таких $d$ не превосходят $z$.

Теперь же вместо $z$ предлагается рассмотреть последовательность точек

$$z = z_1 > z_2 > \dots > z_t \quad \text{с условиями } z_1 < x,\ z_t \ge 2,$$

а вместо $k$ — последовательность четных чисел $k_1, \dots, k_t$. Пусть, далее,

$$P_r = \prod_{z_{r+1} < p \le z_r} p,$$

так что $P_1 P_2 \dots P_t = P = \prod\limits_{p \le z} p$ (для удобства можно считать, что $1 < z_{t+1} < 2$). Тогда всякий делитель $d \mid P$ единственным образом представляется в виде $d_1 \dots d_t$, где $d_r \mid P_r$. Соответственно, для любого целого $n$ справедливы равенства:

$$\sum_{d \mid (n,P)} \mu(d) = \sum_{d_1 \mid (n,P_1)} \mu(d_1) \cdots \sum_{d_t \mid (n,P_t)} \mu(d_t) = X_1 \cdots X_t .$$

Положив $Y_r = \sum\limits_{\substack{d_r \mid (n,P_r) \\ \omega(d_r) \le k_r}} \mu(d_r)$, в силу доказанного выше будем иметь: $0 \le X_r \le Y_r$ и, следовательно,

$$\sum_{d \mid (n,P)} \mu(d) \le Y_1 \cdots Y_t = \prod_{r=1}^{t} \sum_{d_r \mid (n,P_r)} \mu(d_r) =$$

$$= \sum_{\substack{d = d_1 \dots d_t \mid (n,P) \\ \omega(d_r) \le k_r,\ 1 \le r \le t}} \mu(d)$$

Значит, в качестве мажоранты $\lambda_d$ можно взять функцию

$$\lambda_d = \begin{cases} \mu(d), & \text{если } d = d_1 \dots d_t,\ \omega(d_\tau) \le k_\tau,\ \tau = 1, 2, \dots, t, \\ 0, & \text{иначе}. \end{cases}$$

Соответственно,

$$S(A, z) \le \sum_{d|P} \lambda_d |A_d| = \sum_{d_1|P_1} \dots \sum_{d_t|P_t} \mu(d_1) \dots \mu(d_t) |A_{d_1 \dots d_t}| =$$

$$= \sum_{d_1|P_1} \dots \sum_{\substack{d_t|P_t \\ \omega(d_\tau) \le k_\tau,\ \tau=1,\dots,t.}} \mu(d_1) \dots \mu(d_t) \left( X g(d_1 \dots d_t) + r_{d_1 \dots d_t} \right) = XW + R,$$

где $$W = \prod_{\tau=1}^{t} \left( \sum_{\substack{d_\tau | P_\tau \\ \omega(d_\tau) \le k_\tau}} \mu(d_\tau) g(d_\tau) \right).$$

Преимущество такой модификации легко увидеть на примере оценки величины $R$. Действительно, для всякого числа $d_\tau$ справедливо неравенство:

$$d_\tau \le z_\tau^{\omega(d_\tau)} \le z_\tau^{k_\tau}.$$

Следовательно, для чисел $d$, отвечающих ненулевым значениям мажоранты $\lambda_d$, имеем оценку:

$$d = d_1 \dots d_t \le z_1^{k_1} \dots z_t^{k_t} = \mathcal{D}.$$

В качестве $z_\tau$ часто берут числа

$$z_1 = z,\quad z_2 = \sqrt{z_1} = z^{\frac{1}{2}},\quad z_3 = \sqrt{z_2} = z^{\frac{1}{2^2}},\ \dots,\ z_\tau = z^{\frac{1}{2^{\tau-1}}},\ \dots,$$

а в качестве $k_\tau$ – числа вида $b + 2(\tau - 1)$, где $b \ge 2$ – фиксированное чётное число. Такой выбор даёт:

$$\mathcal{D} \le z^a,\quad a = b + \frac{b+2}{2} + \frac{b+4}{2^2} + \frac{b+6}{2^3} + \dots + \frac{b+2(\tau-1)}{2^\tau} + \dots <$$

$< 2b+4$. Следовательно, $|R| < \sum_{\substack{d|P \\ d < z^{2b+4}}} |r_d|$. Обратите внимание: степень $z$ – величина $2b+4$ – теперь константа! Раньше мы были вынуждены брать её растущей (как $\ln\ln x$), и это приводило к появлению в оценках $\pi(x)$, $\pi_2(x)$ "лишних" множителей $\ln\ln x$, $(\ln\ln x)^2$.

Но ещё необходимо подходящим образом оценить произведение $W = W_1 \ldots W_t$. Мы начнем с простого наблюдения. Пусть $m$ — произвольное бесквадратное число, имеющее по крайней мере $(k+1)$ простых делителей, и пусть

$$w = \sum_{\substack{d|m \\ \omega(d)\le k}} \mu(d) g(d) = \Big(\sum_{d|m} - \sum_{\substack{d|m \\ \omega(d)>k}}\Big) \mu(d) g(d) = w_1 - w_2.$$

Тогда знак «хвоста» $w_2$ зависит лишь от чётности $k$. Действительно, всякое $d|m$ с условием $\omega(d)>k$ можно представить в виде $d = p_1 \cdots p_k p_{k+1} \cdots p_s$, где $s=\omega(d)$ и $p_1 > \cdots > p_k > p_{k+1} > \cdots > p_s$. Положив $\delta = p_1 \cdots p_{k+1}$, $\Delta = d/\delta$, будем иметь: $p^+(\Delta) < p^-(\delta)$, где через $p^+(n)$ и $p^-(n)$ обозначены, соответственно, наибольший и наименьший простые делители $n$ (для $n=1$ обе величины полагаем равными единице).

Тогда $$w_2 = \sum_{\substack{\delta|m \\ \omega(\delta)=k+1}} \sum_{\substack{\Delta|\frac{m}{\delta} \\ p^+(\Delta)<p^-(\delta)}} \mu(\delta\Delta) g(\delta\Delta) =$$

$$= \sum_{\substack{\delta|m \\ \omega(\delta)=k+1}} \mu(\delta) g(\delta) \sum_{\substack{\Delta|\frac{m}{\delta} \\ p^+(\Delta)<p^-(\delta)}} \mu(\Delta) g(\Delta) = \sum_{\substack{\delta|m \\ \omega(\delta)=k+1}} \mu(\delta) g(\delta) \prod_{p|\frac{m}{\delta},\, p<p^-(\delta)} (1-g(p))$$

$$= (-1)^{k+1} \sum_{\substack{\delta|m \\ \omega(\delta)=k+1}} g(\delta) \prod_{p|\frac{m}{\delta},\, p<p^-(\delta)} (1-g(p))$$

В силу того, что $0 \le g(p) < 1$ для всех рассматриваемых $p$, последняя сумма (по $\delta|m$) неотрицательна. Следовательно, знак $w_2$ совпадает с $(-1)^{k+1}$.

Соответственно, при $k$-чётном имеем:

$$-w_2 = \sum_{\substack{\delta|m \\ \omega(\delta)=k+1}} g(\delta) \prod_{p|\frac{m}{\delta},\, p<p^-(\delta)} (1-g(p)) \le \sum_{\substack{\delta|m \\ \omega(\delta)=k+1}} g(\delta)$$

Воспользуемся теперь "трюком Эрдеша":

$$\sum_{\substack{\delta | m \\ \omega(\delta)=k+1}} g(\delta) \le \frac{1}{(k+1)!} \left( \sum_{p|m} g(p) \right)^{k+1}.$$

Далее, замечая, что $g(p) \le -\ln(1-g(p))$, оценим правую часть величиной

$$\frac{1}{(k+1)!} \left( -\sum_{p|m} \ln(1-g(p)) \right)^{k+1} =$$

$$= \frac{1}{(k+1)!} \left( \ln \prod_{p|m} (1-g(p))^{-1} \right)^{k+1}$$

Возвращаясь к исходной сумме $w$ и пользуясь очевидным равенством

$$w_1 = \sum_{d|m} \mu(d) g(d) = \prod_{p|m} (1-g(p)),$$

находим:

$$w \le w_1 + \frac{1}{(k+1)!} \left( \ln \frac{1}{w_1} \right)^{k+1} = w_1 \left( 1 + \frac{1}{w_1} \frac{\left( \ln \frac{1}{w_1} \right)^{k+1}}{(k+1)!} \right).$$

Возьмём в качестве $m$ величину $P_r = \prod_{z_{r+1} \le p < z_r} p$ и обозначим $V_r = \prod_{z_{r+1} \le p < z_r} (1-g(p))$, $L_r = \ln \frac{1}{V_r}$. Тогда в силу доказанного будем иметь:

$$W_r = \sum_{\substack{d | P_r \\ \omega(d) \le k_r}} \mu(d) g(d) \le V_r \left( 1 + \frac{1}{V_r} \frac{\left( \ln \frac{1}{V_r} \right)^{k_r+1}}{(k_r+1)!} \right) =$$

$$= V_r \left( 1 + \frac{e^{L_r} L_r^{k_r+1}}{(k_r+1)!} \right).$$

перемножая эти неравенства по всем $r$, $1 \le r \le t$, и пользуясь тем, что $1+x \le e^x$, находим:

$$W_1 \dots W_t \le (V_1 \dots V_t) \prod_{r=1}^{t} \left( 1 + \frac{e^{L_r} L_r^{k_r+1}}{(k_r+1)!} \right) < V \exp(E), \text{ где}$$

$$V = V(z) = V_1 \dots V_t = \prod_{p<z} (1-g(p)), \quad E = \sum_{r=1}^{t} \frac{e^{L_r} L_r^{k_r+1}}{(k_r+1)!}$$

Чтобы двигаться дальше, нужна некоторая дополнительная информация о поведении $g$.

Как и выше, будем считать, что мультипликативная функция $g(d)$ удовлетворяет для всех бесквадратных $d$ неравенствам $0 \le g(d) < 1$. Кроме того, будем также предполагать, что при любых $u$ и $v$ справедлива оценка

$$\prod_{u \le p < v} (1-g(p))^{-1} \le \left(\frac{\ln v}{\ln u}\right)^{\varkappa} \left(1 + \frac{K}{\ln u}\right),$$

где $\varkappa$ и $K$ — некоторые абсолютные положительные постоянные. Ввиду особой важности первой из них присвоено название размерности решета.

Тогда для чисел $z_\tau = z^{\frac{1}{2^{\tau-1}}}$ будем иметь:

$$U_\tau \le 2^{\varkappa}\left(1 + \frac{2^\tau K}{\ln z}\right), \quad L_\tau \le \varkappa \ln 2 + \frac{2^\tau K}{\ln z}$$

$$E \le 2^{\varkappa} \sum_{\tau=1}^{t} \left(1 + \frac{2^\tau K}{\ln z}\right)\left(\varkappa \ln 2 + \frac{2^\tau K}{\ln z}\right)^{b+2\tau-1} \frac{1}{(b+2\tau-1)!}$$

В силу формулы конечных приращений и неравенства Гёльдера, для любых положительных $\xi, \eta$ и целого $m \ge 3$ имеем:

$$(\xi+\eta)^m - \xi^m \le m\eta(\xi+\eta)^{m-1} \le 2^{m-2} m\eta\left(\xi^{m-1} + \eta^{m-1}\right) =$$
$$= m\left(\tfrac{1}{2}(2\xi)^{m-1}\eta + \tfrac{1}{4}(2\eta)^{m-1}\right).$$

Полагая $\xi = \varkappa \ln 2$, $\eta = \frac{2^\tau K}{\ln z}$, $m = b + 2\tau - 1$, получим:

$$E \le 2^{\varkappa} \sum_{\tau=1}^{t} \left(1 + \frac{2^\tau K}{\ln z}\right)\Big( (\varkappa \ln 2)^{b+2\tau-1} + (b+2\tau-1) \times$$
$$\times \left\{ \tfrac{1}{2}(2\varkappa \ln 2)^{b+2\tau-2} \frac{2^\tau K}{\ln z} + \frac{1}{4}\left(\frac{2^{\tau+1} K}{\ln z}\right)^{b+2\tau-2} \right\}\Big) \frac{1}{(b+2\tau-1)!}$$

При перемножении скобок возникнут шесть слагаемых, вклад от которых удобно записать, введя обозначения

$$F(b;y) = \sum_{r=1}^{+\infty} \frac{y^{b+2r-1}}{(b+2r-1)!} = \operatorname{sh}(y) - \sum_{r=1}^{b/2} \frac{y^{b+2r-1}}{(b+2r-1)}.$$

Тогда, проведя несложные выкладки, получим:

$$E \le 2^{\varkappa} \sum_{j=0}^{5} E_j,$$

где
$$E_0 = \sum_{r=1}^{+\infty} \frac{(\varkappa \ln 2)^{b+2r-1}}{(b+2r-1)!} = F(b; \varkappa \ln 2),$$

$$E_1 = \sum_{r=1}^{+\infty} \frac{2^r K}{\ln z} \cdot \frac{(\varkappa \ln 2)^{b+2r-1}}{(b+2r-1)!} = \frac{1}{\ln z} \cdot \frac{K}{2^{(b-1)/2}} F(b; \varkappa \sqrt{2} \ln 2) = \Vdash\!\!\to$$ см. стр. 58

$$E_2 = \sum_{r=1}^{+\infty} \frac{2^r K}{2 \ln z} \cdot \frac{(2\varkappa \ln 2)^{b+2r-2}}{(b+2r-2)!} \le \frac{c_2}{\ln z},$$

$$E_3 = \sum_{r=1}^{+\infty} \frac{1}{2} \left( \frac{2^r K}{\ln z} \right)^2 \frac{(2\varkappa \ln 2)^{b+2r-2}}{(b+2r-2)!} \le \frac{c_3}{(\ln z)^2},$$

$$E_4 = \frac{1}{8} \sum_{1 \le r \le t} \left( \frac{2^{r+1} K}{\ln z} \right)^{b+2r-1} \frac{1}{(b+2r-2)!}$$

$$E_5 = \frac{1}{4} \sum_{1 \le r \le t} \left( \frac{2^{r+1} K}{\ln z} \right)^{b+2r-2} \frac{1}{(b+2r-2)!}$$

Поскольку $\frac{\ln z}{2^t} < \ln 2 \le \frac{\ln z}{2^{t-1}}$, то $2^t \le \frac{2 \ln z}{\ln 2}$ и

$\frac{2^{r+1} K}{\ln z} \le \frac{4K}{\ln 2}$ при любом $r \le t$, то $E_4 \le \frac{2K}{\ln 2} E_5$.

Далее, определим $s$ из неравенств
$$2^s \le \frac{\sqrt{\ln z}}{2K} < 2^{s+1}.$$

Тогда вклад от $r \le s$ в сумму $E_5$ не превзойдет

$$\frac{1}{8} \sum_{r=1}^{s} \left( \frac{1}{\sqrt{\ln z}} \right)^{b+2r-2} \frac{1}{(b+2r-2)!} \le \frac{1}{(\ln z)^{b/2}} \cdot \frac{1}{8} \sum_{r=1}^{\infty} \frac{1}{(b+2r-2)!} \le$$

$$\le \frac{c_5}{\ln z}.$$

Далее, если $s < r \le t$, то $\left( \frac{2^{r+1} K}{\ln z} \right)^{b+2r-2} \frac{1}{(b+2r-2)!} \le$

$$\le \left(\frac{4K}{\ln 2}\cdot\frac{e}{b+2r-2}\right)^{b+2r-2} \le \left(\frac{2eK}{r\ln 2}\right)^{b+2r-2} < \left(\frac{8K}{s}\right)^{b+2r-2}$$

Поскольку $s > \frac{1}{\ln 2}\ln\left(\frac{\sqrt{\ln z}}{2K}\right) = \frac{1}{2\ln 2}\ln\ln z - \frac{\ln(2K)}{\ln 2} > \frac{2}{3}\ln\ln z$,

то вклад от $s<r\le t$ в $E_5$ не превосходит

$$\frac{1}{4}\sum_{r=s+1}^{+\infty}\left(\frac{8K}{s}\right)^{b+2r-2} \le \frac{1}{3}\left(\frac{8K}{s}\right)^{b+2s} \le \frac{1}{3}\left(\frac{12K}{\ln\ln z}\right)^{b+\frac{4}{3}\ln\ln z}$$

$$< e^{-(\ln\ln z)(\ln\ln\ln z)} < e^{-2\ln\ln z} = \frac{1}{(\ln z)^2}.$$

Следовательно,

$$E_5 < \frac{c_5}{\ln z} + \frac{1}{(\ln z)^2} < \frac{2c_5}{\ln z}, \quad E_4 < \frac{2K}{\ln 2}\cdot\frac{2c_5}{\ln z} = \frac{c_6}{\ln z}.$$

Окончательно находим:

$$E \le 2^{\varkappa} F(b;\varkappa\ln 2) + \frac{c}{\ln z},$$ где $c=c(\varkappa,b,K)$

не зависит от $z$. Так приходим к следующему утверждению

Теорема 5. Пусть последовательность неотрицательных чисел $a_n$, $n\in A$, такова, что

$$|A_d| = Xg(d)+r_d$$

для любого бесквадратного $d$, причем мультипликативная функция $g$ удовлетворяет условиям:

(a) $0\le g(p)<1$ для любого простого $p$;

(b) $\prod_{u\le p<v}(1-g(p))^{-1} \le \left(\frac{\ln v}{\ln u}\right)^{\varkappa}\left(1+\frac{K}{\ln u}\right)$

для любых чисел $u$ и $v$ с условиями $\frac{3}{2}\le u<v$, где $\varkappa, K$ — положительные постоянные. Тогда для просеивающей функции $S(A,z) = \sum_{n\in A,\ (n,P(z))=1} a_n$ справедливо неравенство:

$$S(A,z) \le XV(z)e^{E} + R,$$

где $V(z)=\prod_{p<z}(1-g(p))$, $R=\sum_{d|P(z),\ d\le \mathcal{D}}|r_d|$, $\mathcal{D}=z^{2b+4}$,

$E\le 2^{\varkappa}F(b;\varkappa\ln 2)+\frac{c}{\ln z}$, $F(b;y)=\sum_{r=1}^{+\infty}\frac{y^{b+2r-1}}{(b+2r-1)!}$, а $c=c(\varkappa,b,K)$ — некоторая постоянная.

Задача 8 Пользуясь теоремой 5 наряду с формулой Мертенса, получить оценки

$$\pi(x) < c_1 \frac{x}{\ln x}, \qquad \pi_2(x) < c_2 \frac{x}{(\ln x)^2}$$

с явно вычисленными постоянными $c_1$ и $c_2$ (можно положить, например, $c_1 = 5.1$, $c_2 = 285$).

Задача 9 Пользуясь тем, что

(a) сравнение $n^2+1 \equiv 0 \pmod p$ в случае $p \equiv 3 \pmod 4$ не имеет решений, а в случае $p \equiv 1 \pmod 4$ имеет 2 решения с условием $1 \le n \le p$,

а также тем, что

(b) $$\prod_{\substack{p \le z \\ p \equiv 1 \pmod 4}} \left(1 - \frac{2}{p}\right) = \frac{c}{\ln z}\left(1 + O\left(\frac{1}{\ln z}\right)\right),$$

где $C$ — некоторая абсолютная постоянная, получить верхнюю оценку для количества простых чисел вида $p = n^2+1$, $p \le x$.

Задача 10. Пусть $x$ достаточно велико, $a, b$ — целые числа (разной чётности), $(a, b) = 1$, $1 \le a, b \le x$. Оцените сверху количество тех простых $p$, $p \le x$, для которых число $ap+b$ — также простое.

Замечание. В случае $a = 2$, $b = 1$ получим пары простых чисел вида $p$, $2p+1$. Такие простые числа $p$ называются простыми Софи Жермен.

## Глава 4. Решето Бруна: нижние оценки

Все полученные выше результаты носят "негативный характер": мы оцениваем сверху нечто, что может, вообще говоря, оказаться ограниченной величиной. Так, мы не знаем, конечно или нет множество простых Софи Жермен, множество пар простых близнецов и так далее. Можно ли методом решета получать "позитивные" результаты, пусть даже и не столь сильные?

Так, выше мы оценивали сверху величину $S(A;z)$, равную числу целых $n$, $1 \le n \le x$, для которых $n$ и $n+2$ взаимно просты с произведением $P = P(z) = \prod_{p \le z} p$. В модифицированном решете Бруна в качестве $z$ можно брать величину вида $x^{\delta}$, где $\delta = \frac{1-\varepsilon}{2b+4}$, а $\varepsilon$ – сколь угодно малая фиксированная постоянная. Но что значит условие $(n(n+2), P) = 1$? Оно означает, что все простые делители чисел $n$ и $n+2$ превосходят $z = x^{\delta}$. Значит, их не может быть много! Именно, их число не может превосходить величина $k = [\frac{1}{\delta}] + 1$. Если $\varepsilon$ – достаточно мало, то $k \le 2b+5$.

Следовательно, если бы нам удалось найти для $S(A,z)$ нижнюю оценку того же порядка, что и в теореме ..., то тем самым было бы установлено существование абсолютной постоянной $k$ такой, что множество пар чисел $n, n+2$, каждое из которых имеет не более $k$ простых сомножителей, бесконечно. Это было бы серьезным продвижением в решении проблемы простых близнецов.

Оказывается, методы решета позволяют получать нижние оценки такого рода, однако соответствующие рассуждения оказываются более тонкими. Причина этого достаточно очевидна. Задавшись неотрицательными числами $k_r$, $1 \le r \le t$, мы получим суммы

$$\sum_{\substack{d_r \mid (n, P_r) \\ \omega(d_r) \le k_r}} \mu(d_r), \quad r = 1, 2, \dots, t,$$

которые являются нижними оценками сумм,

$$\sum_{d_r \mid (n, P_r)} \mu(d_r)$$

однако их произведение, вообще говоря, уже не будет нижней оценкой суммы

$$\sum_{d \mid (n, P)} \mu(d) = \prod_{r=1}^{t} \sum_{d_r \mid (n, P_r)} \mu(d_r).$$

Тем не менее, доказательство теоремы ... можно надлежащим образом модифицировать и все-таки получить искомую нижнюю оценку. В основе этого рассуждения лежит следующая лемма, принадлежащая К. Форду и Х. Халберстаму.

<u>Лемма</u>. Пусть $0 \le x_r \le y_r$, $r = 1, \dots, t$ – два набора неотрицательных чисел. Тогда

$$x_1 \dots x_t \ge y_1 \dots y_t - \sum_{r=1}^{t} (y_r - x_r) \prod_{j \ne r} y_j.$$

<u>Док-во</u>. При $t = 1$ неравенство имеет вид $x_1 \ge y_1 - (y_1 - x_1)$ и, очевидно, справедливо. Предположим, что утверждение леммы доказано для всех $t \le m$, и проверим его справедливость для $t = m+1$. Имеем:

$$x_1 \dots x_{m+1} = x_1 \dots x_m \cdot x_{m+1} \ge \Big( y_1 \cdots y_m - \sum_{r=1}^{m} (y_r - x_r) \prod_{\substack{j=1 \\ j \ne r}}^{m} y_j \Big) x_{m+1}$$

$$= y_1 \cdots y_m x_{m+1} - \sum_{r=1}^{m} (y_r - x_r) \Big( \prod_{j=1, j \ne r}^{m} y_j \Big) x_{m+1} \ge$$

$$\ge y_1 \cdots y_m (y_{m+1} - (y_{m+1} - x_{m+1})) - \sum_{r=1}^{m} (y_r - x_r) \prod_{\substack{1 \le j \le m+1 \\ j \ne r}} y_j =$$

$$= y_1 \cdots y_{m+1} - \sum_{r=1}^{m+1} (y_r - x_r) \prod_{\substack{1 \le j \le m+1 \\ j \ne r}} y_j,$$ что и требовалось.

Применим теперь неравенство леммы к наборам

$$x_r = X_r = \sum_{d_r | (n, P_r)} \mu(d_r), \quad y_r = Y_r = \sum_{\substack{d_r | (n, P_r) \\ \omega(d_r) \le k_r}} \mu(d_r),$$

где, как и выше, $k_1, \dots, k_t$ - четные числа.

Для начала заметим, что

$$0 \le Y_r - X_r = - \sum_{\substack{d_r | (n, P_r) \\ \omega(d_r) > k_r}} \mu(d_r).$$

Знак последней суммы совпадает с $(-1)^{k_r+1} = -1$. Действительно, пусть $m$ — произвольное бесквадратное число, $k$ - четное, и пусть $w = \sum_{\substack{d | m \\ \omega(d) > k}} \mu(d)$. Всякое $d$ в сумме единственным образом представляется в виде $\delta\Delta$, где $\omega(\delta) = k+1$, а $p^+(\Delta) < p^-(\delta)$. Получим:

$$w = \sum_{\substack{\delta | m \\ \omega(\delta) = k+1}} \sum_{\substack{\Delta | \frac{m}{\delta} \\ p^+(\Delta) < p^-(\delta)}} \mu(\delta\Delta) = (-1)^{k+1} \sum_{\substack{\delta | m \\ \omega(\delta) = k+1}} \sum_{\substack{\Delta | \frac{m}{\delta} \\ p^+(\Delta) < p^-(\delta)}} \mu(\Delta)$$

Если $q$ есть произведение всех простых делителей $m$, меньших $p^-(\delta)$, то сумма по $\Delta$ есть просто

$\sum_{\Delta | q} \mu(\Delta)$ и потому неотрицательна и не превосходит единицы. Поэтому $(-1)^{k+1} w \le \sum_{\substack{\delta | m \\ \omega(\delta) = k+1}} 1$.

Следовательно, беря $m = (n, P_r)$, $k = k_r$, получим:

$$0 \le Y_r - X_r \le \sum_{\substack{\delta_r | (n, P_r) \\ \omega(\delta_r) = k_r + 1}} 1.$$

Применяя лемму ..., заключаем:

$$X_1 \cdots X_t \ge Y_1 \cdots Y_t - \sum_{r=1}^{t} \Bigg( \sum_{\substack{\delta_r | (n, P_r) \\ \omega(\delta_r) = k_r + 1}} 1 \Bigg) \prod_{j \ne r} Y_j$$

или, что то же,

$$\sum_{d|(P,n)} \mu(d) \geqslant \sum_{\substack{d_1\dots d_t | (P,n) \\ \omega(d_r)\le k_r}} \mu(d_1)\dots\mu(d_r) -$$

$$- \sum_{r=1}^{t} \Big( \sum_{\substack{d_r | (P_r,n) \\ \omega(d_r) = k_r+1}} 1 \Big) \prod_{j\ne r} \Big( \sum_{\substack{d_j | (P_j,n) \\ \omega(d_j)\le k_j}} \mu(d_j) \Big) =$$

$$= \sum_{\substack{d_1\dots d_t | (P,n) \\ \omega(d_r)\le k_r}} \mu(d_1)\dots\mu(d_r) - \sum_{r=1}^{t} \sum_{\substack{d_1\dots d_t | (P,n) \\ \omega(d_r) = k_r+1, \\ \omega(d_j)\le k_j,\ j\ne r}} \mu\Big(\frac{d_1\dots d_t}{d_r}\Big).$$

Правая часть последнего неравенства и послужит искомой минорантой.

Переходя к нижней оценке $S(A,z)$, получим:

$$S(A,z) = \sum_{(n,P)=1} a_n = \sum_n a_n \Big( \sum_{d|(n,P)} \mu(d) \Big) \geqslant$$

$$\geqslant \sum_n a_n \sum_{\substack{d_1\dots d_t | (P,n) \\ \omega(d_r)\le k_r}} \mu(d_1)\dots\mu(d_r) -$$

$$- \sum_n a_n \sum_{r=1}^{t} \sum_{\substack{d_1\dots d_t | (P,n) \\ \omega(d_r) = k_r+1 \\ \omega(d_j)\le k_j,\ j\ne r}} \mu\Big(\frac{d_1\dots d_t}{d_r}\Big) =$$

$$= \sum_{\substack{d_1\dots d_t | P \\ \omega(d_r)\le k_r}} \mu(d_1)\dots\mu(d_r) \sum_{n\equiv 0 (\mathrm{mod}\ d_1\dots d_t)} a_n -$$

$$- \sum_{r=1}^{t} \sum_{\substack{d_1\dots d_t | P \\ \omega(d_r) = k_r+1}} \mu\Big(\frac{d_1\dots d_t}{d_r}\Big) \sum_{n\equiv 0 (\mathrm{mod}\ d_1\dots d_t)} a_n$$

Как и выше, будем предполагать, что

$$|A_d| = X g(d) + r_d$$

для всякого бесквадратного $d$, причем мультипликативная функция $g$ удовлетворяет условиям Теоремы ...

Тогда

$$S(A,z) = \sum_{\substack{d_1\dots d_t \mid P \\ \omega(d_\tau)\le k_\tau}} \mu(d_1)\dots\mu(d_t)\left( X g(d_1)\dots g(d_t) + r_{d_1\dots d_t}\right) -$$

$$- \sum_{\tau=1}^{t} \sum_{\substack{d_1\dots d_t \mid P \\ \omega(d_\tau) = k_\tau+1}} \mu\left(\frac{d_1\dots d_t}{d_\tau}\right)\left( X g(d_1)\dots g(d_t) + r_{d_1\dots d_t}\right) =$$

$= X W + R_1 - X W^* - R_2$, где смысл обозначений ясен. Оценим сначала $R_1$ и $R_2$. Повторяя дословно оценку $R$ из теоремы ..., получим: $d = d_1\dots d_t \le z^{2\beta+4}$ для всякого слагаемого суммы $W$. Ввиду того, что для всякого $d = d_1\dots d_t$ из суммы $W^*$ найдется номер $\tau$ с условием $\omega(d_\tau) = k_\tau+1$, получаем: $d \le z^{2\beta+5}$. Так как числа $d$, отвечающие слагаемым сумм $W$ и $W^*$, не повторяются, то окончательно находим: $|R_1|+|R_2| \le R$, где

$$R = \sum_{\substack{d \mid P \\ d \in \mathcal{D}}} |r_d|, \text{ где } \mathcal{D} = z^{2\beta+5}.$$

Далее, пользуясь введенными ранее обозначениями, находим: $W = W_1 \dots W_t$. Кроме того,

$$W^* = \sum_{\tau=1}^{t} \left( \sum_{\substack{d_\tau \mid P_\tau \\ \omega(d_\tau)=k_\tau+1}} g(d_\tau)\right) \prod_{j\ne\tau} \left( \sum_{\substack{d_j \mid P_j \\ \omega(d_j)\le k_j}} \mu(d_j) g(d_j)\right) =$$

$$= \sum_{\tau=1}^{t} \left( \sum_{\substack{d_\tau \mid P_\tau \\ \omega(d_\tau)=k_\tau+1}} g(d_\tau)\right) \prod_{j\ne\tau} W_j .$$

Естественно считать, что все суммы $W_j$ строго положительны: в противном случае ничего, кроме тривиальной оценки $S(A,z)$, нам получить не удастся. Тогда

$$W^* = W_1 \dots W_t \sum_{\tau=1}^{t} \frac{1}{W_\tau} \left( \sum_{\substack{d_\tau \mid P_\tau \\ \omega(d_\tau)=k_\tau+1}} g(d_\tau)\right)$$

Но сумма по $d_\tau$ легко оценивается с помощью трюка Эрдеша:

$$\sum_{\substack{d_r \mid P_r \\ \omega(d_r)=k_r+1}} g(d_r) \le \frac{\left(\ln \frac{1}{V_r}\right)^{k_r+1}}{(k_r+1)!} = \frac{L_r^{k_r+1}}{(k_r+1)!},$$ где, как и выше,

$$V_r = \prod_{z_{r+1} \le p < z_r} (1-g(p)), \quad L_r = \ln \frac{1}{V_r}.$$ Итак,

$$W^* \le W_1 \dots W_t \sum_{r=1}^{t} \frac{1}{W_r} \cdot \frac{L_r^{k_r+1}}{(k_r+1)!} \le W_1 \dots W_t \sum_{r=1}^{t} \frac{1}{V_r} \frac{L_r^{k_r+1}}{(k_r+1)!} =$$

$$= W_1 \dots W_t \sum_{r=1}^{t} \frac{e^{L_r} L_r^{k_r+1}}{(k_r+1)!} = W_1 \dots W_t E.$$

Собирая полученные оценки, находим:

$$S(A,z) \ge XV(z)(1-E) - R.$$

Тем самым доказана

<u>Теорема 6</u>. Если последовательность неотрицательных чисел $a_n$, $n \in A$, и отвечающая ей мультипликативная функция $g$ удовлетворяют условиям теоремы 5, то для просеивающей функции $S(A,z)$ справедливо неравенство:

$$S(A,z) \ge XV(z)(1-E) - R,$$

в котором $E$ – то же, что и в теореме 5, а $R = \sum_{d \mid P, d \le \mathcal{D}} |r_d|$, где $\mathcal{D} = z^{2B+5}$.

Выбор чисел $z_r$ в виде $z_r = z^{\frac{1}{2^{r-1}}}$ не всегда оптимален. Поэтому можно ввести положительный параметр $\lambda$ и выбирать $z_r$ в виде $z^{e^{-(r-1)\lambda}}$ (исходной выбор отвечает, очевидно, $\lambda = \ln 2$). Дословное повторение доказательств теорем 5 и 6 приводит к следующему общему утверждению:

<u>Теорема 7</u>. Пусть последовательность неотрицательных чисел $a_n$, $n \in A$, такова, что для любого бесквадратного $d$ выполнено равенство

$$|A_d| = \sum_{\substack{n \in A \\ n \equiv 0 \pmod d}} a_n = Xg(d) + r_d$$

где $X>0$, а мультипликативная функция $g$ удовлетворяет следующим условиям:

(a) $0 \le g(p) < 1$ для любого простого $p$;

(b) существуют неотрицательные постоянные $\varkappa$ и $K$ такие, что для любых чисел $u$ и $v$, $1<u<v$, справедлива оценка

$$\prod_{u<p\le v} (1-g(p))^{-1} \le \left(\frac{\ln v}{\ln u}\right)^{\varkappa} \left(1+\frac{K}{\ln u}\right).$$

Тогда для любого четного $b \ge 2$ и любого $\lambda>0$ существуют постоянные $c=c(b,\varkappa,\lambda,K)$ и $z_0 = z_0(b,\varkappa,\lambda,K)$ такие, что при любом $z \ge z_0$ для величины

$$S(A,z) = \sum_{\substack{n\in A\\ (n,P)=1}} a_n, \quad P=P(z)=\prod_{p\le z} p,$$

выполняются неравенства:

$$XV(z)(1-E) - R_1 \le S(A,z) \le XV(z)e^{E} + R_0,$$

$$R_j = \sum_{\substack{d\mid P\\ d\le \mathcal{D}_j}} |r_d|, \quad \mathcal{D}_0 = z^{\Delta}, \quad \mathcal{D}_1 = z^{\Delta+1}, \quad \Delta = \frac{b}{1-e^{-\lambda}} + \frac{2e^{-\lambda}}{(1-e^{-\lambda})^2},$$

$$V(z) = \prod_{p\le z}(1-g(p)), \quad E = F(b,\varkappa\lambda) + \frac{c}{\ln z},$$

$$F(b,y) = \sum_{r=1}^{+\infty} \frac{y^{b+2r-1}}{(b+2r-1)!} = \operatorname{sh} y - \sum_{\substack{n=1\\ n\equiv 1 \pmod 2}}^{b-1} \frac{y^n}{n!}.$$

В качестве иллюстрации применим Теорему 7 к доказательству следующего утверждения, которое является шагом по направлению к решению бинарной проблемы Гольдбаха. Напомним, что последняя состоит в том, чтобы доказать разрешимость в нечетных простых числах $p_1, p_2$ уравнения $p_1+p_2=2N$, где $N\ge 3$ - любое целое число.

<u>Теорема 8</u> Существует абсолютная постоянная $N_0$ такая, что при любом целом $N \ge N_0$ число $2N$ представляется суммою $a+b$, в которой каждое из слагаемых имеет не более 10 простых делителей.

<u>Док-во</u>. Рассмотрим последовательность

$$a_n = \begin{cases} 1, \text{ если } n = m(2N-m) \text{ для некоторого } m, \\ \quad 3 \le m \le 2N-3, \\ 0, \text{ в противном случае.} \end{cases}$$

Тогда для бесквадратного $d$ имеем:

$$|A_d| = \sum_{\substack{3 \le m \le 2N-3 \\ m(2N-3) \equiv 0 \pmod d}} 1 = \left[\frac{2N-5}{d}\right] \nu(d) + \theta_1 \nu(d),$$

где $\nu(d)$ - число решений сравнения $m(2N-3) \equiv 0 \pmod d$ с условием $1 \le m \le d$. Несложно видеть, что при $d = p$ - простом

$$\nu(p) = \begin{cases} 1, \text{ если } p \mid 2N, \\ 2, \text{ иначе.} \end{cases}$$

Следовательно, $\nu(d) = 2^{\omega_{2N}(d)}$, где, как и выше, $\omega_c(n)$ - число простых делителей $n$, не делящих $c$.

Отсюда заключаем, что условие (а) теоремы 7 выполнено с $g(d) = \frac{\nu(d)}{d}$, $|r_d| \le \nu(d) \le 2^{\omega(d)}$ и $X = 2N$.

Далее, пусть $2 < u < v$ - произвольные числа. Тогда

$$\prod_{u < p \le v} (1 - g(p))^{-1} = \prod_{u < p \le v} \left(1 - \frac{2^{\omega_{2N}(p)}}{p}\right)^{-1} = \prod_{\substack{u < p \le v \\ p \mid 2N}} \left(1 - \frac{1}{p}\right)^{-1} \cdot$$

$$\cdot \prod_{\substack{u < p \le v \\ p \nmid 2N}} \left(1 - \frac{2}{p}\right)^{-1} \le \prod_{\substack{u < p \le v \\ p \mid 2N}} \left(1 - \frac{2}{p}\right)^{-1} \prod_{\substack{u < p \le v \\ p \nmid 2N}} \left(1 - \frac{2}{p}\right)^{-1} = \prod_{u < p \le v} \left(1 - \frac{2}{p}\right)^{-1}$$

(в силу неравенства $u > 2$ множитель, отвечающий $p = 2$, в произведении отсутствует).

Теперь заметим, что

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

Обозначая через $q$ наименьшее простое с условием $q > u$, будем иметь

$$\prod_{u < p \le v} \left(1 - \frac{2}{p}\right)^{-1} \le \prod_{u < p \le v} \left(1 - \frac{1}{p}\right)^{-2} \prod_{p > u} \frac{(p-1)^2}{p(p-2)}.$$

Несложно проверить, что второе произведение не превосходит

$$\prod_{n=q}^{+\infty} \frac{(n-1)^2}{n(n-2)} = \frac{q-1}{q-2} = 1 + \frac{1}{q-2}.$$

Но $q \geq 3$, так что $q-2 \geq \frac{q}{3} > \frac{u}{3}$. Следовательно, по формуле Мертенса находим:

$$\prod_{u<p\leq v}\left(1-\frac{2}{p}\right)^{-1} \leq \left\{\frac{\prod\limits_{p\leq u}\left(1-\frac{1}{p}\right)}{\prod\limits_{p\leq v}\left(1-\frac{1}{p}\right)}\right\}^2\left(1+\frac{3}{u}\right) = \left(\frac{\ln v}{\ln u}\right)^2 \times$$

$$\times\left(1+\underline{O}\left(\frac{1}{\ln u}\right)\right)\left(1+\underline{O}\left(\frac{1}{\ln v}\right)\right)\left(1+\frac{3}{u}\right) \leq \left(\frac{\ln v}{\ln u}\right)^2\left(1+\frac{K_0}{\ln u}\right),$$

где $K_0$ - достаточно большая абсолютная постоянная. Если же $1<u\leq 2$, то исходное произведение (по $u<p\leq v$) отличается от произведения

$$\prod_{\frac{5}{2}<p\leq v}(1-g(p))^{-1} \leq \left(\frac{\ln v}{\ln\frac{5}{2}}\right)^2\left(1+\frac{K_0}{\ln\frac{5}{2}}\right)$$

множителем $(1-g(2))^{-1} = 2$ и потому не превосходит

$$2\left(\frac{\ln v}{\ln\frac{5}{2}}\right)^2\left(1+\frac{K_0}{\ln\frac{5}{2}}\right) < \left(\frac{\ln v}{\ln u}\right)^2\left(1+\frac{K}{\ln u}\right),$$

где в качестве $K$ можно взять, например, величину $2K_0 + \ln 5/2$.

Итак, условие (b) выполнено с $\varkappa = 2$. Задавшись четным $b \geq 2$ и положительным $\lambda > 0$, получим:

$$S(A,z) \geq 2NV(z)(1-E) - R,$$

где $V(z) = \prod\limits_{p\leq z}(1-g(p))$, $R = \sum\limits_{\substack{d|P\\ d\leq z^\Delta}} r(d)$,

$$\Delta = \Delta(b;\lambda) = \frac{b}{1-e^{-\lambda}} + \frac{2e^{-\lambda}}{(1-e^{-\lambda})^2} + 1,$$

$$E \leq e^{2\lambda}F(b;2\lambda) + \frac{c}{\ln z}.$$

Величину $V(z)$ оценим снизу с помощью тех же соображений, что использовались выше при проверке условия (b). Именно,

$$V(z) = \prod_{\substack{p\le z\\ p|2N}} \left(1-\frac{1}{p}\right) \prod_{\substack{p\le z\\ p\nmid 2N}} \left(1-\frac{2}{p}\right) \geq \prod_{p|2N} \left(1-\frac{1}{p}\right) \prod_{2<p\le z} \left(1-\frac{2}{p}\right) =$$

$$= \frac{\varphi(2N)}{2N} \prod_{2<p\le z} \left(1-\frac{1}{p}\right)^2 \cdot \frac{p(p-2)}{(p-1)^2}$$, где $\varphi(m)$ – функция Эйлера.

последнее произведение не меньше, чем

$$\prod_{2<p\le z} \left(1-\frac{1}{p}\right)^2 \prod_{n=3}^{\infty} \frac{n(n-2)}{(n-1)^2} = \frac{1}{2} \prod_{2<p\le z} \left(1-\frac{1}{p}\right)^2 = 2 \prod_{p\le z} \left(1-\frac{1}{p}\right)^2 \geq$$

$$\geq \frac{2e^{-2\gamma}}{(\ln z)^2} \left(1-\frac{c_1}{\ln z}\right)$$, где $c_1>0$ – должным образом подобранная константа.

Далее, ввиду равенства $2^{\omega(d)} = \tau(d)$, где $\tau(d)=\sum_{d|n} 1$ – число делителей $d$, имеем: $\nu(d) \le \tau(d)$, откуда

$$R \le \sum_{d\le z^\Delta} \tau(d) = \sum_{d\le z^\Delta} \sum_{mn=d} 1 = \sum_{mn\le z^\Delta} 1 = \sum_{m\le z^\Delta} \sum_{n\le \frac{z^\Delta}{m}} 1$$

$$\le \sum_{m\le z^\Delta} \frac{z^\Delta}{m} < z^\Delta (\ln z^\Delta + 1) < 2\Delta z^\Delta (\ln z).$$

Итак,

$$S(A,z) \geq 2N \cdot \frac{\varphi(2N)}{2N} \cdot \frac{2e^{-2\gamma}}{(\ln z)^2} (1-E)\left(1-\frac{c_1}{\ln z}\right) - 2\Delta z^\Delta \ln z.$$

Возьмём $b=2$, $\lambda = 0.595$. Тогда при достаточно большом $z$ будем иметь: $E < 0.991$, $\Delta = 10.9455$.

Беря $\varepsilon$ достаточно малым, положим $z = (2N)^{\frac{1-\varepsilon}{\Delta}}$. Тогда

$$R < (2N)^{1-\varepsilon} \ln(2N) < (2N)^{1-\frac{\varepsilon}{2}} < (\varphi(2N))^{1-\frac{\varepsilon}{3}}$$, откуда

$$S(A,z) \geq \frac{2\Delta^2 e^{-2\gamma}}{(1-\varepsilon)^2} \cdot 0.009 \frac{\varphi(2N)}{(\ln 2N)^2} \left(1 - \frac{\Delta c_1}{1-\varepsilon} \cdot \frac{1}{\ln 2N}\right) -$$

$$- (\varphi(2N))^{1-\frac{\varepsilon}{3}} > \frac{2}{3} \frac{\varphi(2N)}{(\ln 2N)^2}$$

Итак, имеется не менее $\frac{2}{3}\frac{\varphi(2N)}{(\ln 2N)^2}$ представлений $2N$ в виде $a+b$, где оба числа $a$ и $b$ взаимно просты с $P(z)$. Значит, все простые делители $a$ и $b$ превосходят $z = (2N)^{\frac{1-\varepsilon}{\Delta}}$. Поэтому их число не превышает 10 (в противном случае мы имели бы $\Rightarrow$

см. с.58

Вдумчивый читатель вправе спросить: почему бы нам не попытаться оценить число $\pi_2(x)$ простых близнецов не числом тех целых $m$, для которых произведение $m(m+2)$ взаимно просто с $P(z)$, а числом простых $p$, для которых произведение $p(p+2)$ обладает тем же свойством? Это очень естественно: искать не просто пары $m, m+2$, в которых и у $m$, и у $m+2$ мало простых делителей, а пары, в которых первое число заведомо простое.
Действительно, такой подход вполне оправдан и часто приводит к более точным результатам.
Итак, пусть $a_n = \begin{cases} 1, & \text{если } n = p+2,\ p \text{ — простое}, \\ 0, & \text{иначе.} \end{cases}$

Тогда $|A_d|$ есть число тех $p$, что удовлетворяют сравнению $p \equiv -2 \pmod d$ или, что то же, принадлежат арифметической прогрессии с первым членом $d-2$ и разностью $d$. Вводя обозначение $\pi(x; q, a)$ для числа простых $p \le x$ с условием $p \equiv a \pmod q$, получим:

$$|A_d| = \pi(x; d, d-2) \tag{1}$$

Необходимым условием того, чтобы прогрессия $p \equiv a \pmod q$ содержала бесконечно много простых чисел, является взаимная простота разности и первого члена: $(q, a) = 1$. Согласно известной теореме П.Г.Л. Дирихле (185...), это условие является и достаточным.

Поскольку количество чисел $a$ с условиями $1 \le a \le q$, $(a, q) = 1$, представляет собой определение функции Эйлера $\varphi(q)$, уместно напомнить простейшие её свойства:

Задача 11. Докажите, что
(a) $\varphi(q)$ мультипликативна;
(b) $\varphi(p^k) = p^k\left(1-\frac{1}{p}\right)$ для простого $p$.

Итак, имеется $\varphi(q)$ прогрессий с разностью $q$, каждая из которых содержит простые числа. Естественно предположить, что в первом приближении количества простых $p \le x$ в каждой из прогрессий примерно одинаковы. Это даёт повод написать равенство

$$\pi(x;q,a) = \frac{\pi(x)}{\varphi(q)} + R(x;q,a).$$

Формально это лишь определение $R(x;q,a)$. Естественно ожидать, что при определённых условиях величина $R(x;q,a)$ будет мала по сравнению с $\pi(x)/\varphi(q)$.

Если $q$ и $a$ – постоянные величины, то это действительно так; более того, если $q$ растет вместе с $x$, но не быстрее фиксированной степени логарифма ($q \le (\ln x)^A$), асимптотика

$$\pi(x;q,a) = (1+\bar{o}(1))\,\frac{\pi(x)}{\varphi(q)} \qquad (2)$$

все ещё имеет место. Хуже обстоит дело, если $q$ ведёт себя как степень $x$. Имеющиеся оценки являются "условными", т.е. доказаны в предположении справедливости некоторых гипотез. Например, из расширенной гипотезы Римана (что бы это ни значило) следует, что равенство (2) остается справедливым при $q \le x^{1/2-\varepsilon}$, где $\varepsilon > 0$ - сколь угодно малое фиксированное число.

Тем не менее, попробуем применить нижнюю оценку теоремы 7 к случаю, когда $|A_d|$ определяется равенством (1). Здесь имеем $X = \pi(x)$, $g(d) = \frac{1}{\varphi(d)}$ при нечётном $d$ и $g(d) = 0$ в противном случае, и, наконец, $r_d = R(x; d, d-2)$

Несложная проверка, подобная проведенной по ходу доказательства Теоремы 8, показывает, что неравенство

$$\prod_{u<p\le v} (1-g(p))^{-1} = \prod_{\substack{u<p\le v\\ p\ne 2}} \left(1-\frac{1}{p}\right)^{-1} \cdot \left(1+\frac{1}{p(p-2)}\right) \le \left(\frac{\ln v}{\ln u}\right)^{\varkappa} \left(1+\frac{K}{\ln u}\right)$$

выполнено с $\varkappa = 1$ и надлежащем выборе постоянной $K$. Задавшись чётным $b \ge 2$ и параметром $\lambda > 0$, будем иметь:

$S(A,z) \ge \pi(x) V(z) \left(1 - F(b;\lambda) - \frac{c_0}{\ln z}\right) - R_1$, где

$$F(b;\lambda) = \operatorname{sh}\lambda - \sum_{\substack{k=1\\ k\equiv 1 \pmod 2}}^{b-1} \frac{\lambda^k}{k!}, \quad V(z) = \prod_{p\le z} (1-g(p)) =$$

$$= \prod_{2<p\le z} \frac{p-2}{p-1} = \prod_{2<p\le z} \left(1-\frac{1}{p}\right)\left(1-\frac{1}{(p-1)^2}\right) \ge 2\prod_{p\ge 3}\left(1-\frac{1}{(p-1)^2}\right) \prod_{p\le z}\left(1-\frac{1}{p}\right)$$

$$\ge \frac{2C_1 e^{-\gamma}}{\ln z}\left(1-\frac{C_2}{\ln z}\right),$$

$$R_1 \le \sum_{d\le z^{\alpha}} |r_d|, \quad \alpha = \frac{b}{1+e^{-\lambda}} + \frac{2e^{-\lambda}}{(1-e^{-\lambda})^2} + 1$$

Выбор $b = 2$, $\lambda = 1.729$ даёт: $F(b;\lambda) = 0.999777\ldots$, $\alpha = 3.95609\ldots$ Замечая, что $C_1 = \prod_{p\ge 3}\left(1-\frac{1}{(p-1)^2}\right) > 0.65$, при достаточно большом $z$ находим:

$$S(A,z) > 1.6\cdot 10^{-4}\,\frac{\pi(x)}{\ln z} - \sum_{d\le z^{\alpha}} |r_d|$$

Наша цель – выбрать $z$ как можно больше. Как уже отмечалось, оценок величин $|r_d| = |R(x; d, d-2)|$ при больших $d$, в нашем распоряжении нет. Но тем не менее оценку $S(A,z)$ все-таки завершить можно. Дело в том, что нам достаточно иметь не "индивидуальную" оценку $r_d$, справедливую при каждом конкретном $d$, а оценку среднего значения такого остатка. Это вселяет в нас надежду: даже если имеются $d$, для которых остаточный член $r_d$ велик, то таких чисел, по-видимому, не очень много и они не сильно повлияют на сумму по всем $d \le z^\alpha$.

И это действительно так. Утверждение, которым мы собираемся сейчас воспользоваться, называется теоремой Бомбьери - Виноградова* и формулируется следующим образом:

<u>Теорема</u> 9 (Э. Бомбьери, А.И. Виноградов, 1965). Определим для чисел $x, q$ и $a$ с условиями $(q,a)=1$, $1 \le a \le q-1$ величины

$$R(x;q,a) = \pi(x;q,a) - \frac{\pi(x)}{\varphi(q)}, \quad R(x;q) = \max_{(a,q)=1} |R(x;q,a)|.$$

Тогда для любой фиксированной положительной константы $A$ существуют постоянные $B$ и $C$ такие, что

$$\sum_{q \le \sqrt{x}(\ln x)^{-B}} R(x;q) \le \frac{Cx}{(\ln x)^A}.$$

Иными словами, теорема Бомбьери - Виноградова утверждает, что "в среднем" величина $R(x;q)$ при $q$, чуть меньших $\sqrt{x}$, не превосходит по порядку $\sqrt{x}$.

<u>Замечание</u>. Доказано, что можно положить $B = A+4$. Однако в отличие от $B$ константа $C$ неэффективна: мы не имеем способов вычислить значение $C$ по заданному $A$.

Положим $A=3$ (так что $B=7$) и выберем $z$ из условия $z^\alpha = \dfrac{\sqrt{x}}{(\ln x)^7}$. Тогда из теоремы 9 заключаем:
$$\sum_{d \le z^\alpha} |r_d| \le \frac{Cx}{(\ln x)^3},$$

$$S(A,z) \geq 1.6\cdot 10^{-4}\,\frac{\pi(x)}{\ln z} - \frac{Cx}{(\ln x)^3} \geq 1.5\cdot 10^{-4}\,\frac{\pi(x)}{\ln z} >$$

$$> 1.4\cdot 10^{-4}\cdot 2\alpha\,\frac{\pi(x)}{(\ln x)} > \frac{11\cdot x}{(\ln x)^2},$$ если только $x$ достаточно велико: $x \geq x_0$. Неприятным следствием неэффективности постоянной $C$ в теореме 9 оказывается тот факт, что и константа $x_0$ - неэффективна.

Остается заметить, что для каждого простого $p$, которое учитывается в сумме $S(A,z)$, число $p+2$ взаимно просто с произведением $P(z)$. Таким образом, все его простые делители превышают $x^{\frac{1}{2\alpha}}(\ln x)^{-\frac{7}{\alpha}}$. Поскольку $2\alpha = 7{,}91218\ldots$, мы приходим к следующему утверждению:

Теорема 10 Если $x$ достаточно велико, то имеется не менее $\frac{11x}{(\ln x)^2}$ простых чисел $p$, $p \leq x$, для которых $p+2$ имеет не более 7 простых делителей.

Напоследок отметим, что в 1966 г. китайский математик Чэнь Цзин Жунь получил нижнюю оценку (того же порядка) для количества таких простых $p \leq x$, для которых $p+2$ имеет не более 2 простых делителей.

Задача 12. Оцените снизу число представлений четного числа $2N$ суммою вида $p+m$, где $p \geq 3$ - простое, а $m$ имеет не более чем $k$ простых делителей (постарайтесь сделать $k$ как можно меньшим).

## Глава 5. Решето Сельберга

Простой и красивый метод верхней оценки просеивающей функции $S(A,z)$ был предложен в 1947 г. норвежским математиком Атле Сельбергом (1917 - 2007).

В решете Бруна доказательство неравенства $\sum_{d|m} \mu(d) \le \sum_{d|m} \lambda_d$ для выбранных $d$ всё же требовало некоторых усилий. В решете Сельберга это достигается почти автоматически.

Зададимся достаточно большим числом $z$, $z \ge z_0 > 2$, и положим $\mathcal{D} = z^2$. Как и в решете Бруна, $\mathcal{D}$ будет "регулировать" число слагаемых в остаточном члене $R$. Пусть $\rho_d$ - последовательность вещественных чисел с условием $\rho_1 = 1$. Тогда величина

$$\Big(\sum_{d|n} \rho_d\Big)^2$$

неотрицательна для любого $n$, равна единице при $n = 1$ и, следовательно, годится на роль искомой мажоранты:

$$\sum_{d|n} \mu(d) \le \Big(\sum_{d|n} \rho_d\Big)^2.$$

Ей можно придать привычный вид, преобразовав квадрат суммы следующим образом:

$$\Big(\sum_{d|n} \rho_d\Big)^2 = \sum_{d_1, d_2 | n} \rho_{d_1} \rho_{d_2} = \sum_{d_1, d_2 :\ [d_1, d_2] | n} \rho_{d_1} \rho_{d_2} =$$

$$= \sum_{d|n} \Big(\sum_{d_1, d_2 :\ [d_1, d_2] = d} \rho_{d_1} \rho_{d_2}\Big) = \sum_{d|n} \lambda_d .$$

<u>Задача 13</u>. Выразите $\lambda_d$ через $\rho_\delta$ для $d = p, p^2$ ($p$-простое).

Выгода от использования новой мажоранты состоит в том, что последовательность $\rho_d$ можно выбрать так, что для очень многих $d$ будет выполнено равенство $\rho_d = 0$. Именно, будем считать, что $\rho_d = 0$ для всех $d > z$ и для $d$, не делящих $P(z)$. Иными словами, носителем последовательности $\rho_d$ будут делители $P(z)$, не превосходящие $z$. Легко сообразить, что носителем последовательности $\lambda_d$ будут делители $P(z)$, не превосходящие $\mathcal{D} = z^2$.

Другое преимущество решета Сельберга состоит в том, что величины $\rho_d$ можно выбирать в дальнейшем оптимально, с учетом структуры последовательности $a_n$. Поучительно заметим, что решето Бруна было лишено этого преимущества: величины $\lambda_d$ выбирались раз и навсегда — если не брать в расчет некоторую свободу в выборе величин $b$ и $\lambda$ в теореме 7.

Сначала мы применим решето Сельберга к доказательству верхней оценки величины $\pi(x;q,a)$, $(a,q)=1$. Напомним, что $\pi(x;q,a) \sim \frac{\pi(x)}{\varphi(q)}$ для случая, когда $q$ — фиксировано или растет с ростом $x$ не быстрее степени логарифма $x$. Использованная нами выше теорема Бомбьери – Виноградова показывает, что асимптотика для $\pi(x;q,a)$ имеет место для "почти всех" модулей $q$, $q \le \sqrt{x}(\ln x)^{-B}$. Однако в ряде задач необходима правильная по порядку (или близкая к такой) верхняя оценка $\pi(x;q,a)$, которая была бы справедлива в максимально широком диапазоне: $2 \le q \ll x$. Именно такую оценку дает следующая

<u>Теорема</u> 11 (В. Брун, Э. Титчмарш). Существуют абсолютные постоянные $x_0 > 1$ и $C > 1$ такие, что для любого $x \ge x_0$ и любых $a$ и $q$ с условиями $(a,q) = 1$, $2 \le q \le \frac{x}{C}$ выполнено неравенство:

$$\pi(x;q,a) \le \frac{2x}{\varphi(q)\ln\frac{x}{q}}\left(1 + \frac{3\ln\ln\frac{x}{q}}{\ln\frac{x}{q}}\right).$$

<u>Док-во</u>. Задавшись некоторым $z$ и последовательностью $\rho_d$ с перечисленными выше свойствами, для множества $A$ чисел $n$, $n \le x$, $n \equiv a \pmod{q}$, будем иметь:

$$\pi(x;q,a) - \pi(z;q,a) \le S(A;z) = \sum_{\substack{n\le x\\ n\equiv a \pmod q}} \Big(\sum_{d|(n,P)} \mu(d)\Big) \le \sum_{\substack{n\le x\\ n\equiv a \pmod q}} \Big(\sum_{d|(n,P)} \rho_d\Big)^2.$$

Заметим, что в силу соглашения о носителе $\rho_d$ вместо $d|(n,P)$ во внутренней сумме можно писать $d|n$. Таким образом,

$$S(A,z) \le \sum_{\substack{n\le x\\ n\equiv a \pmod q}} \sum_{d_1,d_2|n} \rho_{d_1}\rho_{d_2} = \sum_{d_1,d_2\le z} \rho_{d_1}\rho_{d_2} \sum_{\substack{n\le x\\ n\equiv a \pmod q\\ n\equiv 0 \pmod d}} 1,$$

где обозначено: $d=[d_1,d_2]$. В силу условия $(a,q)=1$ система сравнений

$$\begin{cases} n\equiv a \pmod q,\\ n\equiv 0 \pmod d. \end{cases}$$

совместна лишь в случае, когда $d$ и $q$ взаимно простые. Действительно, в противном случае мы имели бы некоторое простое число $p$, делящее $d$, $q$ и $n$ и, следовательно, делящее $a$, что невозможно. Итак, ненулевой вклад в $S(A,z)$ дают лишь числа $d_1, d_2$, взаимно простые с $q$. Суммирование по таким числам станем далее отмечать штрихом. Если $(d,q)=1$, то положив $n=dm$, будем иметь: $m\equiv ad^* \pmod q$, $1\le m\le \frac{x}{d}$. В этом случае сумма по $n$ будет равна $\frac{x}{qd}+\theta$, где $|\theta|\le 1$. Итак,

$$S(A,z) \le \sum_{d_1,d_2\le z}{}' \rho_{d_1}\rho_{d_2}\Big(\frac{x}{qd}+\theta\Big) = \frac{x}{q}W + R, \text{ где}$$

$$W = \sum_{d_1,d_2\le z}{}' \frac{\rho_{d_1}\rho_{d_2}}{[d_1,d_2]}, \quad |R| \le \sum_{d_1,d_2\le z} |\rho_{d_1}\rho_{d_2}| = \Big(\sum_{d\le z}|\rho_d|\Big)^2.$$

Поскольку нам ещё только предстоит выбрать коэффициенты $\rho_d$, оценку $R$ отложим на потом и займёмся сперва изучением суммы $W$.

Заметим, что она является ничем иным как квадратичной формой от переменных $\rho_d$. Поэтому нашей ближайшей целью станет приведение её к диагональному виду.

Прежде всего, так как $[d_1,d_2](d_1,d_2)=d_1d_2$, то

$$W=\sum_{d_1,d_2\le z}{}' \frac{\rho_{d_1}\rho_{d_2}}{d_1 d_2}(d_1,d_2).$$

Далее воспользуемся тождеством $m=\sum_{\delta|m}\varphi(\delta)$, где $\varphi$, как и выше, — функция Эйлера.

Задача 14. Докажите это тождество.

Полагая в нём $m=(d_1,d_2)$, получим:

$$W=\sum_{d_1,d_2\le z}{}' \frac{\rho_{d_1}\rho_{d_2}}{d_1 d_2}\sum_{\delta|(d_1,d_2)}\varphi(\delta)=\sum_{\delta\le z}{}'\varphi(\delta)\sum_{\substack{d_1,d_2\le z\\ d_1,d_2\equiv 0 (\mathrm{mod}\,\delta)}}{}'\frac{\rho_{d_1}\rho_{d_2}}{d_1d_2}=$$

$$=\sum_{\delta\le z}{}'\varphi(\delta)\Bigg(\sum_{\substack{d\le z\\ d\equiv 0(\mathrm{mod}\,\delta)}}{}'\frac{\rho_d}{d}\Bigg)^2.$$

Ясно теперь, что замена переменных $u_\delta=\sum_{\substack{d\le z\\ d\equiv 0(\mathrm{mod}\,\delta)}}{}'\frac{\rho_d}{d}$ приводит форму $W$ к диагональному виду:

$$W=\sum_{\delta\le z}{}'\varphi(\delta)u_\delta^2. \tag{1}$$

Но желательно иметь и формулы обратной замены. Зафиксируем бесквадратное $m\le z$ и рассмотрим сумму $\sum_{\delta\le \frac{z}{m}}{}'\mu(\delta)u_{m\delta}$. Подставляя в неё выражения для $u_{m\delta}$, приводим её к виду

$$\sum_{\delta m\le z}{}'\mu(\delta)\Bigg(\sum_{\substack{d\le z\\ d\equiv 0(\mathrm{mod}\,m\delta)}}{}'\frac{\rho_d}{d}\Bigg)=\sum_{d=mn\delta\le z}{}'\frac{\mu(\delta)\rho_{mn\delta}}{mn\delta}.$$

Полагая $k=n\delta$, будем иметь: $k\le\frac{z}{m}$, $\delta|k$, так что

$$\sum_{\delta\le\frac{z}{m}}{}'\mu(\delta)u_{m\delta}=\sum_{k\le\frac{z}{m}}{}'\frac{\rho_{km}}{km}\sum_{\delta|k}\mu(\delta)=\frac{\rho_m}{m},$$

$$\rho_m=m\sum_{\delta\le\frac{z}{m}}{}'\mu(\delta)u_{m\delta}.$$

Положив $m=1$, заключаем, что в новых переменных условие $\rho_1=1$ принимает вид

$$\sum_{\delta\le z}{}'\mu(\delta)u_\delta=1. \tag{2}$$

Наша следующая цель — выбрать переменные $u_\delta$ так, чтобы сумма $W$ была как можно меньше. Говоря иначе, нам необходимо минимизировать квадратичную форму (1) при условии (2).

Эту задачу можно решить методом неопределенных множителей Лагранжа, составив функцию $F(\lambda;\bar{u}) = \sum\limits_{\delta\le z}' \varphi(\delta)u_\delta^2 - \lambda\Big(\sum\limits_{\delta\le z}' \mu(\delta)u_\delta - 1\Big)$ и приравняв нулю все ее производные $\frac{\partial F}{\partial u_\delta}$ (проделайте это самостоятельно!). Существование минимума более-менее очевидно из геометрических соображений.

Но мы приведём иное рассуждение, которое опирается лишь на неравенство Коши. Перепишем (2) в виде

$$1 = \sum_{\delta\le z}' u_\delta\sqrt{\varphi(\delta)}\cdot\frac{\mu(\delta)}{\sqrt{\varphi(\delta)}}.$$

Тогда в силу неравенства Коши,

$$1 \le \Big(\sum_{\delta\le z}' \varphi(\delta)u_\delta^2\Big)\Big(\sum_{\delta\le z}' \frac{\mu^2(\delta)}{\varphi(\delta)}\Big) = WG,$$

где $G = G_q(z) = \sum\limits_{\substack{\delta\le z\\ (\delta,q)=1}} \frac{\mu^2(\delta)}{\varphi(\delta)}$. Следовательно,

$W \ge G^{-1}$ при любом допустимом выборе переменных $u_\delta$. Если мы покажем, что на каком-то наборе $u_\delta$ равенство достигается, то задача минимизации будет решена.

Заметим, что неравенство Коши

$$\Big(\sum_n a_n b_n\Big)^2 \le \sum_n a_n^2 \sum_n b_n^2$$

для неотрицательных послед-тей $a_n, b_n$

обращается в равенство, если одна последовательность пропорциональна другой: $b_n = \lambda a_n$, где $\lambda$ не зависит от $n$. Потребуем, чтобы равенство $\lambda u_\delta\sqrt{\varphi(\delta)} = \frac{\mu(\delta)}{\sqrt{\varphi(\delta)}}$ выполнялось для всех $\delta\le z$, $\delta\mid P$, $(\delta,a)=1$. Получим: $u_\delta = \frac{1}{\lambda}\cdot\frac{\mu(\delta)}{\varphi(\delta)}$, где значение $\lambda$

теперь легко находится из (2):

$$1 = {\sum_{\delta\le z}}' \mu(\delta)\cdot\frac{1}{\lambda}\,\frac{\mu(\delta)}{\varphi(\delta)} = \frac{1}{\lambda}{\sum_{\delta\le z}}'\frac{\mu^2(\delta)}{\varphi(\delta)} = \frac{G}{\lambda},\ \lambda = G.$$

Поэтому значения переменных $u_\delta$ и $\rho_d$, минимизирующие $W$, имеют вид

$$u_\delta = \frac{1}{G}\,\frac{\mu(\delta)}{\varphi(\delta)} = \left({\sum_{\delta\le z}}'\frac{\mu^2(\delta)}{\varphi(\delta)}\right)^{-1}\frac{\mu(\delta)}{\varphi(\delta)},\ \text{если } (\delta,a)=1,\ \delta\le z,\ \delta\,|\,P,$$

$$\rho_m = m{\sum_{\delta\le \frac{z}{m}}}'\frac{\mu(\delta)}{G}\cdot\frac{\mu(\delta m)}{\varphi(\delta m)} = \frac{\mu(m)}{G}\cdot\frac{m}{\varphi(m)}{\sum_{\substack{\delta\le \frac{z}{m}\\ (\delta,m)=1}}}'\frac{\mu^2(\delta)}{\varphi(\delta)}.$$

Перейдем теперь к задаче оценки величины $R$. Докажем, что $|\rho_m|\le 1$. Для этого сначала преобразуем дробь $m/\varphi(m)$. Пользуясь тем, что $\varphi(p)=p-1$ для простого $p$, в случае бесквадратного $m$ будем иметь:

$$\frac{m}{\varphi(m)} = \prod_{p|m}\frac{p}{p-1} = \prod_{p|m}\left(1+\frac{1}{\varphi(p)}\right) = \sum_{d|m}\frac{\mu^2(d)}{\varphi(d)}.$$

Следовательно,

$$|\rho_m| \le \frac{\mu^2(m)}{G}\sum_{d|m}{\sum_{\substack{\delta\le\frac{z}{m}\\(\delta,m)=1}}}'\frac{\mu^2(d)\,\mu^2(\delta)}{\varphi(d)\,\varphi(\delta)}$$

Из условия $(\delta,m)=1$ следует, что $(\delta,d)=1$ для всякого делителя $d$ числа $m$. Значит,

$$|\rho_m| \le \frac{\mu^2(m)}{G}\sum_{\substack{d|m\\ \delta\le z/m,\,(\delta,m)=1}}\frac{\mu^2(d\delta)}{\varphi(d\delta)}.$$

Но любое бесквадратное $n$, $n\le z$, единственным образом представляется в виде $n=d\delta$, где $d|m$, $(\delta,m)=1$. (при этом условие $\delta\le z/m$ может нарушаться). Поэтому значения $n=d\delta$ в сумме не повторяются, и при этом все отвечающие им слагаемые встречаются в сумме $G$. Следовательно, $|\rho_m|\le\frac{1}{G}\,G=1$, $|R|\le\left(\sum_{d\le z}|\rho_d|\right)^2\le z^2$. Таким образом,

$$\pi(x;q,a)\le\frac{x}{qG}+z^2+\pi(z;q,a).$$

Слагаемое $\pi(z;q,a)$ не превосходит числа членов прогрессии $n\equiv a \pmod q$ с условием $1\le n\le z$ и потому ограничено величиной $\frac{z}{q}+1\le z$. Поэтому неравенство для $\pi(x;q,a)$ принимает вид

$$\pi(x;q,a)\le \frac{x}{qH}+z^2+z.$$

Нам остается оценить снизу $G=G_q(z)$ и выбрать $z$ оптимально.

Покажем, что для любых $q,z\ge 1$ верно неравенство

$$G_q(z)\ge \frac{\varphi(q)}{q}\left(\ln z+\frac{3}{10}\right).$$

Пусть $q\ge 2$. Сгруппируем вместе те слагаемые суммы $G_1(z)=\sum\limits_{n\le z}\frac{\mu^2(n)}{\varphi(n)}$, что отвечают одному и тому же значению $(n,q)=\delta$, где $\delta$ пробегает делители $q$. Получим:

$$G_1(z)=\sum_{\delta|q}\sum_{\substack{n\le z\\(n,q)=\delta}}\frac{\mu^2(n)}{\varphi(n)}=\sum_{\delta|q}\sum_{\substack{m\le z/\delta\\(m,q)=1}}\frac{\mu^2(m\delta)}{\varphi(m\delta)}=$$

$$=\sum_{\delta|q}\frac{\mu^2(\delta)}{\varphi(\delta)}\sum_{\substack{m\le z/\delta\\(m,q)=1}}\frac{\mu^2(m)}{\varphi(m)}=\sum_{\delta|q}\frac{\mu^2(\delta)}{\varphi(\delta)}G_q\left(\frac{z}{\delta}\right)\le$$

$$\le\sum_{\delta|q}\frac{\mu^2(\delta)}{\varphi(\delta)}G_q(z)=G_q(z)\prod_{p|q}\left(1+\frac{1}{\varphi(p)}\right)=\frac{q}{\varphi(q)}G_q(z),$$

откуда $G_q(z)\ge\frac{\varphi(q)}{q}G_1(z)$. Итак, осталось оценить $H_1(z)$ снизу. Для этого воспользуемся тем же приёмом, что был применен выше для доказательства неравенства $|g_m|\le 1$. Именно,

$$\frac{\mu^2(n)}{\varphi(n)}=\frac{\mu^2(n)}{n}\cdot\frac{n}{\varphi(n)}=\frac{\mu^2(n)}{n}\prod_{p|n}\left(1-\frac{1}{p}\right)^{-1}=$$

$$= \frac{\mu^2(n)}{n}\prod_{p|n}\left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\dots\right) = \frac{\mu^2(n)}{n}\sum_{m|n^\infty}\frac{1}{m},$$

где символическая запись $m|n^\infty$ означает, что в каноническом разложении $m$ участвуют лишь степени простых делителей $n$ (или, что то же: существует целое $a \geq 1$ такое, что $m|n^a$).

Итак, $G_1(z) = \sum\limits_{n\leq z}\sum\limits_{m|n^\infty}\frac{\mu^2(n)}{nm}$.

Очевидно, всякое число $k$ единственным образом представляется в виде $ab$, где

$$a = \prod_{p|k} p \text{ — бесквадратное, а } b\,|\,a^\infty$$

($a$ называют радикалом $k$ и пишут: $a = \mathrm{rad}(k)$). Если при этом $k \leq z$, то тем более $a \leq z$. Следовательно, сумма $H_1(z)$ содержит все дроби $\frac{1}{k}$, $1\leq k\leq z$. Поэтому

$$G_1(z) \geq \sum_{1\leq k\leq z}\frac{1}{k} \geq \ln z + \frac{3}{10}$$

для любого $z \geq 1$.

Задача 15. Проверьте это!

Возвращаясь к неравенству для $\pi(x;q,a)$, получим:

$$\pi(x;q,a) \leq \frac{x}{q}\cdot\frac{q}{\varphi(q)}\left(\ln z+\frac{3}{10}\right)^{-1} + z^2 + z$$

Возьмем теперь $z = \frac{\sqrt{x/q}}{\ln(x/q)}$. Тогда, положив для краткости $y = \ln\frac{x}{q}$, будем иметь:

$$\ln z + \frac{3}{10} = \frac{1}{2}\ln\frac{x}{q} - \ln\ln\frac{x}{q} + \frac{3}{10} = \frac{1}{2}\left(\ln\frac{x}{q}\right)\left(1-\frac{2\ln y - 3/5}{y}\right),$$

$$\pi(x;q,a) \leq \frac{x}{\varphi(q)}\cdot\frac{2}{\left(\ln\frac{x}{q}\right)}\left(1-\frac{2\ln y-3/5}{y}\right)^{-1} + \frac{x}{q}\cdot\frac{1}{\ln^2\frac{x}{q}} + \sqrt{\frac{x}{q}}\,\frac{1}{\ln\frac{x}{q}}$$

$$\leq \frac{2x}{\varphi(q)\ln\frac{x}{q}}\left(\left(1-\frac{2\ln y-3/5}{y}\right)^{-1} + \frac{1}{2y} + \frac{e^{-y/2}}{y}\right) = \frac{2x}{\varphi(q)\ln\frac{x}{q}}\left(1+\Delta(y)\frac{\ln y}{y}\right)$$

Вычисления показывают, что $\Delta(y)\leq 3$ при $y \geq 11.512$. Последнее неравенство приводит к условию $\frac{x}{q} \geq e^{11.512} = 99907.496\ldots$.

Теорема доказана.

Замечание. Можно показать (мы делать этого не будем), что второе слагаемое в скобках можно вовсе опустить. Также отметим, что снижение коэффициента 2 в оценке Бруна-Титчмарша до значения $2-\delta$, где $\delta > 0$ (на всем диапазоне изменения $q$) привело бы к существенным продвижениям в теории т.н. L-рядов Дирихле и многих задачах теории чисел.

Читатель вправе спросить: как будет выглядеть оценка, получаемая решетом Сельберга, в общем случае? Мы дадим лишь частичный ответ на этот вопрос. Итак, предположим, что просеиваемая последовательность $a_n$, $n \in A$, такова, что

$$|A_d| = X g(d) + r_d$$

для любого бесквадратного $d$, причём мультипликативная функция $g$ удовлетворяет условию (a) Теоремы 7. Что изменится в наших выкладках? Прежде всего, сумма $W$ примет вид

$$\sum_{d_1, d_2 \le z}{}' \frac{g(d_1)\rho_{d_1}\, g(d_2)\rho_{d_2}}{g((d_1,d_2))}, \qquad (3)$$

где штрих означает суммирование по делителям числа $P = P(z)$, не имеющих в каноническом разложении простых из некоторого множества $\mathcal{P}$. (В теореме 8 роль $\mathcal{P}$ играло множество всех простых делителей числа $a$; может оказаться, что $\mathcal{P} = \varnothing$).

Чтобы привести (3) к диагональному виду, нужно подобрать мультипликативную функцию $h$ так, чтобы для всех бесквадратных $d$ выполнялось тождество:

$$\frac{1}{g(d)} = \sum_{\delta | d} \frac{1}{h(\delta)}$$

В частном случае $g(d) = 1/d$ роль $h$ сыграла функция $1/\varphi(\delta)$. Найти $h$ в общем случае нам поможет

<u>Лемма</u> (формула обращения Мёбиуса). Пусть $F$ и $f$ – мультипликативные функции, причём

$$F(d) = \sum_{\delta | d} f(\delta) \text{ при всех } d \geq 1. \quad (1)$$

Тогда

$$f(d) = \sum_{\delta | d} \mu(\delta) F\left(\frac{d}{\delta}\right) \text{ при всех } d \geq 1. \quad (2)$$

Верно и обратное: выполнение (2) для всех $d$ влечёт и справедливость (1) для каждого $d \geq 1$.

<u>Док-во</u>. Действительно, беря произвольное $d \geq 1$, из (1) и леммы ... заключаем:

$$\sum_{\Delta | d} \mu(\Delta) F\left(\frac{d}{\Delta}\right) = \sum_{\Delta | d} \mu(\Delta) \sum_{\delta | \frac{d}{\Delta}} f(\delta) = \sum_{d = \delta\Delta m} \mu(\Delta) f(\delta) =$$

$$= \sum_{d = \delta n} f(\delta) \sum_{\Delta | n} \mu(\Delta) = f(d).$$

Второе утверждение доказывается аналогично.

Возвращаясь к задаче нахождения $h$, получаем:

$$\frac{1}{h(d)} = \sum_{\delta | d} \mu(\delta) \frac{1}{g\left(\frac{d}{\delta}\right)} = \frac{1}{g(d)} \sum_{\delta | d} \mu(\delta) g(\delta) =$$

$$= \frac{1}{g(d)} \prod_{p | d} (1 - g(p)) = \prod_{p | d} \frac{1 - g(p)}{g(p)}$$

(обратите внимание: мы несколько раз воспользовались тем, что $d$ – бесквадратное!)

В частности, для простого $p \leq z$, $p \notin \mathcal{P}$ имеем равенства:

$$h(p) = \frac{g(p)}{1 - g(p)}, \quad g(p) = \frac{h(p)}{1 + h(p)}$$

Вновь отметим: в частном случае $g(p) = \frac{1}{p}$ мы приходим к функции, обратной функции Эйлера:

$$h(p) = \frac{1/p}{1 - 1/p} = \frac{1}{\varphi(p)}$$

Соответственно, преобразования суммы $W$ следуют уже знакомому нам пути:

$$W = \sum_{d_1, d_2 \le z}{}' g(d_1)\rho_{d_1} g(d_2)\rho_{d_2} \sum_{\delta \mid (d_1, d_2)} \frac{1}{h(\delta)} =$$

$$= \sum_{\delta \le z}{}' \frac{1}{h(\delta)} \sum_{\substack{d_1, d_2 \le z \\ d_1, d_2 \equiv 0 \,(\mathrm{mod}\ \delta)}} g(d_1)\rho_{d_1} g(d_2)\rho_{d_2} =$$

$$= \sum_{\delta \le z}{}' \frac{u_\delta^2}{h(\delta)}, \quad \text{где} \quad u_\delta = \sum_{\substack{d \le z \\ d \equiv 0 \,(\mathrm{mod}\ \delta)}}{}' g(d)\rho_d . \qquad (4)$$

(условие $\delta \mid P(z)$ в сумме по $\delta \le z$ можно опустить: в силу соглашения на носитель $\rho_d$ слагаемые, не удовлетворяющие этому условию, дадут нулевой вклад).

Далее, формулы обратной замены получаются с помощью теоремы 1: если $m \mid P$ и $m \le z$, то

$$\sum_{\delta \le \frac{z}{m}}{}' \mu(\delta) u_{m\delta} = \sum_{\delta m \le z}{}' \mu(\delta) \sum_{\substack{d \le z \\ d \equiv 0 \,(\mathrm{mod}\ \delta m)}}{}' g(d)\rho_d =$$

$$= \sum_{d = \Delta\delta m \le z}{}' g(d)\rho_d\, \mu(\delta) = \sum_{km \le z}{}' g(km)\rho_{km} \sum_{\delta \mid k} \mu(k) =$$

$$= g(m)\rho_m, \quad \text{откуда} \quad \rho_m = \frac{1}{g(m)} \sum_{\delta \le \frac{z}{m}}{}' \mu(\delta) u_{m\delta}$$

В частности, равенство $\rho_1 = 1$ в новых переменных принимает вид

$$\sum_{\delta \le z}{}' \mu(\delta) u_\delta = 1 \qquad (5)$$

Минимизация формы (4) при условии (5) проводится точно так же. При этом наименьшее значение $W$ оказывается равным $\frac{1}{G(z)}$, где

$$G(z) = \sum_{d \le z} \mu^2(d) h(d),$$

а значения переменных $u_\delta$ и $\rho_m$, доставляющие этот минимум, задаются равенствами

$$u_\delta = \frac{\mu^2(\delta)\, h(\delta)}{G(z)}, \quad \rho_m = \frac{\mu(m)}{G(z)} \frac{h(m)}{g(m)} \sideset{}{'}\sum_{\substack{d \le z/m \\ (d,m)=1}} \mu^2(d)\, h(d)$$

Пользуясь представлением

$$\frac{h(m)}{g(m)} = \prod_{p|m} \frac{1}{1-g(p)} = \prod_{p|m} (1+h(p)) = \sum_{\delta | m} \mu^2(\delta)\, h(\delta),$$

несложно доказать (сделайте это!), что $|\rho_m| \le 1$.
Переходя к оценке остаточного члена, будем иметь:

$$|R| \le \sideset{}{'}\sum_{d_1, d_2 \le z} |\rho_{d_1} \rho_{d_2}| \cdot |r_{[d_1,d_2]}| \le \sideset{}{'}\sum_{\substack{d_1, d_2 \le z \\ d_1, d_2 | P}} |r_{[d_1,d_2]}| \le$$

$\le \sum\limits_{d|P,\, d \le z^2} |r_d| f(d)$, где символом $f(d)$ обозначено число пар $d_1, d_2$, отвечающих условию $[d_1, d_2] = d$.

<u>Задача 16</u> Докажите, что $f(d) = 3^{\omega(d)}$ для бесквадратного $d$.

Следовательно, $|R| \le \sum\limits_{\substack{d \le z^2 \\ d|P}} 3^{\omega(d)} |r_d|$

Попутно отметим два важных частных случая. Если $|r_d| \le B$ для любого $d$, где $B$ – некоторая постоянная, то $|R| \le B \Big( \sideset{}{'}\sum\limits_{d \le z} |\rho_d| \Big)^2 \le B z^2$. (именно этот случай имел место в теореме 8). Если же $|r_d| \le B d g(d)$ для всех бесквадратных $d$, то

$$|R| \le \frac{Bz^2}{V(z)}, \quad V(z) = \prod_{p \le z} (1 - g(p)).$$

Действительно,

$$|R| \le B \sum_{\substack{d \le z^2 \\ d|P}} 3^{\omega(d)} d g(d) \le Bz^2 \sum_{\substack{d \le z^2 \\ d|P}} 3^{\omega(d)} g(d) =$$

$$= Bz^2 \prod_{p \le z} (1 + 3g(p)) \le Bz^2 \prod_{p \le z} (1+g(p))^3 \le Bz^2 \prod_{p \le z} (1 - g(p))^{-3}$$

$= Bz^2 V^{-3}(z)$, что и требовалось.

Так мы приходим к общему утверждению:

Теорема 12. Пусть последовательность неотрицательных чисел $a_n$, $n \in A$, такова, что

$$|A_d| = Xg(d) + r_d$$

для любого бесквадратного $d$, где $g(d)$ – мультипликативная функция, такая, что $0 \le g(p) < 1$ для любого простого $p$. Тогда для просеивающей функции $S(A,z)$ справедливо неравенство

$$S(A,z) \le \frac{X}{G(z)} + R,$$

в котором $G(z) = \sum_{d \le z} \mu^2(d) h(d)$, мультипликативная функция $h(d)$ определена на простых числах формулой

$$h(p) = \frac{g(p)}{1-g(p)},$$

а величина $R$ в общем случае допускает оценку

$$|R| \le \sum_{\substack{d \le z^2 \\ d | P}} 3^{\omega(d)} |r_d|.$$

Если же $|r_d| \le B$ или $|r_d| \le Bdg(d)$ для некоторой постоянной $B$, то

$$|R| \le Bz^2 \quad и \quad |R| \le Bz^2 V^{-3}(z), \; V(z) = \prod_{p \le z} (1-g(p))$$

соответственно.

Задача 16 Определим для четного $a \ge 2$ величину $\pi_a(x)$ равной числу простых $p$, $p \le x$, для которых $p+a$ – простое. Пользуясь решетом Сельберга, докажите следующее утверждение: для любого $x \ge x_0$ и любого $a$ с условием $a \le x$ справедлива оценка

$$\pi_a(x) \le C \prod_{p|a} \left(1+\frac{1}{p}\right) \frac{x}{(\ln x)^2},$$

где $c$ – абсолютная постоянная.

Воспользуемся результатом задачи для доказательства наличия "аномалии" в распределении простых чисел. Из приведенной ранее асимптотической формулы для $\pi(x)$ следует, что разность $p_{n+1}-p_n$ между соседними простыми числами "в среднем" ведет себя как $(1+\bar{\bar{o}}(1)) \ln p_n$.

Мы же докажем существование бесконечного множества пар последовательных простых чисел, расстояние между которыми существенно меньше среднего значения. Именно, справедлива

Теорема 13. Существует абсолютная постоянная $c$, $0<c<1$, такая, что для бесконечного множества пар соседних простых чисел $p_n, p_{n+1}$ выполнено неравенство: $p_{n+1}-p_n \le (1-c)\ln p_n$.

Док-во. Зададимся достаточно большим $X$ и достаточно малой постоянной $\delta$. Предположим, что все простые числа $p_n$, $X<p_n\le 2X$, удовлетворяют условию $p_{n+1}-p_n > (1-\delta)\ln X$.

Разобьем $p_n$ на классы, относя в один класс $E_a$ ($a$ – чётное) все те $p_n$, для которых $p_{n+1}=p_n+a$. В силу предположения, классы $E_a$ при $2\le a\le(1-\delta)\ln X$ пусты. Оценим двумя способами сумму

$$S = \sum_{X<p_n\le 2X} (p_{n+1}-p_n).$$

Если $p_k$ – ближайшее справа к $X$, $p_e$ – ближайшее слева к $2X$ простые числа, то в силу асимптотического закона распределения простых чисел $p_k - X = \bar{\bar{o}}(X)$, $2X-p_e=\bar{\bar{o}}(X)$, так что

$$S = X + \bar{\bar{o}}(X).$$

С другой стороны, полагая $U=(1-\delta)\ln X$, $V=(1+\delta)\ln X$, будем иметь (штрих означает суммирование по чётным $a$)

$$S = \sum_{a>U}{}' a|E_a| = \Big(\sum_{U<a\le V}{}' + \sum_{a>V}{}'\Big) a|E_a| \ge$$

$$\geqslant \sum_{U<a\le V}{}' a|E_a| + V\sum_{a>V}{}' |E_a| = \sum_{U<a\le V}{}' a|E_a| + V\Big(\pi(2X)-\pi(X) -$$

$$-\sum_{U<a\le V}|E_a|\Big) = V\big(\pi(2X)-\pi(X)\big) - \sum_{U<a\le V}{}'|E_a|\,(V-a).$$

Слагаемые последней суммы неотрицательны. Обозначая сумму через $S_1$, оценим её сверху, пользуясь результатом задачи ... . Очевидно, $|E_a| \le \pi_a(2X) \le C\prod_{p|a}\left(1+\frac{1}{p}\right)\frac{X}{(\ln X)^2}$

Следовательно,

$$S_1 \le \frac{CX}{(\ln X)^2}\sum_{U<a\le V}{}' (V-a)\prod_{p|a}\left(1+\frac{1}{p}\right) = \frac{CX}{(\ln X)^2}\left(VS_2 - S_3\right),$$

где смысл обозначений $S_2$ и $S_3$ очевиден.

Имеем, далее:

$$S_2 = \sum_{U<a\le V}{}' \sum_{d|a}\frac{\mu^2(d)}{d} = \sum_{d\le V}\frac{\mu^2(d)}{d}\sum_{\substack{U<a\le V\\ a\equiv 0 \pmod d\\ a\equiv 0 \pmod 2}} 1$$

Если $d$ - нечетное, то сумма по $a$ приводится к виду $\frac{V-U}{2d}+\underline{O}(1)$, а если $d$ - четное, то к виду $\frac{V-U}{d}+\underline{O}(1)$. Поэтому

$$S_2 = \frac{V-U}{2}\sum_{\substack{d\le V\\ d\equiv 1 \pmod 2}}\frac{\mu^2(d)}{d^2} + (V-U)\sum_{\substack{d\le V\\ d\equiv 0 \pmod 2}}\frac{\mu^2(d)}{d^2} + \underline{O}(\ln V)$$

Суммы по $d$ заменим бесконечными: ошибка от такой замены не превзойдет по порядку

$$\sum_{d>V}\frac{1}{d^2} = \underline{O}\left(\frac{1}{V}\right).$$

<u>Задача 17</u> Считая известными формулы $\zeta(2) = \sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}$, $\zeta(4) = \sum_{n=1}^{\infty}\frac{1}{n^4} = \frac{\pi^4}{90}$, и пользуясь тождеством Эйлера, докажите, что $\sum_{\substack{d=1\\ d\equiv 1 \pmod 2}}^{+\infty}\frac{\mu^2(d)}{d^2} = \frac{12}{\pi^2}$, $\sum_{\substack{d=1\\ d\equiv 0 \pmod 2}}^{\infty}\frac{\mu^2(d)}{d^2} = \frac{3}{\pi^2}$.

<u>Указание</u>: $1+\frac{1}{p^2} = \dfrac{1-\frac{1}{p^4}}{1-\frac{1}{p^2}}$

Пользуясь результатом задачи ..., находим:

$$S_2 = \frac{9}{\pi^2}(V-U) + \underline{O}(\ln V) = \frac{18}{\pi^2}\delta \ln X + \underline{O}(\ln\ln X).$$

Подобным образом вычисляется сумма $S_3$:

$$S_3 = \sum_{U<a\le V}{}' a \sum_{d|a} \frac{\mu^2(d)}{d} = \sum_{d\le V} \frac{\mu^2(d)}{d} \sum_{\substack{U<a\le V\\ a\equiv 0 \pmod d\\ a\equiv 0 \pmod 2}} a =$$

$$= \sum_{\substack{d\le V\\ d\equiv 1 \pmod 2}} \frac{\mu^2(d)}{d}\left(\frac{V^2-U^2}{4d} + \underline{O}(V)\right) + \sum_{\substack{d\le V\\ d\equiv 0 \pmod 2}} \frac{\mu^2(d)}{d} \times$$

$$\times \left(\frac{V^2-U^2}{2d} + \underline{O}(V)\right) = \frac{9}{2\pi^2}(V^2-U^2) + \underline{O}(V\ln V) = \frac{18}{\pi^2}\delta(\ln X)^2 + \underline{O}((\ln X)\ln\ln X).$$

Возвращаясь к оценке $S_1$, будем иметь:

$$S_1 \le \frac{CX}{(\ln X)^2}\, \frac{18}{\pi^2}\delta\left((1+\delta)(\ln X)^2 - (\ln X)^2 + \underline{O}((\ln X)\ln\ln X)\right) =$$

$$= \frac{18C\delta^2}{\pi^2} X\,(1+\bar{\bar{o}}(1)).$$

Следовательно,

$$S \ge (\pi(2X) - \pi(X)) - S_1 \ge (1+\delta)(\ln X)\cdot(1+\bar{\bar{o}}(1))\frac{X}{\ln X} -$$

$$- \frac{18C}{\pi^2}\delta^2 X\,(1+\bar{\bar{o}}(1)) = \left(1+\delta - \frac{18C}{\pi^2}\delta^2 + \bar{\bar{o}}(1)\right) X.$$

Выбирая $\delta$ так, чтобы выполнялось неравенство

$$\frac{18C\delta^2}{\pi^2} \le \frac{\delta}{3},$$

при большом $X$ получаем: $S \ge (1+\frac{\delta}{2})X$, что противоречит равенству $S = (1+\bar{\bar{o}}(1))X$. Теорема доказана.

<u>Замечание</u>. Теорема Эрдеша – это лишь первый шаг на долгом пути исследования маленьких разностей $p_{n+1}-p_n$. Если положить $\Delta = \liminf\limits_{n\to+\infty} \frac{p_{n+1}-p_n}{\ln p_n}$, то теорема 11 означает, что $\Delta \le 1-\bar{\bar{c}}$ при некотором $\bar{\bar{c}}>0$. Уточнению оценки $\Delta$ был посвящен целый ряд работ, из которых мы упомянем лишь некоторые: $\Delta \le (2+\sqrt{3})/8 = 0{,}466\ldots$ (Э. Бомбьери, Г. Дэвенпорт, 1966), $\Delta \le 0{,}248$ (Х. Майер, 1988). Эпохальным событием

стало доказательство равенства $\Delta = 0$ Д. Голдстоном, Я. Пинтцем. С. Йилдиримом (2005). И настоящим триумфом оказалась теорема И. Чжана (2013) о том, что имеется бесконечное множество простых чисел $p_n$ таких, что $p_{n+1} - p_n \leq C$, где $C = 7 \cdot 10^7$ – постоянная. Результат Чжана был усилен и обобщен Дж. Майнардом, Т. Тао и другими исследователями, но это уже другая история.

К стр. 4:

$\Vert\!\!\to$ Более того, для любых взаимно простых чисел $q$ и $a$, $1 \le a \le q-1$, можно доказать справедливость следующего обобщения формулы Мертенса:

$$\prod_{\substack{p \le x \\ p \equiv a (\mathrm{mod}\, q)}} \left(1 - \frac{1}{p}\right) = \frac{C(q,a)}{(\ln x)^{1/\varphi(q)}} \left(1 + \underline{O}_{q,a}\left(\frac{1}{\ln x}\right)\right),$$

где $\varphi(q)$ – функция Эйлера, $C(q,a)$ – некоторая положительная постоянная, а запись $\underline{O}_{q,a}(\cdot)$ означает, что константа в знаке $\underline{O}$ зависит от $q$ и $a$. Чуть подробнее о функции Эйлера и простых числах в арифметической прогрессии будет сказано далее (см. стр. 36-37).

К стр. 23

$\Vert\!\!\to$ $= \dfrac{c_1}{\ln z}$, где $c_1 = c_1(\varkappa, b, K)$ не зависит от $z$.

подобным образом находим:

К стр. 35

$\Vert\!\!\to$ неравенства $\max(a,b) \ge (2N)^{\frac{11}{\Delta}(1-\varepsilon)} > 2N$, что невозможно (конечно, при условии $0 < \varepsilon < 1 - \frac{\Delta}{11} = 0.004954\ldots$).

Теорема доказана.

Замечание. Этот же результат можно получить выбором $b = 4$, $\lambda = 0.89$.