Введение в метод решета

М.А. Королёв

Настоящая брошюра посвящена, как это следует из её названия, краткому введению в *метод решета* — один 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 Янош Пинтц, Дэниел Голдстон, Джем Йилдирим, Йоичи Мотохаши, Итан Чжан, лауреат филдсовской медали Джеймс Мейнард и многие другие учёные.

Брошюра познакомит читателей с верхними оценками на количество простых близнецов и простых чисел Софи Жермен. Из неё читатель узнает о функции Мёбиуса, формуле Мертенса и теореме Бомбьери-Виноградова и с их помощью сделает первые шаги по направлению к доказательству бинарной гипотезы Гольдбаха и вообще получит в свои руки инструменты, полезные для решения задач из разных разделов математики.

Основу брошюры составил текст миникурса «Чудеса в решете, или как отсеивали простые числа Эратосфен, Брун, Сельберг», прочитанного автором на летней школе «Современная математика» в Дубне в июле 2022 г.

Содержание

1 Решето Эратосфена

1.1 Классическое решето

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 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 неё 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 $\sqrt{N} = 8$, то есть 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~~.

1.2 Функция Мёбиуса и её основное свойство

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

Определение 1. *Функция Мёбиуса* $\mu(n)$ задаётся равенствами

$$\mu(n) = \begin{cases} 1, \text{ если } n = 1, \\ 0, \text{ если } n \text{ делится на квадрат простого числа}, \\ (-1)^k, \text{ если } n = p_1 \dots p_k \\ \qquad\qquad \text{– произведение } k \text{ различных простых чисел} \end{cases}$$

Несложно проверить, что

$$\mu(2) = \mu(3) = \mu(5) = \mu(7) = -1, \ \mu(4) = \mu(8) = \mu(9) = 0, \quad \mu(6) = \mu(10) = 1$$

и так далее.

Задача 1. Пусть $\operatorname{Re} s > 1$. Определим *дзета-функцию Римана* $\zeta(s)$ как сумму ряда $\displaystyle\sum_{n=1}^{+\infty} \frac{1}{n^s}$. Докажите, что

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

Указание. 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).

Задача 2. Чему равны суммы $\sum\limits_{d|30} d$ и $\sum\limits_{d|30} d^{-1}$? Как, зная одну, сразу найти вторую?

Определение 2. Арифметическую функцию f назовём *мультипликативной*, если f не равна нулю тождественно и для любых взаимно простых чисел m, n удовлетворяет равенству $f(mn) = f(m)f(n)$.

Задача 3. Покажите, что функция Мёбиуса мультипликативна.

Задача 4. Пусть функция f мультипликативна. Тогда функция F, определённая для всякого n равенством $F(n) = \sum\limits_{d|n} f(d)$, тоже мультипликативна.

Теорема 1 (основное свойство функции Мёбиуса). Справедливо равенство

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

Доказательство. Из результатов Задач 3 и 4 следует, что утверждение достаточно проверить для чисел вида $n = p^k$, где p — простое, а $k \geqslant 1$. 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.

Доказательство. Так как 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, то есть числа вида $p_1^{\ell_1} \dots p_r^{\ell_r}$, где каждый из показателей ℓ_j принимает два значения: 0 и 1.

Количество таких делителей, имеющих в каноническом разложении ровно $s \geqslant 0$ сомножителей, совпадает с биномиальным коэффициентом 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 $x \geqslant 2$. Тогда справедливо неравенство

$$\prod_{p \leqslant x} \left(1 - \frac{1}{p}\right) < \frac{1}{\ln x}.$$

Доказательство. Положим $\Pi = \prod\limits_{p \leqslant x} (1 - 1/p)^{-1}$ и докажем, что $\Pi > \ln x$. Обращая каждый из сомножителей в геометрическую прогрессию, получим

$$\Pi = \prod_{p \leqslant x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^k} + \ldots\right) = 1 + \sum \frac{1}{p_1^{k_1} \ldots p_r^{k_r}},$$

где $r \geqslant 1$, $p_1, \ldots, p_r$ — различные простые числа, не превосходящие x, $k_1, \ldots, k_r \geqslant 0$. В силу основной теоремы арифметики, в последней сумме встретятся все дроби $1/n$, $2 \leqslant n \leqslant x$. Следовательно,

$$\Pi > \sum_{1 \leqslant n \leqslant x} \frac{1}{n} > \ln x.$$

□

Замечание 1. При $x \to +\infty$ справедлива следующая асимптотическая формула (*формула Мертенса*):

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

где $\gamma = 0.5772156649\ldots$ — постоянная Эйлера. Более того, для любых взаимно простых чисел q и a, $1 \leqslant a \leqslant q - 1$, можно доказать справедливость следующего обобщения формулы Мертенса:

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

где $\varphi(q)$ — *функция Эйлера*, $C = C(q, a)$ — некоторая положительная величина, а запись $O_{q,a}(\cdot)$ означает, что константа в знаке O зависит от q и a. Чуть подробнее о функции Эйлера и простых числах в арифметической прогрессии будет сказано далее (см. с. 40).

1.3 Формула Лежандра

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 так далее. Как ведёт 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 числа за исключением двойки нечётные, то

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

но такая оценка слишком груба. Чтобы уточнить её, используем конструкцию Эратосфена. Пусть $x \geqslant 4$, и пусть $P = \prod\limits_{p \leqslant \sqrt{x}} p$. Как мы уже видели, если $\sqrt{x} < n \leqslant x$ и $(n, P) = 1$, то число n — простое. Если же $n \leqslant \sqrt{x}$, то $(n, P) > 1$ за единственным исключением $n = 1$. Следовательно, количество всех n, $1 \leqslant n \leqslant x$, удовлетворяющих условию $(n, P) = 1$, равно количество всех простых на промежутке $(\sqrt{x}, x]$ плюс единица (вклад от $n = 1$), то есть

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

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

$$\sum_{d|(n,P)} \mu(d) = \begin{cases} 1, & (n, P) = 1, \\ 0, & (n, P) > 1. \end{cases}$$

Получим

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

Сумма в правой части приводится к виду

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

где $[\cdot]$ — целая часть числа. Так нами доказана

Теорема 2 (формула Лежандра). Для любого $x \geqslant 2$ справедливо равенство

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

Красота формулы Лежандра 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 всё же извлечём.

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

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

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 функция $W = W(P)$ есть мультипликативная функция аргумента P, так что

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

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

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

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

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

Хотя мы не знаем порядка роста $\pi(\sqrt{x})$, 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.

1.4 Варьируем P: уступка, дающая выигрыш

Однако не будем спешить. Иногда полезно «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 $\prod\limits_{p \leqslant z} p$ (которое для простоты будем обозначать той же буквой P).

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

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

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

Стало быть,

$$\pi(x) \leqslant z + \sum_{1 \leqslant n \leqslant x} \sum_{d \mid (n,P)} \mu(d) = z + \sum_{d \mid P} \mu(d) \sum_{\substack{1 \leqslant n \leqslant x \\ n \equiv 0 \pmod d}} 1 =$$

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

$$= xW + z - R.$$

Далее,

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

Следовательно,

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

Возьмём теперь $z = \ln x$. Тогда $2^z = x^{\ln 2} < x^{7/10}$, и, таким образом,

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

Тем самым доказана

Теорема 3. Если x достаточно велико, то

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

Эта оценка Теоремы 3 уже содержательна. Из неё, в частности, следует, что

$$\frac{\pi(x)}{x} \to 0 \quad \text{при} \quad x \to \infty.$$

Иными словами, простых чисел в натуральном ряду «гораздо меньше», чем членов любой арифметической прогрессии. Насколько точна оценка Теоремы 3? Известно, что

$$\pi(x) = (1 + o(1))\,\frac{x}{\ln x} \quad \text{при} \quad x \to +\infty \quad \text{или, короче,} \quad \pi(x) \sim \frac{x}{\ln x}.$$

Это утверждение называется *асимптотическим законом распределения простых чисел*. Из него, в частности, следует, что

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

при любом сколь угодно малом ε и всех $x \geqslant x_0(\varepsilon)$.

Поэтому найденная нами оценка остаётся достаточно грубой. Можно ли выжать что-то ещё из нашей конструкции? Оказывается, можно, но для это её нужно подвергнуть новой модификации.

2 Простейшее решето Бруна

2.1 Отказ от функции Мёбиуса

Основная идея такой модификации, принадлежащая норвежскому математику Вигго Бруну (1885—1978), состоит в замене функции Мёбиуса $\mu(d)$ некоторой другой арифметической функцией λ_d, «носитель» которой (то есть 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 слабой: количество ненулевых слагаемых в сумме R было очень большим.

Чтобы изложить идею Бруна, удобно рассмотреть более общую задачу. Пусть $\mathcal{A}$ — некоторое конечное подмножество натурального ряда, и

пусть a_n, $n \in \mathcal{A}$, — некоторая последовательность неотрицательных чисел. Пусть, наконец, $z > 2$ и $P = P(z) = \prod\limits_{p \leqslant z} p$. Требуется оценить сверху сумму величин a_n по всем n, взаимно простым с $P(z)$. Эту сумму называют *просеивающей функцией* и обозначают через $S(\mathcal{A}; z)$. Заметим, что задача оценки $\pi(x)$ отвечает случаю, когда $a_n = 1$ для всех $n \leqslant x$, а $z = \sqrt{x}$. Тогда

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

Здесь мы свернём со старого пути. Предположим, что имеется функция λ_d такая, что для любого $m \geqslant 1$ выполнено неравенство

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

Пользуясь тем, что все числа a_n неотрицательны, будем иметь:

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

Выкладки сами подсказывают нам новые обозначения. Пусть $\mathcal{A}_d$ — совокупность номеров $n \in \mathcal{A}$, кратных d. Символом $|\mathcal{A}_d|$ станем обозначать сумму величин a_n по всем $n \in \mathcal{A}_d$.

Итак, имеем

$$S(\mathcal{A}; z) \leqslant \sum_{d|P} \lambda_d |\mathcal{A}_d|.$$

Чтобы двигаться дальше, нужно что-то потребовать от величин $|\mathcal{A}_d|$. В большинстве случаев оказывается, что $|\mathcal{A}_d| = Xg(d) + r_d$, где $g(d)$ — некоторая мультипликативная функция, удовлетворяющая неравенствам $0 \leqslant g(d) < 1$ для всех бесквадратных $d > 1$, r_d — некоторая величина, которая «в среднем» невелика. Смысл параметра X откроется, если положить $d = 1$: X есть хорошее приближение к величине $|\mathcal{A}_1| = |\mathcal{A}| = \sum\limits_n a_n$. Соответственно,

$$S(\mathcal{A}; z) \leqslant \sum_{d|P} \lambda_d \left(Xg(d) + r_d\right) = X \sum_{d|P} g(d)\lambda_d + \sum_{d|P} \lambda_d r_d = XW + R.$$

Новый подход позволяет выбрать λ_d так, что в сумме R будет мало ненулевых слагаемых.

Чтобы предъявить пример функции λ_d, обозначим через $\omega(n)$ количество простых делителей числа n без учёта их кратности:

$$\omega(1)=0,\quad \omega(2)=\omega(3)=\omega(4)=\omega(5)=1,\quad \omega(6)=2,$$
$$\omega(7)=\omega(8)=\omega(9)=1,\quad \omega(10)=2$$

и т. д. Далее, зададимся чётным числом $r\geqslant 2$ и для бесквадратного d положим

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

Покажем, что λ_d обладает требуемым свойством: проверим выполнение неравенства

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

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

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

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

$$\sum_{k=0}^{r}(-1)^kC_s^k=C_s^0-C_s^1+C_s^2-\ldots+(-1)^{r-1}C_s^{r-1}+(-1)^rC_s^r=$$
$$=C_{s-1}^0-(C_{s-1}^0+C_{s-1}^1)+(C_{s-1}^1+C_{s-1}^2)-\ldots+(-1)^{r-1}(C_{s-1}^{r-2}+C_{s-1}^{r-1})+$$
$$+(-1)^r(C_{s-1}^{r-1}+C_{s-1}^r)=(-1)^rC_{s-1}^r=C_{s-1}^r>0,$$

так что

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

Задача 5. Пусть $r\geqslant 1$ — нечётное число. Докажите, что функция

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

при любом n удовлетворяет неравенству

$$\sum_{d|m} \nu_d \leqslant \sum_{d|m} \mu(d).$$

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

$$|\mathcal{A}_d| = \sum_{\substack{1\leqslant n\leqslant x \\ n\equiv 0 (\mathrm{mod}\, d)}} 1 = \left[\frac{x}{d}\right] = \frac{x}{d} - \left\{\frac{x}{d}\right\},$$

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

$$\pi(x) - \pi(z) + 1 \leqslant S(\mathcal{A}; z) \leqslant xW + R,$$

где

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

Сразу заметим: все делители d числа P, для которых $\lambda_d \neq 0$, подчинены условию $\omega(d) \leqslant r$. Поэтому для каждого из них справедливо неравенство $d \leqslant z^{\omega(d)} \leqslant z^r$. Таким образом, $|R| \leqslant z^r$.

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

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

Сумма W_1 уже оценивалась в Лемме 1:

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

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

$$|W_2| \leqslant \sum_{\substack{d|P \\ \omega(d)=r+1}} \frac{1}{d} + \ldots + \sum_{\substack{d|P \\ \omega(d)=s}} \frac{1}{d} + \ldots = \omega_{r+1} + \ldots + \omega_s + \ldots$$

Но несложно проверить, что

$$\omega_s \leqslant \frac{1}{s!}\left(\sum_{p\leqslant z}\frac{1}{p}\right)^s = \frac{\sigma^s}{s!}, \quad \sigma = \sum_{p\leqslant z}\frac{1}{p}. \tag{1}$$

Действительно, все слагаемые, возникающие при раскрытии скобок, положительны, причём всякая дробь вида $1/d$ с условиями $d|P$, $\omega(d) = s$ встретится в правой части (1) с коэффициентом $(1/s!)\cdot s! = 1$. Это красивое рассуждение иногда называют *трюком Эрдеша*.

Задача 6. Докажите, что $\sigma < \ln\ln z + c\ln\ln\ln z$ при любом $z \geqslant 16$, где c — некоторая постоянная.

Указание — набросок доказательства. Воспользовавшись формулой

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

докажите сначала, что при любом $n \geqslant 2$ справедливо неравенство

$$S(n) = \sum_{p\leqslant n}\frac{\ln p}{p} \leqslant \ln n + \frac{1}{n}\sum_{p\leqslant n}\ln p + c_1,$$

в котором c_1 - абсолютная постоянная. Затем, пользуясь Теоремой 3, оцените сумму по простым в правой части и выведите неравенство

$$S(n) \leqslant \ln n + \frac{c_2\ln n}{\ln\ln n}.$$

Поскольку

$$\frac{S(n)-S(n-1)}{\ln n} = \begin{cases} 1/p, & \text{если } n = p - \text{ простое,} \\ 0, & \text{иначе,} \end{cases}$$

для исходной суммы имеем ($N = [z] \geqslant 16$):

$$\sigma = \frac{1}{2} + \sum_{n=3}^{N}\frac{1}{\ln n}(S(n)-S(n-1)) =$$

$$= \frac{1}{2} + \sum_{n=3}^{N} S(n)\left(\frac{1}{\ln n} - \frac{1}{\ln(n+1)}\right) + \frac{S(N)}{\ln(N+1)} - \frac{S(2)}{\ln 2}.$$

Поскольку

$$\frac{1}{\ln n} - \frac{1}{\ln (n+1)} = \frac{\ln (1+1/n)}{\ln n \ln (n+1)} < \frac{1}{n(\ln n)^2},$$

то

$$\sigma \leqslant \sum_{n=3}^{N} \frac{1}{n(\ln n)^2} \left(\ln n + \frac{c_2 \ln n}{\ln \ln n} \right) + c_3 =$$

$$= \sum_{n=3}^{N} \frac{1}{n \ln n} + c_2 \sum_{n=3}^{N} \frac{1}{n \ln n \ln \ln n} + c_3.$$

Последние две суммы проще оценить с помощью неравенств

$$\frac{1}{n \ln n} \leqslant \int_{n-1}^{n} \frac{du}{u \ln u}, \quad \frac{1}{n \ln n \ln \ln n} \leqslant \int_{n-1}^{n} \frac{du}{u \ln u \ln \ln u}.$$

□

Так как $z \leqslant \sqrt{x} < x$, то $\sigma \leqslant \tau$, где $\tau = \ln \ln x + c \ln \ln \ln x$. Согласно формуле Стирлинга, $s! > \sqrt{2\pi s} \left(\frac{s}{e}\right)^s > \left(\frac{s}{e}\right)^s$, так что

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

Положим теперь $r = 2([e\tau] + 1)$. Тогда $e\tau/r \leqslant 1/2$ и

$$W_2 < \sum_{s=r+1}^{\infty} 2^{-s} = 2^{-r} \leqslant 2^{-2e\tau} = e^{-2e(\ln 2)(\ln \ln x + c \ln \ln \ln x)}.$$

Замечая, что $2e \ln 2 = 3.76833\ldots > 3$, при достаточно большом x получим: $W_2 < (\ln x)^{-3}$. Итак,

$$W \leqslant \frac{1}{\ln z} + \frac{1}{(\ln x)^3} < \frac{2}{\ln z},$$

$$\pi(x) \leqslant \pi(z) - 1 + xW + |R| \leqslant \frac{2x}{\ln z} + z + z^r < \frac{2x}{\ln z} + 2z^r.$$

Всё, 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 велико, так как второе слагаемое может перевесить первое. Положим $z = \exp\left(\dfrac{\ln x}{6 \ln\ln x}\right)$. Тогда

$$z^r = \exp\left(\frac{r}{6} \cdot \frac{\ln x}{\ln\ln x}\right) < \exp\left(\frac{1}{6}(2e \ln\ln x + 2ec_1 + 1)\frac{\ln x}{\ln\ln x}\right) = \\ = \exp\left(\frac{e}{3}\ln x + \frac{c_2 \ln x}{\ln\ln x}\right), \quad c_2 = \frac{1}{6}(2ec_1 + 1).$$

Так как $\dfrac{e}{3} = 0.90609\ldots < \dfrac{10}{11}$, то при достаточно больших x получим

$$z^r < x^{10/11}, \quad \pi(x) < \frac{12x}{\ln x}\ln\ln x + 2x^{10/11} < \frac{x}{\ln x} \cdot 14 \ln\ln x.$$

Как уже говорилось, $\pi(x) \sim \dfrac{x}{\ln x}$, 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*.

2.2 Простые близнецы: оценка сверху

Простые близнецы — это пары простых чисел, отличающихся на двойку, то есть 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 так далее). Упомянутая гипотеза утверждает, что множество таких пар бесконечно. Она до сих пор не доказана.

Введём функцию $\pi_2(x)$, равную количеству таких пар с условием $p \leqslant x$. 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.

Теорема 4. Для достаточно больших x справедлива оценка

$$\pi_2(x) < cx\left(\frac{\ln\ln x}{\ln x}\right)^2,$$

где $c > 0$ — некоторая постоянная.

Доказательство. Пусть $2 < z \leqslant \sqrt{x}$ и $P = P(z) = \prod\limits_{p \leqslant z} p$. Положим

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

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

$$\pi_2(x) - \pi_2(z) \leqslant S(\mathcal{A}; z) \leqslant \sum_{d|P} \lambda_d |\mathcal{A}_d|.$$

В отличие от предыдущей задачи нахождение $|\mathcal{A}_d|$ потребует теперь некоторых усилий. Величина $|\mathcal{A}_d|$ равна количеству тех $m, 1 \leqslant m \leqslant x$, которые делятся на d или, что то же, числу решений сравнения

$$m(m+2) \equiv 0 \pmod{d} \tag{2}$$

с условием $1 \leqslant m \leqslant x$. Ясно, что если m_0 — решение (2), то число $m_0 + d$ — также решение, и обратно. Поэтому достаточно найти количество решений этого сравнения с условием $1 \leqslant m \leqslant d$. 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 же $d > 2$, то решениями будут различные вычеты $m \equiv 0 \pmod{d}$ и $m \equiv d - 2 \pmod{d}$. Итак, для простого d имеем:

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

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

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

Пусть $m_1, \dots, m_k$ — произвольные решения первого, …, k-го сравнений системы. В силу китайской теоремы об остатках, существует единственный вычет m_0 по модулю $d = p_1 \dots p_k$ такой, что

$$m_0 \equiv m_1 \pmod{p_1}, \quad \dots, \quad m_0 \equiv m_k \pmod{p_k}.$$

Иными словами, всякий набор $(m_1, \dots, m_k)$ порождает решение сравнения по модулю d. Верно, очевидно, и обратное. Общее количество различных наборов равно произведению $\nu(p_1) \dots \nu(p_k)$. Если все числа $p_1, \dots, p_k$ – нечётные, то $\nu(d) = 2^k = 2^{\omega(d)}$. Если среди чисел $p_1, \dots, p_k$ 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

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

При переходе к сравнению с условием $1 \leqslant m \leqslant x$ число $\nu(d)$ нужно домножить на количество отрезков длины d, которые полностью укладываются в промежуток $1 \leqslant m \leqslant x$. Оставшийся отрезок (если он непуст) содержит не более $\nu(d)$ решений. Следовательно,

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

Преобразуя это выражение, найдём

$$|\mathcal{A}_d| = xg(d) + r_d, \quad \text{где} \quad g(d) = \frac{\nu(d)}{d}, \ |r_d| \leqslant \nu(d).$$

Соответственно, $S(\mathcal{A}; z) \leqslant xW + R$, где

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

Как и выше, при оценке $|R|$ воспользуемся тем, что $\lambda_d \neq 0$ лишь в случае $\omega(d) \leqslant r$. Для таких d имеем $\nu(d) \leqslant 2^{\omega(d)} \leqslant 2^r$, так что

$$|R| \leqslant 2^r \sum_{\substack{d|P \\ \omega(d) \leqslant r}} 1 \leqslant (2z)^r.$$

Сумма W оценивается подобно тому, как это делалось выше. Прежде всего,

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

Пользуясь Леммой 1, получаем:

$$W_1 = \prod_{p\leqslant z}\left(1-\frac{\nu(p)}{p}\right) = \left(1-\frac{1}{2}\right)\prod_{2<p\leqslant z}\left(1-\frac{2}{p}\right) <$$
$$< \frac{1}{2}\prod_{2<p\leqslant z}\left(1-\frac{2}{p}+\frac{1}{p^2}\right) = \frac{1}{2}\prod_{2<p\leqslant z}\left(1-\frac{1}{p}\right)^2 = 2\prod_{p\leqslant z}\left(1-\frac{1}{p}\right)^2 <$$
$$< \frac{2}{(\ln z)^2}.$$

Далее,

$$|W_2| \leqslant \omega_{r+1} + \ldots + \omega_s + \ldots, \quad \omega_s = \sum_{\substack{d|P\\ \omega(d)=s}} \frac{\nu(d)}{d}.$$

Пользуясь оценкой, установленной ранее с помощью трюка Эрдеша, будем иметь:

$$\omega_s \leqslant \sum_{\substack{d|P\\ \omega(d)=s}} \frac{2^{\omega(d)}}{d} = 2^s \sum_{\substack{d|P\\ \omega(d)=s}} \frac{1}{d} \leqslant \frac{2^s\sigma^s}{s!} < \frac{(2\tau)^s}{s!},$$

где σ и τ - те же, что и выше.

Вновь применяя формулу Стирлинга и полагая $r = 4([e\tau]+1)$, находим

$$W_2 < \sum_{s=r+1}^{+\infty}\left(\frac{2e\tau}{r}\right)^s < \frac{1}{(\ln x)^3},$$
$$W < \frac{2}{(\ln z)^2} + \frac{1}{(\ln x)^3} < \frac{3}{(\ln z)^2}.$$

Итак,

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

Положив, наконец, $z = \exp\left(\dfrac{\ln x}{12\ln\ln x}\right)$, приходим к искомому неравенству:

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

Теорема доказана. □

Выведем теперь обещанное

Следствие 1. Ряд

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

сходится.

Доказательство. Положим

$$S(x) = \sum_{\substack{x<p\leqslant 2x \\ p+2 \text{ — простое}}} \left(\frac{1}{p} + \frac{1}{p+2}\right).$$

Очевидно, $S_1(x) < S(x) < 2S_1(x)$, где

$$S_1(x) = \sum_{\substack{x<p\leqslant 2x \\ p+2 \text{ — простое}}} \frac{1}{p}.$$

Считая $x \geqslant x_0$ (где x_0 достаточно велико), будем иметь:

$$S_1(x) \leqslant \frac{1}{x}(\pi_2(2x) - \pi_2(x)) \leqslant \frac{\pi_2(2x)}{x} \leqslant \frac{1}{x} \cdot 433 \cdot 2x \left(\frac{\ln\ln 2x}{\ln 2x}\right)^2 = \\ = 866 \left(\frac{\ln\ln 2x}{\ln 2x}\right)^2.$$

Определяя k_0 из условий $x_0 < 2^{k_0} \leqslant 2x_0$, получим

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

Отсюда следует искомое утверждение. □

Замечание 2. Как следует из Леммы 1, ряд, составленный из чисел, обратных к простым, расходится. Всё познаётся в сравнении!

Замечание 3. Сумма ряда из Следствия 1 называется константой Бруна и обозначается через B_2. Даже приближённое вычисление B_2 является трудной задачей. Сейчас известно лишь, что

$$1.830484424658 < B_2 < 2.347.$$

Нижняя граница - ничто иное как результат отыскания всех пар простых близнецов, не превосходящих 10^{16}, а верхняя - результат оценки $\pi_2(x)$ того типа, о которой пойдёт речь в Главе 3 (см. Задачу 7). Полагают, что точное значение константы Бруна близко к 1.902160583. Интересно отметить, что именно в ходе работ по вычислению B_2 была обнаружена ошибка в арифметике с плавающей точкой процессора Pentium, стоившая производителю миллионы долларов.

Индекс в обозначении B_2 отражает тот факт, что постоянная Бруна - лишь один из представителей большого семейства теоретико-числовых констант. Например, обозначение B_4 зарезервировано за суммой

$$\sum_p \left(\frac{1}{p} + \frac{1}{p+2} + \frac{1}{p+6} + \frac{1}{p+8}\right) =$$
$$= \left(\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}\right)+\left(\frac{1}{101}+\frac{1}{103}+\frac{1}{107}+\frac{1}{109}\right)+\ldots,$$

распространённой на все четвёрки простых чисел вида $p, p+2, p+6, p+8$.

3 Модификация решета Бруна

3.1 Не все делители равноправны: «тонкая настройка» λ_d

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

Выше при построении мажоранты λ_d мы ограничились делителями d числа P, у которых $\omega(d) \leqslant k$, где k — чётное число. Все простые делители таких d не превосходили z.

Теперь же вместо z предлагается рассмотреть последовательность точек $z = z_1 > z_2 > \ldots > z_t$ с условиями $z_1 < x, z_t \geqslant 2$, а вместо числа k — последовательность чётных чисел $k_1, \ldots, k_t$. Пусть, далее,

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

так что $P_1P_2\dots P_t = P = \prod\limits_{p\leqslant z} p$ (для удобства можно считать, что $1 < z_{t+1} < 2$). Тогда всякий делитель $d|P$ единственным образом представляется в виде $d_1\dots d_t$, где $d_r|P_r$. Соответственно, для любого целого n справедливы равенства:

$$\sum_{d|(n,P)} \mu(d) = \sum_{d_1|(n,P_1)} \mu(d_1)\cdot\ldots\cdot \sum_{d_t|(n,P_t)} \mu(d_t) = X_1\dots X_t.$$

Положив

$$Y_r = \sum_{\substack{d_r|(n,P_r)\\ \omega(d_r)\leqslant k_r}} \mu(d_r)$$

будем иметь: $0 \leqslant X_r \leqslant Y_r$ и, следовательно,

$$\sum_{d|(n,P)} \mu(d) \leqslant Y_1\dots Y_t = \prod_{r=1}^{t} \sum_{d_r|(n,P_r)} \mu(d_r) = \sum_{\substack{d=d_1\dots d_t|(n,P),\\ \omega(d_r)\leqslant k_r,\ 1\leqslant r\leqslant t}} \mu(d).$$

Значит, в качестве мажоранты λ_d можно взять функцию

$$\lambda_d = \begin{cases} \mu(d), \text{ если } d = d_1\dots d_t,\ \omega(d_r)\leqslant k_r,\ r = 1,2,\dots,t,\\ 0, \text{ иначе.}\end{cases}$$

Соответственно,

$$\begin{aligned} S(\mathcal{A},z) &\leqslant \sum_{d|P} \lambda_d|\mathcal{A}_d| = \sum_{d_1|P_1}\dots\sum_{d_t|P_t} \mu(d_1)\dots\mu(d_t)|\mathcal{A}_{d_1\dots d_t}| = \\ &= \sum_{d_1|P_1}\dots\sum_{d_t|P_t} \mu(d_1)\dots\mu(d_t)\,(Xg(d_1\dots d_t) + r_{d_1\dots d_t}) = XW + R, \end{aligned}$$

где

$$W = \prod_{r=1}^{t}\left(\sum_{\substack{d_r|P_r\\ \omega(d_r)\leqslant k_r}} \mu(d_r)g(d_r)\right).$$

Преимущество такой модификации легко увидеть на примере оценки величины R. Действительно, для всякого числа d_r справедливы неравенства

$$d_r \leqslant z_r^{\omega(d_r)} \leqslant z_r^{k_r}.$$

Следовательно, для чисел d, отвечающих ненулевым значениям мажоранты λ_d, имеем оценку:

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

В качестве z_r часто берут числа

$$z_1 = z,\ z_2 = \sqrt{z_1} = z^{1/2},\ z_3 = \sqrt{z_2} = z^{1/2^2}, \dots, z_r = z^{1/2^{r-1}}, \dots,$$

а в качестве k_r — числа вида $b + 2(r-1)$, где $b \geqslant 2$ — фиксированное чётное число. Такой выбор даёт

$$D \leqslant z^{\Delta},\ \Delta = b + \frac{b+2}{2} + \frac{b+4}{2^2} + \frac{b+6}{2^3} + \dots + \frac{b+2(r-1)}{2^r} + \dots < 2b+4.$$

Следовательно,

$$|R| < \sum_{d|P,\ d<z^{2b+4}} |r_d|.$$

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 вида $\ln\ln x$, $(\ln\ln x)^2$.

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

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

Тогда знак «хвоста» w_2 зависит лишь от чётности k. Действительно, всякое $d|m$ с условием $\omega(d) > k$ можно представить в виде

$$d = p_1 \dots p_k p_{k+1} \dots p_s, \quad \text{где} \quad s = \omega(d) \ \text{ и } \ p_1 > \dots > p_k > p_{k+1} > \dots > p_s.$$

Положив $\delta = p_1 \dots p_{k+1}$, $\Delta = d/\delta$, будем иметь $p^+(\Delta) < p^-(\delta)$, где через $p^+(n)$ и $p^-(n)$ обозначены, соответственно, наибольший и наименьший простые делители числа n (для $n = 1$ обе величины полагаем равными

единице). Тогда

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

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

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

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

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

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

Воспользуемся теперь трюком Эрдеша:

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

Далее, замечая, что $g(p) \leqslant -\ln(1-g(p))$, оценим первую 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

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

Возьмём в качестве m величину

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

и обозначим

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

Тогда в силу доказанного будем иметь

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

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

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

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

где

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

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

3.2 О размерности решета и не только: общая оценка $S(\mathcal{A}, z)$

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

$\frac{3}{2} \leqslant u < v$ справедлива оценка

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

где $\varkappa$ и K — некоторые абсолютные положительные постоянные. Ввиду особой важности первой из них присвоено название размерности решета. Тогда для чисел $z_r = z^{2^{1-r}}$ будем иметь:

$$\frac{1}{V_r} \leqslant 2^{\varkappa}\left(1+\frac{2^r K}{\ln z}\right), \quad L_r \leqslant \varkappa \ln 2 + \frac{2^r K}{\ln z},$$

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

В силу формулы конечных приращений и неравенства Гёльдера, для любых положительных ξ, η и целого $m \geqslant 3$ имеем:

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

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

$$E \leqslant 2^{\varkappa} \sum_{r=1}^{t} \left(1+\frac{2^r K}{\ln z}\right)\left((\varkappa \ln 2)^{b+2r-1} + (b+2r-1)\times \right. \\ \left. \left\{\frac{2^r K}{\ln z}\cdot\frac{1}{2}(2\varkappa \ln 2)^{b+2r-2} + \frac{1}{4}\left(\frac{2^{r+1}K}{\ln z}\right)^{b+2r-1}\right\}\right)\frac{1}{(b+2r-1)!}$$

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

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

(здесь $\operatorname{sh}(y) = (e^y - e^{-y})/2$ — гиперболический синус). Тогда, проведя несложные выкладки, получим:

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

где

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

$$E_1 = \sum_{r=1}^{+\infty} \frac{2^r K}{\ln z} \frac{(\varkappa \ln 2)^{b+2r-1}}{(b+2r-1)!} = \frac{K \cdot 2^{(1-b)/2}}{\ln z} F(b; \varkappa\sqrt{2} \ln 2) = \frac{c_1}{\ln z}$$

(здесь и далее через c_j обозначены положительные величины, не зависящие от z: $c_j = c_j(\varkappa, b, K)$). Подобным образом находим:

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

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

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

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

Поскольку

$$\frac{\ln z}{2^t} < \ln 2 \leqslant \frac{\ln z}{2^{t-1}}, \quad \text{то} \quad 2^t \leqslant \frac{2 \ln z}{\ln 2} \quad \text{и} \quad \frac{2^{r+1} K}{\ln z} \leqslant \frac{4K}{\ln 2}$$

при любом $r \leqslant t$. Поэтому $E_4 \leqslant 2K E_5/(\ln 2)$.

Далее, определим s из неравенств

$$2^s \leqslant \frac{\sqrt{\ln z}}{2K} < 2^{s+1}.$$

Тогда вклад от $r \leqslant s$ в сумму E_5 не превзойдёт

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

$$\leqslant \frac{1}{(\ln z)^{(b+1)/2}} \cdot \frac{1}{8} \sum_{r=1}^{+\infty} \frac{1}{(b+2r-2)!} \leqslant \frac{c_5}{(\ln z)^{3/2}}.$$

Далее, если $s < r \leqslant t$, то

$$\left(\frac{2^{r+1}K}{\ln z}\right)^{b+2r-1} \frac{1}{(b+2r-2)!} \leqslant \frac{4K}{\ln 2}\left(\frac{4K}{\ln 2}\cdot\frac{e}{b+2r-2}\right)^{b+2r-2} \leqslant$$
$$\leqslant \frac{4K}{\ln 2}\left(\frac{2eK}{r\ln 2}\right)^{b+2r-2} < \frac{4K}{\ln 2}\left(\frac{8K}{r}\right)^{b+2r-2}$$

Поскольку

$$s > \frac{1}{\ln 2}\ln\left(\frac{\sqrt{\ln z}}{4K}\right) = \frac{\ln\ln z}{2\ln 2} - \frac{\ln(4K)}{\ln 2} > \frac{2}{3}\ln\ln z,$$

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

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

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:

$$E \leqslant 2^{\varkappa}F(b, \varkappa\ln 2) + \frac{c}{\ln z},$$

где величина $c = c(\varkappa, b, K)$ не зависит от z. Так приходим к следующему утверждению:

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

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

для любого бесквадратного d, причём мультипликативная функция g удовлетворяет условиям:

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

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

для любых чисел u и v с условиями $\frac{3}{2} \leqslant u < v$, где $\varkappa$, K — положительные постоянные. Тогда для просеивающей функции $S(\mathcal{A}, z)$ справедливо неравенство

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

где

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

$$E \leqslant 2^{\varkappa} F(b, \varkappa \ln 2) + \frac{c}{\ln z}, \quad F(b, y) = \operatorname{sh}(y) - \sum_{r=1}^{b/2} \frac{y^{2r-1}}{(2r-1)!},$$

а $c = c(\varkappa, b, K)$ — некоторая постоянная.

Задача 7. Пользуясь Теоремой 5 наряду с формулой Мертенса, получить при всех достаточно больших x оценки

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

с явно вычисленными постоянными c_1 и c_2 (можно положить, например, $c_1 = 51$, $c_2 = 285$).

Замечание 4. Существует гипотеза, согласно которой

$$\pi_2(x) \sim \frac{Cx}{(\ln x)^2}, \quad \text{где} \quad C = 2\prod_{p>2}\left(1 - \frac{1}{(p-1)^2}\right) = 0.6601618158\ldots$$

Задача 8. Пользуясь тем, что сравнение $m^2 + 1 \equiv 0 \pmod p$ в случае простого $p \equiv 3 \pmod 4$ не имеет решений, а в случае $p \equiv 1 \pmod 4$ имеет 2 решения с условием $1 \leqslant m \leqslant p$, а также тем, что

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

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

Задача 9. Пусть x достаточно велико, a, b — целые числа, $(a, b) = 1$, $1 \leqslant a, b \leqslant x$. Оцените сверху количество тех простых p, $p \leqslant x$, для которых число $ap + b$ также простое.

Замечание 5. В случае $a = 2, b = 1$ получим пары простых чисел вида p, $2p + 1$. Такие простые числа p называются *простыми Софи Жермен.*

4 Решето Бруна: нижние оценки

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

Так, выше мы оценивали сверху величину $S(\mathcal{A}, z)$, равную числу целых n, $1 \leqslant n \leqslant x$, таких, что и n, и $n+2$ взаимно просты с произведением $P = P(z) = \prod\limits_{p \leqslant z} p$. В модифицированном решете Бруна в качестве z можно брать величину вида x^δ, где $\delta = (1-\varepsilon)/(2b+4)$, а ε — сколь угодно малая фиксированная постоянная. Но условие $(n(n+2), P) = 1$ означает, что все простые делители чисел n и $n+2$ превосходят $z = x^\delta$. Поэтому их не может быть слишком много! Точнее, их число не превосходит величины $k = \left[\delta^{-1}\right] + 1$. Если ε достаточно мало, то $k \leqslant 2b+5$.

Предположим, что нам удалось найти для $S(\mathcal{A}, z)$ нижнюю оценку того же порядка, что и в Теореме 5. Тем самым было бы доказано существование абсолютной постоянной k такой, что множество пар чисел n, $n+2$, каждое из которых имеет не более k простых сомножителей, бесконечно. Это стало бы серьезным продвижением в решении задачи о простых близнецах.

4.1 Трюк Форда-Халберстама

Оказывается, методы решета позволяют получать нижние оценка такого рода, однако соответствующие рассуждения оказываются более тонкими. Причина этого достаточно очевидна. Задавшись нечётными числами k_r, $1 \leqslant r \leqslant t$, мы получим величины

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

которые в силу Задачи 5 являются нижними оценками сумм

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

Однако их произведение, вообще говоря, уже не будет нижней оценкой для суммы

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

Тем не менее, доказательство Теоремы 5 можно надлежащим образом модифицировать и всё-такие получить искомую нижнюю оценку. В основе этого рассуждения (предложенного К. Фордом и Х. Халберстамом) лежит следующая

Лемма 2. Пусть $0 \leqslant x_r \leqslant y_r$, $r = 1, \dots, t$, — два набора неотрицательных чисел. Тогда

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

Доказательство. При $t = 1$ неравенство имеет вид

$$x_1 \geqslant y_1 - (y_1 - x_1)$$

и, очевидно, справедливо. Предположим, что утверждение леммы доказано для всех $t \leqslant m$, и проверим его справедливость для $t = m + 1$. Имеем:

$$\begin{aligned}
x_1 \dots x_{m+1} = x_1 \dots x_m \cdot x_{m+1} \geqslant \\
\geqslant \left(y_1 \dots y_m - \sum_{r=1}^{m} (y_r - x_r) \prod_{j=1,\dots,m,\ j \neq r} y_j \right) x_{m+1} = \\
= y_1 \dots y_m x_{m+1} - \sum_{r=1}^{m} (y_r - x_r) \left(\prod_{j=1,\dots,m,\ j \neq r} y_j \right) x_{m+1} \geqslant \\
\geqslant y_1 \dots y_m (y_{m+1} - (y_{m+1} - x_{m+1})) - \sum_{r=1}^{m} (y_r - x_r) \prod_{j=1,\dots,m+1,\ j \neq r} y_j = \\
= y_1 \dots y_{m+1} - \sum_{r=1}^{m+1} (y_r - x_r) \prod_{j=1,\dots,m+1,\ j \neq r} y_j,
\end{aligned}$$

что и требовалось. □

Применим теперь неравенство Леммы 2 к наборам

$$x_r = X_r = \sum_{d_r|(n,P_r)} \mu(d_r), \quad y_r = Y_r = \sum_{\substack{d_r|(n,P_r)\\ \omega(d_r)\leqslant k_r}} \mu(d_r), \quad r = 1, \ldots, t,$$

где, как и выше, $k_1, \ldots, k_t$ — чётные числа.

Для начала заметим, что

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

Знак последней суммы совпадает с $(-1)^{k_r+1} = -1$. Действительно, пусть m — произвольное бесквадратное число, k — чётное, 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 Δ совпадает с величиной $\sum\limits_{\Delta|q} \mu(\Delta)$ и поэтому неотрицательна и не превосходит единицы. Таким образом,

$$(-1)^{k+1} w \leqslant \sum_{\substack{\delta|m\\ \omega(\delta)=k+1}} 1.$$

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

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

В силу Леммы 2

$$X_1 \dots X_t \geqslant Y_1 \dots Y_t - \sum_{r=1}^{t} \Bigg(\sum_{\substack{\delta_r \mid (n, P_r) \\ \omega(\delta_r) = k_r + 1}} 1 \Bigg) \prod_{j \neq r} Y_j,$$

или, что то же,

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

$$- \sum_{r=1}^{t} \Bigg(\sum_{\substack{d_r \mid (n, P_r) \\ \omega(d_r) = k_r + 1}} 1 \Bigg) \prod_{j \neq r} \Bigg(\sum_{\substack{d_j \mid (n, P_j) \\ \omega(d_j) \leqslant k_j}} \mu(d_j) \Bigg) =$$

$$= \sum_{\substack{d_1 \dots d_t \mid (n,P) \\ \omega(d_r) \leqslant k_r}} \mu(d_1) \dots \mu(d_r) - \sum_{r=1}^{t} \sum_{\substack{d_1 \dots d_t \mid (n,P) \\ \omega(d_r) = k_r + 1 \\ \omega(d_j) \leqslant k_j, j \neq r}} \mu \left(\frac{d_1 \dots d_t}{d_r} \right)$$

Правая часть последнего неравенства и послужит искомой минорантой.

Переходя к нижней оценке $S(\mathcal{A}, z)$, получим

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

$$\geqslant \sum_n a_n \sum_{\substack{d_1 \dots d_t \mid (n,P) \\ \omega(d_r) \leqslant k_r}} \mu(d_1) \dots \mu(d_r) - \sum_n a_n \sum_{r=1}^{t} \sum_{\substack{d_1 \dots d_t \mid (n,P) \\ \omega(d_r) = k_r + 1 \\ \omega(d_j) \leqslant k_j,\ j \neq r}} \mu \left(\frac{d_1 \dots d_t}{d_r} \right) =$$

$$= \sum_{\substack{d_1 \dots d_t \mid P \\ \omega(d_r) \leqslant k_r}} \mu(d_1) \dots \mu(d_r) \sum_{n \equiv 0 \pmod{d_1 \dots d_t}} a_n -$$

$$- \sum_{r=1}^{t} \sum_{\substack{d_1 \dots d_t \mid P \\ \omega(d_r) = k_r + 1}} \mu \left(\frac{d_1 \dots d_t}{d_r} \right) \sum_{n \equiv 0 \pmod{d_1 \dots d_t}} a_n.$$

Как и выше, будем предполагать, что

$$|\mathcal{A}_d| = X g(d) + r_d$$

для всякого бесквадратного d, причём мультипликативная функция g удовлетворяет условиям Теоремы 5. Тогда

$$S(\mathcal{A},z)=\sum_{\substack{d_1\dots d_t\mid P\\ \omega(d_r)\leqslant k_r}}\mu(d_1)\dots\mu(d_t)\,(Xg(d_1)\dots g(d_t)+r_{d_1\dots d_t})-$$

$$-\sum_{r=1}^{t}\sum_{\substack{d_1\dots d_t\mid P\\ \omega(d_r)=k_r+1}}\mu\left(\frac{d_1\dots d_t}{d_r}\right)(Xg(d_1)\dots g(d_t)+r_{d_1\dots d_t})=$$

$$=XW+R_1-XW^*-R_2,$$

где смысл обозначений ясен.

Оценим сначала R_1 и R_2. Повторяя дословно оценку R из Теоремы 5, получим

$$d=d_1\dots d_t\leqslant z^{2b+4}$$

для всякого слагаемого суммы W. Ввиду того, что для всякого $d=d_1\dots d_t$ из суммы W^* найдется номер r с условием $\omega(d_r)=k_r+1$, получаем: $d\leqslant z^{2b+5}$. Так как числа d, отвечающие слагаемым сумм W и W^*, не повторяются, то окончательно находим:

$$|R_1|+|R_2|\leqslant R,\quad\text{где}\quad R=\sum_{d\mid P,\ d\leqslant D}|r_d|,\quad D=z^{2b+5}.$$

Далее, пользуясь введёнными ранее обозначениями, будем иметь: $W=W_1\dots W_t$. Кроме того,

$$W^*=\sum_{r=1}^{t}\Bigg(\sum_{\substack{d_r\mid P_r\\ \omega(d_r)=k_r+1}}g(d_r)\Bigg)\prod_{j\neq r}\Bigg(\sum_{\substack{d_j\mid P_j\\ \omega(d_j)\leqslant k_j}}\mu(d_j)g(d_j)\Bigg)=$$

$$=\sum_{r=1}^{t}\Bigg(\sum_{\substack{d_r\mid P_r\\ \omega(d_r)=k_r+1}}g(d_r)\Bigg)\prod_{j\neq r}W_j$$

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

$$W^*=W_1\dots W_t\sum_{r=1}^{t}\frac{1}{W_r}\Bigg(\sum_{\substack{d_r\mid P_r\\ \omega(d_r)=k_r+1}}g(d_r)\Bigg).$$

Но сумма по d_r легко оценивается с помощью трюка Эрдеша:

$$\sum_{\substack{d_r|P_r\\ \omega(d_r)=k_r+1}} g(d_r) \leqslant \frac{\big(\ln(1/V_r)\big)^{k_r+1}}{(k_r+1)!} = \frac{L_r^{k_r+1}}{(k_r+1)!},$$

где, как и выше,

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

Итак,

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

Собирая полученные оценки, находим:

$$S(\mathcal{A}, z) \geqslant XV(z)(1-E) - R.$$

Тем самым доказана

Теорема 6. Если последовательность неотрицательных чисел a_n, $n \in \mathcal{A}$, и отвечающая ей мультипликативная функция g удовлетворяют условиям Теоремы 5, то для просеивающей функции $S(\mathcal{A}, z)$ справедливо неравенство:

$$S(\mathcal{A}, z) \geqslant XV(z)(1-E) - R,$$

в котором

$$R = \sum_{d|P,\ d\leqslant D} |r_d|, \quad D = z^{2b+5},$$

а E — то же, что и в Теореме 5.

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

Теорема 7. Пусть последовательность неотрицательных чисел a_n, $n \in \mathcal{A}$, такова, что для любого бесквадратного числа d выполнено равенство

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

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

$$\text{(a) } 0 \leqslant g(p) < 1 \quad \text{для любого простого } p;$$

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

для любых чисел u и v с условиями $\frac{3}{2} \leqslant u < v$, где $\varkappa, K$ - положительные постоянные. Тогда для любого чётного $b \geqslant 2$ 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 $z \geqslant z_0$ для величины

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

выполняются неравенства:

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

$$R_j = \sum_{d|P,\ d \leqslant D_j} |r_d|,\ D_0 = z^{\Delta},\ D_1 = z^{\Delta+1},\ \Delta = \frac{b}{1 - e^{-\lambda}} + \frac{2e^{-\lambda}}{(1 - e^{-\lambda})^2},$$

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

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

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 нечётных простых числах p_1, p_2 уравнения $p_1 + p_2 = 2N$, где $N \geqslant 3$ — любое целое число.

Теорема 8. Существует абсолютная постоянная N_0 такая, что при любом целом $N \geqslant N_0$ число $2N$ представляется как сумма $a + b$, в которой каждое из слагаемых имеет не более 10 простых делителей.

Доказательство. Рассмотрим последовательность

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

Тогда для бесквадратного d имеем:

$$|\mathcal{A}_d| = \sum_{\substack{3 \leqslant m \leqslant 2N-3 \\ m(2N-m) \equiv 0 \,(\mathrm{mod}\, d)}} = \left[\frac{2N-5}{d}\right] \nu(d) + \theta_1 \nu(d),$$

где $\nu(d)$ — число решений сравнения $m(2N-m) \equiv 0 \,(\mathrm{mod}\, d)$ с условием $1 \leqslant m \leqslant d$. Несложно видеть, что при $d = p$ - простом

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

Следовательно, $\nu(d) = 2^{\omega_{2N}(d)}$, где, как и выше, $\omega_a(n)$ — число простых делителей n, не делящих a. Отсюда заключаем, что первое условие Теоремы 7 выполнено с

$$g(d) = \frac{\nu(d)}{d}, \quad |r_d| \leqslant \nu(d) \leqslant 2^{\omega(d)} \quad \text{и} \quad X = 2N.$$

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

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

$$= \prod_{u<p\leqslant v,\, p|2N} \left(1-\frac{1}{p}\right)^{-1} \times \prod_{u<p\leqslant v,\, p\nmid 2N} \left(1-\frac{2}{p}\right)^{-1} \leqslant$$

$$\leqslant \prod_{u<p\leqslant v,\, p|2N} \left(1-\frac{2}{p}\right)^{-1} \times \prod_{u<p\leqslant v,\, p\nmid 2N} \left(1-\frac{2}{p}\right)^{-1} = \prod_{u<p\leqslant v} \left(1-\frac{2}{p}\right)^{-1}$$

(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

$$\prod_{u<p\leqslant v}\left(1-\frac{2}{p}\right)^{-1} \leqslant \prod_{u<p\leqslant v}\left(1-\frac{1}{p}\right)^{-2}\prod_{p\geqslant q}\frac{(p-1)^2}{p(p-2)}.$$

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 $q \geqslant 3$, так что $q-2 \geqslant q/3 > u/3$. Следовательно, по формуле Мертенса находим:

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

$$= \left(\frac{\ln v}{\ln u}\right)^2 \times \left(1+O\left(\frac{1}{\ln u}\right)\right)\left(1+O\left(\frac{1}{\ln v}\right)\right)\left(1+\frac{3}{u}\right) \leqslant$$

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

где K_0 — достаточно большая абсолютная постоянная.

Если же $\frac{3}{2} < u \leqslant 2$, то исходное произведение (по $u < p \leqslant v$) отличается от произведения

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

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

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

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

где в качестве K можно взять, например, величину $1 + K_0/\ln(5/2)$.

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

$$S(\mathcal{A}, z) \geqslant 2NV(z)(1-E) - R,$$

где

$$V(z)=\prod_{p\leqslant z}(1-g(p)),\quad R=\sum_{d|P,\ d\leqslant z^{\Delta}}\nu(d),$$

$$\Delta=\Delta(b,\lambda)=\frac{b}{1-e^{-\lambda}}+\frac{2e^{-\lambda}}{(1-e^{-\lambda})^2}+1,\quad E\leqslant e^{2\lambda}F(b,2\lambda)+\frac{c}{\ln z}.$$

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

$$V(z)=\prod_{p\leqslant z,\ p|2N}\left(1-\frac{1}{p}\right)\prod_{p\leqslant z,\ p\nmid 2N}\left(1-\frac{2}{p}\right)\geqslant$$
$$\geqslant\prod_{p|2N}\left(1-\frac{1}{p}\right)\prod_{2<p\leqslant z}\left(1-\frac{2}{p}\right)=\frac{\varphi(2N)}{2N}\prod_{2<p\leqslant z}\left(1-\frac{1}{p}\right)^2\cdot\frac{p(p-2)}{(p-1)^2},$$

где $\varphi(m)$ — функция Эйлера.

Последнее произведение не меньше, чем

$$\prod_{2<p\leqslant z}\left(1-\frac{1}{p}\right)^2\cdot\prod_{n=3}^{+\infty}\frac{n(n-2)}{(n-1)^2}=\frac{1}{2}\prod_{2<p\leqslant z}\left(1-\frac{1}{p}\right)^2\geqslant$$
$$\geqslant 2\prod_{p\leqslant z}\left(1-\frac{1}{p}\right)^2\geqslant\frac{2e^{-2\gamma}}{(\ln z)^2}\left(1-\frac{c_1}{\ln z}\right),$$

где $c_1>0$ — должным образом подобранная константа.

Далее, ввиду равенства $2^{\omega(d)}=\tau(d)$, где $\tau(d)=\sum\limits_{d|n}1$ — число делителей d, имеем: $\nu(d)\leqslant\tau(d)$, откуда

$$R\leqslant\sum_{d\leqslant z^{\Delta}}\tau(d)=\sum_{d\leqslant z^{\Delta}}\sum_{mn=d}1=\sum_{mn\leqslant z^{\Delta}}1=$$
$$=\sum_{m\leqslant z^{\Delta}}\sum_{n\leqslant\frac{z^{\Delta}}{m}}1\leqslant\sum_{m\leqslant z^{\Delta}}\frac{z^{\Delta}}{m}<z^{\Delta}(\ln z^{\Delta}+1)<2\Delta z^{\Delta}(\ln z).$$

Итак,

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

Возьмём $b = 2, \lambda = 0.595$. Тогда при достаточно большом z будем иметь $E < 0.991$, $\Delta = 10.9455$. Беря ε достаточно малым, положим $z = (2N)^{(1-\varepsilon)/\Delta}$. Можно показать (см. далее Задачу 10), что $\varphi(2N) > N/(\ln N)$ для всех достаточно больших N. Поэтому

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

откуда

$$S(\mathcal{A}, z) \geqslant \frac{2\Delta^2 e^{-2\gamma}}{(1-\varepsilon)^2} \cdot 0.009 \frac{\varphi(2N)}{(\ln 2N)^2} \left(1 - \frac{\Delta c_1}{(1-\varepsilon)} \frac{1}{\ln 2N}\right) - (\varphi(2N))^{1-\varepsilon/3} > \\ > \frac{2}{3} \frac{\varphi(2N)}{(\ln 2N)^2}.$$

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 $z = (2N)^{(1-\varepsilon)/\Delta}$. Поэтому их число не превышает 10. В противном случае мы имели бы неравенства

$$\max(a, b) \geqslant (2N)^{11(1-\varepsilon)/\Delta} > 2N,$$

что невозможно (конечно, при условии $0 < \varepsilon < 1 - \Delta/11 = 0.004954\ldots$). Теорема доказана. □

Замечание 6. Этот же результат можно получить выбором $b = 4, \lambda = 0.89$.

Вдумчивый читатель вправе спросить: почему бы нам не попытаться оценить число $\pi_2(x)$ простых близнецов не количеством тех целых m, для которых произведение $m(m+2)$ взаимно просто с $P(z)$, а количеством 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

$$a_n = \begin{cases} 1, \text{ если } n = p + 2, \text{ где } p \text{ — простое}, \\ 0, \text{ иначе.} \end{cases}$$

Тогда $|\mathcal{A}_d|$ 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 $p \leqslant x$ с условием $p \equiv a \pmod q$, получим

$$|\mathcal{A}_d| = \pi(x, d, d-2). \tag{3}$$

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 (1837), это условие является и достаточным.

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

Задача 10. Докажите, что: а) $\varphi(q)$ мультипликативна; б) для простого p и целого $k \geqslant 1$ справедливо равенство: $\varphi(p^k) = p^k\,(1 - 1/p)$; в) $\varphi(N) > N/\ln N$ для всех достаточно больших N.

Указание. Пусть $q_1^{k_1} \dots q_r^{k_r}$ - каноническое разложение N, причём $q_1 < q_2 < \dots < q_r$; тогда $q_s \geqslant p_s$ (где p_s - s-е по счёту простое число); далее воспользоваться п.п. а), б) и неравенством Леммы 1.

Итак, имеется $\varphi(q)$ прогрессий с разностью q, каждая из которых содержит простые числа. Естественно предположить, что в первом приближении количества простых $p \leqslant x$ 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 выполнении некоторых условий величина $R(x, q, a)$ будет мала по сравнению с $\pi(x)/\varphi(q)$.

Если q — постоянная величина, то это действительно так; более того, если q растёт вместе с x, но не быстрее произвольной фиксированной степени логарифма ($q \leqslant (\ln x)^A$), асимптотика

$$\pi(x, q, a) = (1 + o(1))\,\frac{\pi(x)}{\varphi(q)} \tag{4}$$

всё ещё имеет место. Хуже обстоит дело, если q ведёт себя как степень x. Имеющиеся оценки являются «условными», то есть доказаны в предпо-

ложении справедливости некоторых гипотез. Например, из расширенной гипотезы Римана (что бы это ни значило) следует, что асимптотическое равенство (4) остаётся справедливым при $q \leqslant x^{1/2-\varepsilon}$, где $\varepsilon > 0$ – сколь угодно малое фиксированное число.

Тем не менее, попробуем применить нижнюю оценку Теоремы 7 к случаю, когда $|\mathcal{A}_d|$ определяется равенством (3). Здесь имеем $X = \pi(x)$, $g(d) = 1/\varphi(d)$ при нечетном d и $g(d) = 0$ в противном случае, и, наконец, $r_d = R(x, d, d-2)$.

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

$$\prod_{u<p\leqslant v} (1-g(p))^{-1} = \prod_{u<p\leqslant v,\ p\neq 2} \left(1-\frac{1}{p}\right)^{-1}\left(1+\frac{1}{p(p-2)}\right) \leqslant \\ \leqslant \left(\frac{\ln v}{\ln u}\right)^{\varkappa}\left(1+\frac{K}{\ln u}\right)$$

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

$$S(\mathcal{A}, z) \geqslant \pi(x)V(z)\left(1 - E - \frac{c_0}{\ln z}\right) - R_1,$$

где

$$E \leqslant e^{\lambda}F(b,\lambda), \quad F(b,\lambda) = \operatorname{sh}(\lambda) - \sum_{r=1}^{b/2}\frac{\lambda^{2r-1}}{(2r-1)!},$$

$$V(z) = \prod_{p\leqslant z}(1-g(p)) = \prod_{2<p\leqslant z}\frac{p-2}{p-1} = \prod\left(1-\frac{1}{p}\right)\left(1-\frac{1}{(p-1)^2}\right) \geqslant \\ \geqslant 2\prod_{p\geqslant 3}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\leqslant z}\left(1-\frac{1}{p}\right) \geqslant \frac{2C_1e^{-\gamma}}{\ln z}\left(1-\frac{C_2}{\ln z}\right),$$

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

Выбор $b = 2, \lambda = 1.192$ даёт $E < 0.99806\ldots, \Delta = 5.1241\ldots$ Замечая, что

$$C_1 = \prod_{p\geqslant 3}\left(1-\frac{1}{(p-1)^2}\right) > 0.65,$$

при достаточно большом z находим

$$S(\mathcal{A}, z) > 1.4 \cdot 10^{-3} \frac{\pi(x)}{\ln z} - \sum_{d \leqslant z^{\Delta}} |r_d|.$$

Как уже отмечалось, оценок величин $|r_d| = |R(x, d, d-2)|$ при больших d в нашем распоряжении нет. Тем не менее завершить оценку $S(\mathcal{A}, z)$ всё-таки 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 слишком велик, то таких чисел, по-видимому, не очень много и они не сильно повлияют на сумму по всем $d \leqslant z^{\Delta}$.

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

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

$$R(x, q, a) = \pi(x, q, a) - \frac{\pi(x)}{\varphi(q)}, \quad R(x, q) = \max_{2 \leqslant y \leqslant x} \max_{(a,q)=1} |R(y, q, a)|.$$

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

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

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

Замечание 7. Доказано, что можно положить $B = A + 2$ (имеются и более точные результаты). Однако в отличие от B константа C неэффективна: мы не имеем способа вычислить значение C по заданному A.

Положим $A = 3$ (так что $B = 5$) и выберем z из условия $z^{\Delta} =$

$\sqrt{x}(\ln x)^{-5}$. Тогда из Теоремы 9 заключаем

$$\sum_{d\leqslant z^{\Delta}} |r_d| \leqslant \frac{Cx}{(\ln x)^3},$$

$$S(\mathcal{A},z) \geqslant 1.4\cdot 10^{-3}\cdot\frac{\pi(x)}{\ln z} - \frac{Cx}{(\ln x)^3} \geqslant 1.3\cdot 10^{-3}\cdot\frac{\pi(x)}{\ln z} > \\ > 1.3\cdot 10^{-3}\cdot 2\Delta\,\frac{\pi(x)}{(\ln x)} > \frac{x}{(9\ln x)^2},$$

если только достаточно велико: $x \geqslant x_0$. Неприятным следствием неэффективности постоянной C в Теореме 9 оказывается тот факт, что и константа x_0 — неэффективна.

Остаётся заметить, что для каждого простого p, которое учитывается в сумме $S(\mathcal{A},z)$, число $p+2$ взаимно просто с произведением $P(z)$. Таким образом, все его простые делители превышают $x^{1/(2\Delta)}\,(\ln x)^{-7/\Delta}$. Поскольку $2\Delta < 11$, мы приходим к следующему утверждению:

Теорема 10. Если x достаточно велико, имеется не менее $x/(9\ln x)^2$ простых чисел $p, p\leqslant x$, для которых $p+2$ имеет не более 10 простых делителей.

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

Задача 11. Оцените снизу число представлений чётного числа $2N$ суммою вида $p+m$, где $p\geqslant 3$ — простое, а m имеет не более чем k простых делителей (постарайтесь сделать k как можно меньшим).

5 Решето Сельберга

5.1 Неотрицательность квадрата: тривиальная посылка и нетривиальные следствия

Простой и красивый метод верхней оценки просеивающей функции был предложен в 1947 году норвежским математиков Атле Сельбергом (1917-2007). В решете Бруна доказательство неравенства

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

для выбранных d требовало определённых усилий. В решете Сельберга это достигается почти автоматически.

Зададимся достаточно большим числом z, $z \geqslant z_0 > 2$, и положим $D = z^2$. Как и в решете Бруна, параметр D будет отвечать за число слагаемых в остаточном члене R. Пусть ρ_d — последовательность вещественных чисел с условием $\rho_1 = 1$. Тогда величина

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

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

$$\sum_{d|n} \mu(d) \leqslant \left(\sum_{d|n} \rho_d\right)^2.$$

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

$$\left(\sum_{d|n} \rho_d\right)^2 = \sum_{d_1,d_2|n} \rho_{d_1}\rho_{d_2} =$$

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

Задача 12. Выразите λ_d через ρ_δ для $d = p, pq$ (p, q — простые, $p \neq q$).

В чём преимущество новой мажоранты? Последовательность ρ_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, носителями последовательности ρ_d будут делители $P(z)$, не превосходящие z. Легко сообразить, что носителем последовательности λ_d будут делители $P(z)$, не превосходящие $D = z^2$.

Другое преимущество решета Сельберга состоит в том, что величины ρ_d можно выбирать в дальнейшем оптимально с учётом структуры последовательности a_n. Попутно заметим, что решето Бруна было лишено этого преимущества: величины λ_d выбирались раз и навсегда — если не брать в расчёт некоторую свободу в выборе величин b и λ в Теореме 7.

5.2 Простые числа в арифметических прогрессиях

Сначала мы применим решето Сельберга к доказательству верхней оценки величины $\pi(x, q, a)$, $(a, q) = 1$. Напомним, что

$$\pi(x, q, a) \sim \pi(x)/\varphi(q)$$

для случая, когда q фиксировано или растёт с ростом x не быстрее степени логарифма x. Использованная нами выше теореме Бомбьери-Виноградова показывает, что асимптотика для $\pi(x, q, a)$ имеет место для «почти всех» модулей q, $q \leqslant \sqrt{x}(\ln x)^{-B}$. Однако в ряде задач необходима правильная по порядку (или близкая к таковой) верхняя оценка $\pi(x, q, a)$, которая была бы справедлива в максимально широком диапазоне: $3 \leqslant q \ll x$. Именно такую оценку даёт следующая

Теорема 11 (В. Брун, Э. Титчмарш). Существует абсолютная постоянная $x_0 > 1$ такая, что для любого $x \geqslant x_0$ и любых a и q с условиями $(a, q) = 1$, $3 \leqslant q \leqslant 5x/16$ выполнено неравенство:

$$\pi(x, q, a) \leqslant \frac{2x}{\varphi(q)\ln(x/q)}\left(1 + \frac{4\ln\ln(x/q)}{\ln(x/q)}\right)$$

Доказательство. Задавшись некоторым z и последовательностью ρ_d с перечисленными выше свойствами, для множества $\mathcal{A}$ чисел n, $n \leqslant x$, $n \equiv a \pmod q$, будем иметь:

$$\pi(x, q, a) - \pi(z, q, a) \leqslant S(\mathcal{A}, z) = \sum_{\substack{n \leqslant x \\ n \equiv a \,(\mathrm{mod}\, q)}} \left(\sum_{d|(n,P)} \mu(d)\right) \leqslant$$

$$\leqslant \sum_{\substack{n \leqslant x \\ n \equiv a \,(\mathrm{mod}\, q)}} \left(\sum_{d|(n,P)} \rho_d\right)^2, \quad \text{где} \quad P = P(z) = \prod_{p \leqslant z} p.$$

Заметим, что в силу свойств ρ_d вместо $d|(n, P)$ во внутренней сумме можно писать $d|n$.

Таким образом,

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

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

$$\begin{cases} n \equiv a \,(\mathrm{mod}\, q), \\ n \equiv 0 \,(\mathrm{mod}\, d) \end{cases}$$

совместна лишь в случае, когда d и q взаимно просты.

Действительно, в противном случае мы имели бы некоторое простое число p, делящее d, q и n и потому делящее a, что невозможно. Итак, ненулевой вклад в $S(\mathcal{A}, z)$ вносят лишь те d_1, d_2, что взаимно просты с q. Суммирование по таким числам станем далее отмечать штрихом. Если $(d, q) = 1$, то положив $n = dm$, будем иметь:

$$m \equiv ad^* \,(\mathrm{mod}\, q), \quad 1 \leqslant m \leqslant \frac{x}{d}$$

(символом d^* обозначается обратный вычет: $dd^* \equiv 1 \,(\mathrm{mod}\, q)$). В этом случае сумма по n будет равна $x/(qd) + \theta$, где $|\theta| \leqslant 1$. Итак,

$$S(\mathcal{A}, z) \leqslant \sum_{d_1, d_2 \leqslant z}{}' \rho_{d_1}\rho_{d_2}\left(\frac{x}{qd} + \theta\right) = \frac{x}{q}W + R,$$

где

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

Поскольку нам ещё только предстоит выбрать коэффициенты ρ_d, оценку R отложим на потом и займемся сперва изучением суммы W. Заметим, что она является ничем иным как квадратичной формой от переменных ρ_d. Поэтому нашей ближайшей целью станет приведение её к диагональному виду.

Прежде всего, равенство $[d_1, d_2](d_1, d_2) = d_1 d_2$ даёт:

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

Воспользуемся теперь тождеством

$$m = \sum_{\delta | m} \varphi(\delta)$$

где φ, как и выше, — функция Эйлера.

Задача 13. Докажите это тождество.

Полагая в нём $m = (d_1, d_2)$, получим:

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

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

Ясно теперь, что замена

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

приводит форму W к диагональному виду:

$$W = \sum_{\delta\leqslant z}{}' \varphi(\delta) u_\delta^2. \tag{5}$$

Но желательно иметь и формулы обратной замены. Зафиксируем бесквадратное $m \leqslant z$ и рассмотрим сумму

$$\sum_{\delta\leqslant z/m}{}' \mu(\delta) u_{m\delta}.$$

Подставляя в неё выражения для $u_{m\delta}$, приводим её к виду

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

Вводя обозначение $k = n\delta$, будем иметь $k \leqslant z/m$, $\delta \mid k$, так что

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

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

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

$$\sum_{\delta\leqslant z}{}' \mu(\delta) u_\delta = 1. \tag{6}$$

5.3 Минимизация квадратичной формы

Наша следующая цель — выбрать переменные u_δ так, чтобы сумма W была как можно меньше. Иначе говоря, нам необходимо минимизировать квадратичную форму (5) при условии (6).

Эту задачу можно решить методом неопределённых множителей Лагранжа, составив функцию

$$F(\lambda, \bar{u}) = \sum_{\delta \leqslant z}{}' \varphi(\delta) u_\delta^2 - \lambda \left(\sum_{\delta \leqslant z}{}' \mu(\delta) u_\delta - 1 \right), \quad \bar{u} = (u_\delta)_\delta,$$

и приравняв нулю все её производные $\partial F / \partial u_\delta$ (проделайте это самостоятельно!). Существование минимума более-менее очевидно из геометрических соображений.

Но мы приведём иное рассуждение, которое опирается лишь на неравенство Коши. Перепишем (6) в виде

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

Тогда в силу неравенства Коши,

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

где

$$G = G_q(z) = \sum_{\substack{\delta \leqslant z \\ (\delta, q) = 1}} \frac{\mu^2(\delta)}{\varphi(\delta)}.$$

Следовательно, $W \geqslant G^{-1}$ при любом допустимом выборе переменных u_δ. Если мы покажем, что на каком-то наборе $\bar{u} = (u_\delta)_\delta$ равенство достигается, то задача минимизации будет решена.

Заметим, что неравенство Коши

$$\left(\sum_n a_n b_n \right)^2 \leqslant \sum_n a_n^2 \sum_n b_n^2$$

для последовательностей a_n, b_n одного знака обращается в равенство, если одна последовательность пропорциональна другой: $b_n = \lambda a_n$, где λ

не зависит от n. Потребуем, чтобы равенство

$$\lambda u_\delta \sqrt{\varphi(\delta)} = \frac{\mu(\delta)}{\sqrt{\varphi(\delta)}}$$

выполнялось для всех $\delta \leqslant z, \delta \mid P, (\delta, a) = 1$. Получим

$$u_\delta = \frac{1}{\lambda} \cdot \frac{\mu(\delta)}{\varphi(\delta)},$$

где значение λ теперь легко находится из условия (6):

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

Поэтому значения переменных u_δ и ρ_d, минимизирующие W, имеют вид

$$u_\delta = \frac{1}{G} \frac{\mu(\delta)}{\varphi(\delta)} = \left(\sum_{\delta \leqslant z}{}' \frac{\mu^2(\delta)}{\varphi(\delta)} \right)^{-1} \frac{\mu(\delta)}{\varphi(\delta)}, \text{ если } (\delta, q) = 1, \delta \leqslant z, \delta \mid P.$$

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

5.4 Оценка величины R

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

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

Следовательно,

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

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

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

Но любое бесквадратное n, $n \leqslant z$, единственным образом представляется в виде $n = d\delta$, где $d|m$, $(\delta, m) = 1$ (при этом условие $\delta \leqslant z/m$ может нарушаться). Поэтому значения $n = d\delta$ в сумме не повторяются, и при этом все отвечающие им слагаемые встречаются в сумме G. Следовательно,

$$|\rho_m| \leqslant \frac{1}{G} \cdot G = 1, \quad |R| \leqslant \left(\sum_{d \leqslant z} |\rho_d| \right)^2 \leqslant z^2.$$

Таким образом,

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

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

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

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

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

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

Пусть $q \geqslant 2$. Сгруппируем вместе те слагаемые суммы

$$G_1(z) = \sum_{n \leqslant z} \frac{\mu^2(n)}{\varphi(n)},$$

что отвечают одному и тому же значению $(n, q) = \delta$, где δ — делитель q.

Получим:

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

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

откуда

$$G_q(z) \geqslant \frac{\varphi(q)}{q}\, G_1(z).$$

Итак, осталось оценить $G_1(z)$ снизу. Для этого заметим, что

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

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

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

$$G_1(z) = \sum_{n\leqslant z} \sum_{m|n^\infty} \frac{\mu^2(n)}{nm}.$$

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

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

(a называют радикалом k и пишут: $a = \mathrm{rad}(k)$). Если при этом $k \leqslant z$, то тем более $a \leqslant z$. Следовательно, сумма $G_1(z)$ содержит все дроби $1/k, 1 \leqslant k \leqslant z$. Поэтому

$$G_1(z) \geqslant \sum_{1\leqslant k\leqslant z} \frac{1}{k} > \ln z + \frac{3}{10}$$

для любого $z \geqslant 1$.

Задача 14. Проверьте это!

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

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

Возьмём теперь

$$z=\frac{\sqrt{x/q}}{\ln(x/q)}.$$

Тогда, положив для краткости $y=\ln(x/q)$, будем иметь:

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

$$\begin{aligned}\pi(x,q,a) &\leqslant \frac{x}{\varphi(q)}\cdot\frac{2}{y}\left(1-\frac{2\ln y-3/5}{y}\right)^{-1}+\frac{e^y}{y}\left(\frac{1}{y}+e^{-y/2}\right)=\\ &=\frac{2x}{\varphi(q)y}\left\{\left(1-\frac{2\ln y-3/5}{y}\right)^{-1}+\frac{\varphi(q)}{x}\,\frac{y}{2}\frac{e^y}{y}\left(\frac{1}{y}+e^{-y/2}\right)\right\}\leqslant\\ &\leqslant\frac{2x}{\varphi(q)y}\left(1+\Delta(y)\,\frac{\ln y}{y}\right),\\ \Delta(y)&=\frac{2(1-3/(10\ln y))}{1-2(\ln y)/y+3/(5y)}+\frac{1+ye^{-y/2}}{2\ln y}.\end{aligned}$$

Вычисления показывают, что $\Delta(y)\leqslant 4$ при $y\geqslant\ln(16/5)$. Теорема доказана. □

Замечание 8. 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 определённом диапазоне изменения q) привело бы к существенным продвижениям во многих задачах теории чисел.

5.5 Решето Сельберга: общий случай

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 такова, что

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

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

$$\sum_{d_1,d_2\leqslant z}{}' \frac{g(d_1)g(d_2)}{g((d_1,d_2))}\,\rho_{d_1}\rho_{d_2}, \tag{7}$$

где штрих означает суммирование по делителям числа $P = P(z)$, не имеющим в каноническом разложении простых из некоторого множества $\mathcal{P}$ (так, в Теореме 11 роль $\mathcal{P}$ фактически играло множество простых делителей разности прогрессии q).

Чтобы привести форму (7) 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

Лемма 3 (формула обращения Мёбиуса). Пусть F и f — мультипликативные функции, причём

$$F(d) = \sum_{\delta|d} f(\delta) \quad \text{при всех} \quad d \geqslant 1. \tag{8}$$

Тогда

$$f(d) = \sum_{\delta|d}\mu(\delta)F\left(\frac{d}{\delta}\right) \quad \text{при всех} \quad d \geqslant 1. \tag{9}$$

Верно и обратное: выполнение (9) для всех d влечёт и справедливость (8) для каждого $d \geqslant 1$.

Доказательство. Действительно, беря произвольное $d \geqslant 1$, из (8) и Теоремы 1 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:

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

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

(обратите внимание: мы несколько раз воспользовались тем, что d — бесквадратное!).

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

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

Вновь отметим: в частном случае $g(p) = 1/p$ 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:

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

$$= \sum_{\delta \leqslant z}{}' \frac{1}{h(\delta)} \sum_{\substack{d_1, d_2 \leqslant z \\ d_1, d_2 \equiv 0 \,(\mathrm{mod}\, \delta)}} g(d_1) \rho_{d_1} g(d_2) \rho_{d_2} = \sum_{\delta \leqslant z}{}' \frac{u_\delta^2}{h(\delta)},$$

где

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

(условие $\delta | P(z)$ в сумме по $\delta \leqslant z$ можно опустить: в силу свойств величин ρ_d слагаемые, не удовлетворяющие этому условию, дадут нулевой вклад).

Далее, формулы обратной замены получаются с помощью Теоремы 1:

если $m|P$ и $m \leqslant z$, то

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

$$= \sum_{km \leqslant z}{}' g(km)\rho_{km} \sum_{\delta | k} \mu(\delta) = g(m)\rho_m,$$

откуда

$$\rho_m = \frac{1}{g(m)} \sum_{\delta \leqslant z/m}{}' \mu(\delta) u_{m\delta}.$$

В частности, равенство $\rho_1 = 1$ в новых переменных принимает вид (6). Минимизация формы (7) при условии (6) проводится точно так же. При этом наименьшее значение W оказывается равным $1/G(z)$, где

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

а значения переменных u_δ и ρ_m, доставляющие этот минимум, задаются равенствами

$$u_\delta = \frac{\mu(\delta) h(\delta)}{G(z)},$$

$$\rho_m = \frac{\mu(m)}{G(z)} \frac{h(m)}{g(m)} \sum_{\substack{d \leqslant z/m \\ (d,m)=1}}{}' \mu^2(d) h(d).$$

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 $|\rho_m| \leqslant 1$. Переходя к оценке остаточного члена, будем иметь:

$$|R| \leqslant \sum_{d_1, d_2 \leqslant z}{}' |\rho_{d_1} \rho_{d_2}| \cdot |r_{[d_1,d_2]}| \leqslant \sum_{\substack{d_1, d_2 \leqslant z \\ d_1, d_2 | P}}{}' |r_{[d_1,d_2]}| \leqslant \sum_{\substack{d | P \\ d \leqslant z^2}} |r_d| f(d),$$

где символом $f(d)$ обозначено число пар d_1, d_2, отвечающих условию $[d_1, d_2] = d$.

Задача 15. Докажите, что $f(d) = 3^{\omega(d)}$ для бесквадратного d.

Следовательно,

$$|R| \leqslant \sum_{\substack{d|P \\ d\leqslant z^2}} 3^{\omega(d)}|r_d|. \tag{10}$$

В частном случае (который, однако, нередко встречается на практике), когда $|r_d| \leqslant Bdg(d)$, где B — некоторая постоянная, имеем цепочку неравенств

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

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

$$\leqslant Bz^2\prod_{p\leqslant z}(1-g(p))^{-3} = Bz^2V^{-3}(z), \quad V(z) = \prod_{p\leqslant z}(1-g(p)).$$

Отметим ещё один частный случай, в котором оценка (10) может быть указана явно. Именно, пусть $|r_d| \leqslant B$ для любого бесквадратного d. Тогда

$$|R| \leqslant \sum_{\substack{d_1,d_2|P \\ d_1,d_2\leqslant z}}{}' |r_{[d_1,d_2]}| \leqslant B\sum_{\substack{d_1,d_2|P \\ d_1,d_2\leqslant z}}{}' 1 \leqslant B\left(\sum_{d\leqslant z} 1\right)^2 = Bz^2.$$

Так мы приходим к общему утверждению:

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

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

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

$$S(\mathcal{A}, z) \leqslant \frac{X}{G(z)} + R, \quad \text{в котором} \quad G(z) = \sum_{d\leqslant z}\mu^2(d)h(d),$$

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

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

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

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

соответственно.

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

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

где C — абсолютная постоянная.

5.6 Малые промежутки между простыми

Воспользуемся результатом Задачи 16 для доказательства наличия одной «аномалии» в распределении простых чисел. С этого момента договоримся, что все простые числа занумерованы в порядке возрастания, а символ p_n означает n-е простое число: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$ и т.д. Из приведённой ранее асимптотической формулы для $\pi(x)$ следует, что разность $p_{n+1} - p_n$ между соседними простыми числами «в среднем» ведёт себя как $(1 + o(1)) \ln p_n$.

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

Теорема 13 (П. Эрдёш, 1940). Существует абсолютная положительная постоянная $\delta < 1$, такая, что для бесконечного множества пар соседних простых чисел p_n, p_{n+1} выполнено неравенство

$$p_{n+1} - p_n \leqslant (1 - \delta) \ln p_n.$$

Доказательство. Зададимся достаточно большим X и достаточно малой постоянной δ. Предположим, что все простые числа p_n, $X < p_n \leqslant 2X$, удовлетворяют условию

$$p_{n+1} - p_n > (1-\delta)\ln X.$$

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

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

Если p_k, p_l — ближайшие справа к X и $2X$ простые числа, то в силу асимптотического закона $p_k - X = o(X)$, $p_l - 2X = o(X)$, так что

$$S = (p_{k+1} - p_k) + \ldots + (p_l - p_{l-1}) = p_l - p_k = X + o(X).$$

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

$$\begin{aligned} S = \sum_{a>U}{}' a|E_a| &= \left(\sum_{U<a\leqslant V}{}' + \sum_{a>V}{}'\right) a|E_a| \geqslant \\ &\geqslant \sum_{U<a\leqslant V}{}' a|E_a| + V\sum_{a>V}{}' E_a = \\ &= \sum_{U<a\leqslant V}{}' a|E_a| + V\left(\pi(2X) - \pi(X) - \sum_{U<a\leqslant V} |E_a|\right) = \\ &= V(\pi(2X) - \pi(X)) - \sum_{U<a\leqslant V}{}' |E_a|(V-a). \end{aligned}$$

Слагаемые последней суммы неотрицательны. Обозначая сумму через S_1, оценим её сверху, пользуясь неравенством Задачи 16. Очевидно,

$$|E_a| \leqslant \pi_a(2X) \leqslant C\prod_{p|a}\left(1+\frac{1}{p}\right)\frac{X}{(\ln X)^2}.$$

Следовательно,

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

где смысл обозначений S_2 и S_3 очевиден.

Имеем, далее:

$$S_2 = \sum_{U<a\leqslant V}{}' \sum_{d|a} \frac{\mu^2(d)}{d} = \sum_{d\leqslant V} \frac{\mu^2(d)}{d} \sum_{\substack{U<a\leqslant V \\ a\equiv 0 \,(\mathrm{mod}\, d) \\ a\equiv 0 \,(\mathrm{mod}\, 2)}} 1.$$

Если d — нечётное, то сумма по a приводится к виду $(V-U)/(2d)+O(1)$, а если d — чётное, то к виду $(V-U)/d+O(1)$. Поэтому

$$S_2 = \frac{V-U}{2} \sum_{\substack{d\leqslant V \\ d\equiv 1 \,(\mathrm{mod}\, 2)}} \frac{\mu^2(d)}{d^2} + (V-U) \sum_{\substack{d\leqslant V \\ d\equiv 0 \,(\mathrm{mod}\, 2)}} \frac{\mu^2(d)}{d^2} + O(\ln V).$$

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

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

Задача 17. Считая известными формулы

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}, \quad \zeta(4) = \sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90},$$

и применяя тождество Эйлера, докажите, что

$$\sum_{\substack{d=1 \\ d\equiv 1 \,(\mathrm{mod}\, 2)}}^{\infty} \frac{\mu^2(d)}{d^2} = \frac{12}{\pi^2}, \qquad \sum_{\substack{d=1 \\ d\equiv 0 \,(\mathrm{mod}\, 2)}}^{\infty} \frac{\mu^2(d)}{d^2} = \frac{3}{\pi^2}.$$

Указание.

$$1 + \frac{1}{p^2} = \frac{1-1/p^4}{1-1/p^2}.$$

Пользуясь результатом Задачи 17, находим:

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

Подобным образом вычисляется сумма S_3:

$$S_3 = \sum_{U<a\leqslant V}{}' a \sum_{d|a} \frac{\mu^2(d)}{d} = \sum_{d\leqslant V} \frac{\mu^2(d)}{d} \sum_{\substack{U<a\leqslant V \\ a\equiv 0 \,(\mathrm{mod}\, d) \\ a\equiv 0 \,(\mathrm{mod}\, 2)}} a =$$

$$= \sum_{\substack{d\leqslant V \\ d\equiv 1 \,(\mathrm{mod}\, 2)}} \frac{\mu^2(d)}{d} \left(\frac{V^2-U^2}{4d} + O(V) \right) +$$

$$+ \sum_{\substack{d\leqslant V \\ d\equiv 0 \,(\mathrm{mod}\, 2)}} \frac{\mu^2(d)}{d} \left(\frac{V^2-U^2}{2d} + O(V) \right) =$$

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

Возвращаясь к оценке S_1, будем иметь:

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

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

Следовательно,

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

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

Выбирая δ так, чтобы выполнялось неравенство

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

при большом X получаем:

$$S \geqslant \left(1+\frac{\delta}{2}\right) X,$$

что противоречит равенству $S = (1+o(1))X$. Теорема доказана. $\square$

Замечание 9. Теорема Эрдёша — это лишь первый шаг на долгом пути исследования «маленьких» разностей $p_{n+1} - p_n$. Если положить

$$\Delta = \liminf_{n \to +\infty} \frac{p_{n+1} - p_n}{\ln p_n},$$

то Теорема 11 означает, что $\Delta \leqslant 1 - \delta$ при некотором $\delta > 0$. Уточнению оценки Δ был посвящён целый ряд работ, из которых мы упомянем лишь некоторые: $\Delta \leqslant 0.9661$ (Р. Ранкин, 1947), $\Delta \leqslant (2 + \sqrt{3})/8 = 0.466\ldots$ (Э. Бомбьери, Г. Дэвенпорт, 1966), $\Delta \leqslant 0.248$ (Х. Майер, 1988).

Эпохальным событием стало доказательство в 2005 году Д. Голдстоном, Я. Пинтцем, Дж. Йилдиримом равенства $\Delta = 0$. И настоящим триумфом оказалась теорема И. Чжана (2013) о том, что имеется бесконечное множество простых чисел p_n таких, что $p_{n+1} - p_n \leqslant C$, где $C = 7 \cdot 10^7$ — постоянная. Результат Чжана был существенно усилен и обобщён Дж. Мейнардом, Т. Тао и другими исследователями (доказано, в частности, что постоянную C можно заменить на 246), но это уже другая история.

В заключение автор считает приятным долгом поблагодарить организаторов летней школы «Современная математика» и, в частности, Николая Андреева, Григория Мерзона, Виктора Клепцына, а также Никиту Солодовникова, взявшего на себя труд по подготовке исходной LaTeX–версии этой брошюры и Кирилла Аржаных за внимательное прочтение текста и ценные замечания.