Math-Net.Ru

Общероссийский математический портал

С. В. Конягин, Задачи о множестве чисел, свободных от квадратов, *Изв. РАН. Сер. матем.*, 2004, том 68, выпуск 3, 63–90

DOI: <https://doi.org/10.4213/im486>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.198.187.58

26 апреля 2023 г., 16:45:40

УДК 511.337

С. В. Конягин

Задачи о множестве чисел, свободных от квадратов

Пусть N – натуральное число, ES_N – наибольшая мощность подмножества $\mathcal{A} \subset \{1, \dots, N\}$ такого, что число $a + a'$ свободно от квадратов для любых $a \in \mathcal{A}$, $a' \in \mathcal{A}$. Для больших N получены новые оценки величины ES_N сверху и снизу.

Библиография: 17 наименований.

§ 1. Введение

Пусть $\mathcal{S}$ – подмножество множества $\mathbb{N}$ натуральных чисел. Для $N \in \mathbb{N}$ через $ES_N(\mathcal{S})$ обозначим наибольшую мощность подмножества $\mathcal{A} \subset \{1, \dots, N\}$ такого, что $a + a' \in \mathcal{S}$ для любых $a \in \mathcal{A}$, $a' \in \mathcal{A}$ (случай совпадения a и a' не исключается). В основном будем рассматривать $\mathcal{S} = \mathcal{S}_0$ – множество натуральных чисел, свободных от квадратов (т.е. не делящихся ни на какой квадрат простого числа). Будем обозначать $ES_N(\mathcal{S}_0) = ES_N$.

П. Эрдеши и А. Шаркози [6] доказали, что для достаточно большого N справедливо неравенства

$$\frac{\log N}{248} < ES_N < 3N^{3/4} \log N \quad (1.1)$$

(в настоящей работе $\log a$ обозначает натуральный логарифм числа a).

Позднее А. Шаркози [15] усилил верхнюю оценку до $ES_N \ll N^{3/4}$, Х. Элшолц отметил (устное сообщение), что метод работы [6] позволяет уточнить нижнюю оценку: $ES_N \gg \log N \log \log N$. К. Дьярмати [9] доказала существование множеств $\mathcal{A} \subset \{1, \dots, N\}$ и $\mathcal{B} \subset \{1, \dots, N\}$ таких, что $|\mathcal{A}| \gg \log^2 N$, $|\mathcal{B}| \gg \log^2 N$, и при этом все суммы $a + b$, где $a \in \mathcal{A}$, $b \in \mathcal{B}$, свободны от квадратов.

Наряду с $ES_N(\mathcal{S})$ нас будет интересовать величина

$$BR_N(\mathcal{S}) = \sup_M \frac{\max_x |M(x)|}{\int_0^1 |M(x)| dx},$$

где верхняя грань берется по множеству всех ненулевых тригонометрических полиномов $M(x) = \sum_{\substack{n \in \mathcal{S} \\ n \leq N}} a_n e(nx)$, $e(u) = e^{2\pi i u}$. Для определенности положим

$BR_N(\mathcal{S}) = 0$ в случае $\mathcal{S} \cap \{1, \dots, N\} = \emptyset$. Асимптотика величины $BR_N(\mathbb{N})$ при $N \rightarrow \infty$ исследовалась в работах [16], [17] и электронной статье [8].

Работа выполнена при финансовой поддержке РФФИ (грант № 02-01-00248) и Программой поддержки ведущих научных школ РФ (грант № НШ-3004.2003.1).

Будем обозначать $\text{BR}_N(\mathcal{S}_0) = \text{BR}_N$. А. Балог и И. Ружи [1] фактически доказали, что

$$\text{BR}_N \ll N^{3/4} \log N, \quad N \geq 2. \quad (1.2)$$

Существует простая связь между введенными величинами.

ПРЕДЛОЖЕНИЕ 1. $\text{ES}_N(\mathcal{S}) \leq \text{BR}_{2N}(\mathcal{S})$.

ДОКАЗАТЕЛЬСТВО. Пусть множество $\mathcal{A} \subset \{1, \dots, N\}$ таково, что $|\mathcal{A}| = \text{ES}_N(\mathcal{S})$, и $a + a' \in \mathcal{S}$ для любых $a \in \mathcal{A}$, $a' \in \mathcal{A}$. Для полинома $M(x) = \left(\sum_{a \in \mathcal{A}} e(ax)\right)^2$ мы имеем

$$\max_x |M(x)| = |\mathcal{A}|^2, \quad \int_0^1 |M(x)| dx = |\mathcal{A}|,$$

откуда

$$\text{BR}_{2N}(\mathcal{S}) \geq |\mathcal{A}| = \text{ES}_N(\mathcal{S}),$$

что и требовалось доказать.

Не вызывает сомнений, что с ростом N величина ES_N растет значительно медленнее, чем BR_N . Можно ожидать, что для любого $\varepsilon > 0$ справедливо неравенство $\text{ES}_N = o(N^\varepsilon)$ при $N \rightarrow \infty$. В то же время из результатов работы [2] следует, что $\text{BR}_N \gg N^{2/3}$. Однако пока не доказано, что $\text{ES}_N = o(\text{BR}_N)$ при $N \rightarrow \infty$.

В настоящей работе при больших N улучшены оценки сверху для ES_N и BR_N .

ТЕОРЕМА 1. *Существуют эффективные положительные постоянные C_1 и C_2 такие, что для любого $N \geq 3$ справедливы неравенства*

$$\text{BR}_N \leq N^{11/15} \exp\left(\frac{C_1 \log N}{\sqrt{\log \log N}}\right), \quad (1.3)$$

$$\text{ES}_N \leq N^{11/15} \exp\left(\frac{C_2 \log N}{\sqrt{\log \log N}}\right). \quad (1.4)$$

Верхняя оценка величины ES_N в [6] доказана на основе большого решета для квадратных модулей. Фиксировав различные натуральные числа $n_1, \dots, n_Z$, для натурального q и целого h обозначим

$$Z(q, h) = |\{j: n_j \equiv h \pmod{q}\}|.$$

Через p (иногда с индексами) будем обозначать простые числа. Пусть все числа $n_1, \dots, n_Z$ не превосходят натурального числа N . Применение классического большого решета Э. Бомбьери (см., например, [4, § 23] или [13, гл. 3]) приводит к неравенству

$$\sum_{p \leq X} p \sum_{h=0}^{p-1} \left(Z(p, h) - \frac{Z}{p}\right)^2 \ll (X^2 + N)Z$$

(с явно выписываемыми константами). В работе [6] установлена оценка

$$\sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left(Z(p^2, h) - \frac{Z}{p^2}\right)^2 \leq (X^4 + \pi N)Z. \quad (1.5)$$

Используя результаты Э. Бомбьери и У. Заннье, опубликованные в настоящем номере журнала [3], мы улучшаем (1.5) для некоторых параметров N , Z , X , что позволяет получить неравенство (1.4).

ТЕОРЕМА 2. Пусть $n_1, \dots, n_Z$ – различные натуральные числа, не превосходящие N . Тогда для любого натурального $X \geq 3$ справедливо неравенство

$$\sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left(Z(p^2, h) - \frac{Z}{p^2} \right)^2 \leq C_3 N Z + X^{16/5} Z^{6/5} \exp\left(\frac{C_3 \log X}{\sqrt{\log \log X}}\right),$$

где C_3 – эффективная положительная постоянная.

Теорема 2 содержательна, если X растёт с ростом Z не слишком быстро или медленно. При $X \leq Z^{1/4}$ оценка мажорируется неравенством (1.5).

Докажем новую нижнюю оценку для ES_N .

ТЕОРЕМА 3. Существует эффективная положительная постоянная c_1 такая, что для любого $N \geq 3$ справедливо неравенство

$$ES_N \geq c_1 \log^2 N \log \log N. \quad (1.6)$$

Теорема 3 анонсирована в [11].

Для $N \in \mathbb{N}$ через AP_N обозначим наибольшую мощность арифметической прогрессии, содержащейся в $S_0 \cap \{1, \dots, N\}$.

ТЕОРЕМА 4. Существуют эффективные положительные постоянные c_2 и C_4 такие, что для любого $N \geq 2$ справедливо неравенство

$$c_2 \log^2 N \leq AP_N \leq C_4 \log^2 N. \quad (1.7)$$

Отметим, что из теоремы 4 легко вытекает оценка снизу для ES_N , которая не много слабее (1.6) и отличается от нее на множитель порядка $\log \log N$. В самом деле, в силу теоремы 4 существует арифметическая прогрессия $\mathcal{A} \subset S_0 \cap \{1, \dots, N\}$ такая, что $|\mathcal{A}| \geq c_2 \log^2 N$. Без ограничения общности можно считать, что элементы $\mathcal{A}$ (в совокупности) взаимно просты; в противном случае можно разделить эти элементы на их наибольший общий делитель и получить другую прогрессию с необходимыми нам свойствами. Пусть $\mathcal{A}_1 = \{a \in \mathcal{A}: a \equiv 1 \pmod{2}\}$. Тогда $\mathcal{A}_1$ – также арифметическая прогрессия, причем

$$|\mathcal{A}_1| \geq \max\left(1, \left\lfloor \frac{|\mathcal{A}|}{2} \right\rfloor\right) \geq \frac{|\mathcal{A}|}{3}.$$

Взяв члены прогрессии $\mathcal{A}_1$ через один, мы получим множество $\mathcal{A}_2$ такое, что

$$|\mathcal{A}_2| \geq \frac{|\mathcal{A}_1|}{2} \geq \frac{|\mathcal{A}|}{6} \geq c_2 \frac{\log^2 N}{6}.$$

При этом легко проверить, что $a + a' \in S_0$ для любых $a \in \mathcal{A}_2$, $a' \in \mathcal{A}_2$. Следовательно, $ES_N \geq c_2 \log^2 N / 6$. Отметим, что доказательство теоремы 4 проще доказательства теоремы 3: если первое использует только стандартные идеи решета Бруна, то для доказательства теоремы 3 это решето будет применяться к случайным множествам, и нам потребуются специальные теоретико-вероятностные конструкции.

Всюду далее через $C_1, C_2, \dots$ и $c_1, c_2, \dots$ будем обозначать эффективные положительные постоянные.

Автор благодарен К. Померансу и К. Форду за внимание к работе и полезные замечания.

§2. Большое решето для квадратных модулей

Следующее утверждение доказано в [3].

ЛЕММА 1. Для любого натурального $X \geq 3$ и любых натуральных чисел Δ_{ij} , $1 \leq i < j \leq 4$, количество четверок различных простых чисел p_1, p_2, p_3, p_4 , не превосходящих X , таких, что при всех $1 \leq i < j < k \leq 4$ выполнено равенство $p_i^2 \Delta_{jk} - p_j^2 \Delta_{ik} + p_k^2 \Delta_{ij} = 0$, не превосходит $\exp(C_{20} \log X / \sqrt{\log \log X})$.

Пусть $X \geq 3$ – натуральное число, $Y > 0$. Через $\mathcal{Q}_Y(X)$ обозначим множество восьмерок чисел $(p_1, p_2, p_3, p_4, a_1, a_2, a_3, a_4)$ таких, что простые числа p_1, p_2, p_3, p_4 различны и не превосходят X , $a_i < p_i^2$, $i = 1, 2, 3, 4$, и все числа $\Delta_{ij} = a_j p_i^2 - a_i p_j^2$ положительны и не превосходят Y .

ЛЕММА 2. $|\mathcal{Q}_Y(X)| \leq Y^4 \exp(C_{21} \log X / \sqrt{\log \log X})$.

ДОКАЗАТЕЛЬСТВО. Пусть $1 \leq i < j < k \leq 4$. Поскольку определитель матрицы

$$\begin{pmatrix} p_i^2 & p_j^2 & p_k^2 \\ p_i^2 & p_j^2 & p_k^2 \\ a_i & a_j & a_k \end{pmatrix}$$

равен нулю, то выполнено равенство $p_i^2 \Delta_{jk} - p_j^2 \Delta_{ik} + p_k^2 \Delta_{ij} = 0$. Далее, используя равенство нулю определителя матрицы

$$\begin{pmatrix} p_1^2 & p_2^2 & p_3^2 & p_4^2 \\ a_1 & a_2 & a_3 & a_4 \\ p_1^2 & p_2^2 & p_3^2 & p_4^2 \\ a_1 & a_2 & a_3 & a_4 \end{pmatrix},$$

получаем, что

$$\Delta_{12} \Delta_{34} - \Delta_{13} \Delta_{24} + \Delta_{14} \Delta_{23} = 0. \quad (*)$$

Фиксируем натуральные числа S_1 и S_2 такие, что $S_1 + S_2 \leq Y^2$. Тогда количество наборов $(\Delta_{ij})_{1 \leq i < j \leq 4}$, удовлетворяющих равенству (*) и таких, что $\Delta_{12} \Delta_{34} = S_1$, $\Delta_{14} \Delta_{23} = S_2$, не превосходит $\tau(S_1) \tau(S_2) \tau(S_1 + S_2)$, где $\tau(n)$ – количество делителей числа n . Значит, по лемме 1 числам S_1 и S_2 соответствует не более $\tau(S_1) \tau(S_2) \tau(S_1 + S_2) \exp(C_{20} \log X / \sqrt{\log \log X})$ четверок простых чисел p_1, p_2, p_3, p_4 . Заметим, что для заданных $i < j$, p_i, p_j и Δ_{ij} числа a_i и a_j определены однозначно, т. е. количество восьмерок $(p_1, p_2, p_3, p_4, a_1, a_2, a_3, a_4)$, соответствующих S_1 и S_2 , также не превосходит $\tau(S_1) \tau(S_2) \tau(S_1 + S_2) \exp(C_{20} \log X / \sqrt{\log \log X})$. Следовательно,

$$|\mathcal{Q}_Y(X)| \leq \exp\left(\frac{C_{20} \log X}{\sqrt{\log \log X}}\right) \sum_{S_1 + S_2 \leq Y^2} \tau(S_1) \tau(S_2) \tau(S_1 + S_2).$$

Отсюда и из известной оценки $\tau(S) \ll \exp(\log S / \log \log S)$ при $S \geq 3$ (см., например, [14, с. 32]) мы получаем утверждение леммы.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2. Пусть

$$S(x) = \sum_{j=1}^Z e(n_j x).$$

Хорошо известно, что для любого натурального q имеет место равенство

$$\sum_{a=1}^{q-1} \left| S\left(\frac{a}{q}\right) \right|^2 = q \sum_{h=0}^{q-1} \left(Z(q, h) - \frac{Z}{q} \right)^2. \quad (2.1)$$

Для простых q равенство (2.1) доказано, например, в [4, с. 156], но доказательство переносится без изменений на случай произвольного натурального q (случай $q = p^2$ разобран также в [6]). Суммируя (2.1) по всем $q = p^2$, $p \leq X$, получаем

$$\sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left(Z(p^2, h) - \frac{Z}{p^2} \right)^2 = \sum_{p \leq X} \sum_{a=1}^{p^2-1} \left| S\left(\frac{a}{p^2}\right) \right|^2. \quad (2.2)$$

Упорядочив все числа a/p^2 , $p \leq X$, $1 \leq a < p^2$, по возрастанию: $a_1/p_1^2 < \dots < a_K/p_K^2$, перепишем (2.2) в виде

$$\sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left(Z(p^2, h) - \frac{Z}{p^2} \right)^2 = \sum_{k=1}^K \left| S\left(\frac{a_k}{p_k^2}\right) \right|^2. \quad (2.3)$$

Возьмем произвольное $Y > 0$. Сначала рассмотрим случай $Y < X^2$ (именно этот случай оказывается наиболее содержательным). Пусть

$$\begin{aligned} \mathcal{K}' &= \left\{ k : 4 \leq k \leq K, \frac{a_k}{p_k^2} - \frac{a_{k-3}}{p_{k-3}^2} \leq \frac{Y}{X^2} \right\}, \\ \mathcal{K}_j &= \{ k : 1 \leq k \leq K, k \notin \mathcal{K}', k \equiv j \pmod{3} \}, \quad j = 0, 1, 2. \end{aligned}$$

Равенство (2.3) может быть переписано в виде

$$\sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left(Z(p^2, h) - \frac{Z}{p^2} \right)^2 = S' + \sum_{j=0}^2 S_j, \quad (2.4)$$

где

$$\begin{aligned} S' &= \sum_{k \in \mathcal{K}'} \left| S\left(\frac{a_k}{p_k^2}\right) \right|^2, \\ S_j &= \sum_{k \in \mathcal{K}_j} \left| S\left(\frac{a_k}{p_k^2}\right) \right|^2, \quad j = 0, 1, 2. \end{aligned}$$

Заметим, что если $k \in \mathcal{K}'$, то все простые числа p_{k-i} , $i = 0, 1, 2, 3$, различны. В самом деле, предположим, что $p_{k-i} = p_{k-j}$, $0 \leq i < j \leq 3$. Тогда

$$\frac{a_k}{p_k^2} - \frac{a_{k-3}}{p_{k-3}^2} \geq \frac{a_{k-i}}{p_{k-i}^2} - \frac{a_{k-j}}{p_{k-j}^2} \geq \frac{1}{p_{k-i}^2} \geq \frac{1}{X^2},$$

откуда в силу предположения $Y < X^2$ получаем, что $a_k/p_k^2 - a_{k-3}/p_{k-3}^2 > Y/X^2$, но тогда $k \notin \mathcal{K}'$.

Пусть $k \in \mathcal{K}'$, $0 \leq i < j \leq 3$. Из неравенства

$$0 < \frac{a_{k-i}}{p_{k-i}^2} - \frac{a_{k-j}}{p_{k-j}^2} \leq \frac{a_k}{p_k^2} - \frac{a_{k-3}}{p_{k-3}^2} \leq \frac{Y}{X^4}$$

следует, что $0 < a_{k-i}p_{k-j}^2 - a_{k-j}p_{k-i}^2 \leq Y$. Значит, восьмерка

$$(p_{k-3}, p_{k-2}, p_{k-1}, p_k, a_{k-3}, a_{k-2}, a_{k-1}, a_k)$$

принадлежит множеству $\mathcal{Q}_Y(X)$, и по лемме 2

$$|\mathcal{K}| \leq Y^4 \exp\left(\frac{C_{21} \log X}{\sqrt{\log \log X}}\right).$$

Используя для $k \in \mathcal{K}$ тривиальную оценку $|S(a_k/p_k^2)| \leq Z$, получаем

$$S' \leq Y^4 Z^2 \exp\left(\frac{C_{21} \log X}{\sqrt{\log \log X}}\right). \quad (2.5)$$

Заметим теперь, что если $k < l$ и $k, l \in \mathcal{K}_j$ для некоторого $j = 0, 1, 2$, то $a_l/p_l^2 - a_k/p_k^2 > Y/X^4$. Кроме того, $a_k/p_k^2 \geq 1/X^2 > Y/X^4$ (здесь мы вновь воспользовались предположением $Y < X^2$). Отсюда, применяя следствие 2.2 из [13, с. 21], получаем

$$S_j \leq \left(\frac{X^4}{Y} + \pi N\right) Z, \quad j = 0, 1, 2. \quad (2.6)$$

Из соотношений (2.4)–(2.6) следует, что при $Y < X^2$

$$\sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left(Z(p^2, h) - \frac{Z}{p^2}\right)^2 \leq 3\pi N Z + \frac{3X^4}{YZ} + Y^4 Z^2 \exp\left(\frac{C_{21} \log X}{\sqrt{\log \log X}}\right). \quad (2.7)$$

Неравенство (2.7) справедливо и при $Y \geq X^2$ вследствие тривиальной оценки

$$\sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left(Z(p^2, h) - \frac{Z}{p^2}\right)^2 \leq \sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} Z^2 \leq \sum_{p \leq X} p^4 Z^2 \leq X^5 Z^2.$$

Взяв $Y = (X^4/Z)^{1/5}$, мы получаем из (2.7) утверждение теоремы при подходящем C_3 .

§ 3. Полтора доказательства теоремы 1

ЛЕММА 3. Пусть $X \geq 3$ – натуральное число,

$$Y = X^{1/4} \exp\left(-\frac{C_{30} \log X}{\sqrt{\log \log X}}\right).$$

Тогда существует множество $\mathcal{P}$ простых чисел, не превосходящих X , такое, что $|\mathcal{P}| \geq \pi(X)/2$ и для любых четверок p_1, p_2, p_3, p_4 из $\mathcal{P}$ и четверок натуральных чисел a_1, a_2, a_3, a_4 таких, что $a_i < p_i^2$, $i = 1, 2, 3, 4$, и $a_1/p_1^2 < a_2/p_2^2 < a_3/p_3^2 < a_4/p_4^2$, выполнено неравенство

$$\frac{a_4}{p_4^2} - \frac{a_1}{p_1^2} > \frac{Y}{X^2}.$$

ДОКАЗАТЕЛЬСТВО. По лемме 2

$$|Q_Y(X)| \leq X \exp\left((C_{21} - 4C_{30}) \frac{\log X}{\sqrt{\log \log X}}\right),$$

и за счет выбора C_{30} можно добиться выполнения для всех $X \geq 3$ неравенства $|Q_Y(X)| \leq \pi(X)/2$. Взяв в качестве $\mathcal{P}$ множество всех простых чисел, не превосходящих X и не являющихся первым элементом ни одной восьмерки из $Q_Y(X)$, имеем

$$|\mathcal{P}| \geq \pi(X) - 4|Q_Y(X)| \geq \frac{\pi(X)}{2}.$$

Рассмотрим произвольные четверки p_1, p_2, p_3, p_4 и a_1, a_2, a_3, a_4 , удовлетворяющие условиям леммы. Если из чисел p_1, p_2, p_3, p_4 какие-либо два p_i и p_j , $i < j$, совпадают, то

$$\frac{a_4}{p_4^2} - \frac{a_1}{p_1^2} > \frac{a_j}{p_j^2} - \frac{a_i}{p_i^2} \geq \frac{1}{p_i^2} \geq \frac{1}{X^2},$$

и утверждение леммы выполнено.

Пусть теперь все числа p_1, p_2, p_3, p_4 различны. Если все числа $\Delta_{ij} = a_j p_i^2 - a_i p_j^2$, $1 \leq i < j \leq 4$, не превосходят Y , то $(p_1, p_2, p_3, p_4, a_1, a_2, a_3, a_4) \in Q_Y(X)$, что противоречит выбору $\mathcal{P}$. Значит, для некоторых i и j имеет место неравенство $\Delta_{ij} > Y$. Следовательно,

$$\frac{a_4}{p_4^2} - \frac{a_1}{p_1^2} > \frac{a_j}{p_j^2} - \frac{a_i}{p_i^2} = \frac{\Delta_{ij}}{p_i^2 p_j^2} > \frac{Y}{X^4}.$$

Лемма доказана.

Доказательство теоремы 1 проводится повторением рассуждений из работы [1]. Вначале определим функцию

$$F(x) = \sum_{n=1}^N e(nx)$$

и заметим, что для любого натурального q справедливо соотношение

$$F_q(x) := \sum_{a=1}^q F\left(x - \frac{a}{q}\right) = \sum_{n=1}^N e(nx) \sum_{a=1}^q e\left(\frac{-an}{q}\right) = q \sum_{\substack{1 \leq n \leq N \\ q|n}} e(nx).$$

Положим $X = \max(3, [N^{4/15}])$, возьмем Y и $\mathcal{P}$ в соответствии с леммой 3 и определим функцию

$$G(x) = \frac{1}{|\mathcal{P}|} \sum_{p \in \mathcal{P}} F_{p^2}(x) = \sum_{n=1}^N d_n e(nx).$$

Отметим, что $d_n = 0$, если n свободно от квадратов.

ЛЕММА 4. *Неравенство*

$$G(x) - F(x) \leq N^{11/15} \exp\left(\frac{C_1 \log N}{\sqrt{\log \log N}}\right)$$

выполнено равномерно по x .

ДОКАЗАТЕЛЬСТВО. Хорошо известно, что

$$|F(x)| \leq \min\left(N, \frac{1}{\|x\|^{-1}}\right),$$

где $\|x\|$ – расстояние от числа x до ближайшего целого (см., например, [12, с. 12]). Следовательно,

$$G(x) - F(x) = \frac{1}{|\mathcal{P}|} \sum_{p \in \mathcal{P}} \sum_{a=1}^{p^2-1} F\left(x - \frac{a}{p^2}\right) \leq \frac{1}{|\mathcal{P}|} \sum_{p \in \mathcal{P}} \sum_{a=1}^{p^2-1} \min\left(N, \left\|x - \frac{a}{p^2}\right\|^{-1}\right).$$

Отсюда и из неравенства $|\mathcal{P}| \geq \pi(X)/2 \gg N^{4/15}/\log N$ вытекает, что

$$G(x) - F(x) \ll N^{-4/15} \log N \sum_{p \in \mathcal{P}} \sum_{a=1}^{p^2-1} \min\left(N, \left\|x - \frac{a}{p^2}\right\|^{-1}\right). \quad (3.1)$$

Фиксируем x . Для трех дробей, ближайших к x , оценим минимум через N . Остальные можно упорядочить так, что для k -й дроби a/p^2 справедливо неравенство $\|x - a/p^2\| \geq kY/(6X^4)$. Последнее вытекает из того, что по лемме 3 для любого натурального l количество дробей a/p^2 , удовлетворяющих неравенству $\|x - a/p^2\| < lY/(2X^4)$, не превосходит $3l$. Таким образом, мы получаем из (3.1) оценку

$$G(x) - F(x) \ll N^{-4/15} \log N \left(N + \sum_{k \leq X^3} \frac{X^4}{kY}\right),$$

откуда вытекает утверждение леммы при подходящем выборе C_1 .

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1. Рассмотрим произвольный тригонометрический полином

$$M(x) = \sum_{\substack{1 \leq n \leq N \\ n \in \mathcal{S}_0}} a_n e(nx).$$

Для любого фиксированного x имеем

$$\begin{aligned} \int_0^1 G(x-y)M(y) dy &= \sum_{1 \leq n \leq N} \sum_{1 \leq m \leq N} d_n a_m e(nx) \int_0^1 e((m-n)y) dy \\ &= \sum_{1 \leq n \leq N} d_n a_n e(nx) = 0. \end{aligned}$$

Аналогично,

$$\begin{aligned} \int_0^1 F(x-y)M(y) dy &= \sum_{1 \leq n \leq N} \sum_{1 \leq m \leq N} a_m e(nx) \int_0^1 e((m-n)y) dy \\ &= \sum_{1 \leq n \leq N} a_n e(nx) = M(x). \end{aligned}$$

Следовательно,

$$M(x) = \int_0^1 (F(x-y) - G(x-y))M(y) dy,$$

и, пользуясь леммой 4, мы получаем

$$\begin{aligned} |M(x)| &\leq \int_0^1 |G(x-y) - F(x-y)| |M(y)| dy \\ &\leq N^{11/15} \exp\left(\frac{C \log N}{\sqrt{\log \log N}}\right) \int_0^1 |M(y)| dy. \end{aligned}$$

Тем самым оценка (1.3) доказана. Неравенство (1.4) вытекает из (1.3) и предложения 1.

Следуя [6], приведем другое доказательство неравенства (1.4), основанное на использовании метода большого решета. Пусть $n_1, \dots, n_Z$ — различные натуральные числа, не превосходящие N , и все числа $n_i + n_j$ свободны от квадратов. Тогда для любого p имеется более $p^2/2$ вычетов по модулю p^2 , свободных от чисел $n_1, \dots, n_Z$. Следовательно,

$$\sum_{h=0}^{p^2-1} \left(Z(p^2, h) - \frac{Z}{p^2} \right)^2 > \frac{p^2}{2} \left(\frac{Z}{p^2} \right)^2 = \frac{Z^2}{2p^2},$$

и, значит, для любого натурального $X \geq 3$

$$\sum_{p \leq X} p^2 \sum_{h=0}^{p^2-1} \left(Z(p^2, h) - \frac{Z}{p^2} \right)^2 > \frac{Z^2 \pi(X)}{2}.$$

Сравнивая последнее неравенство с оценкой теоремы 2, получаем

$$\frac{Z^2 \pi(X)}{2} < C_3 N Z + X^{16/5} Z^{6/5} \exp\left(\frac{C_3 \log X}{\sqrt{\log \log X}}\right). \quad (3.2)$$

Положим X равным минимальному числу, удовлетворяющему неравенствам $X \geq 3$, $\pi(X) \geq 4C_3 N/Z$. Тогда для некоторого C_{31} выполнены неравенства

$$X \leq \frac{C_{31} N \log N}{Z}, \quad \exp\left(\frac{C_3 \log X}{\sqrt{\log \log X}}\right) \leq \exp\left(\frac{C_{31} \log N}{\sqrt{\log \log N}}\right). \quad (3.3)$$

Далее, по определению X имеем $Z^2 \pi(X)/2 \geq 2C_3 N Z$, и мы получаем из (3.2), что

$$\frac{Z^2 \pi(X)}{2} < 2X^{16/5} Z^{6/5} \exp\left(\frac{C_3 \log X}{\sqrt{\log \log X}}\right),$$

или, с учетом (3.3),

$$Z^{4/5} < \frac{(C_{31} N \log N/Z)^{16/5}}{C_3 N/Z} \exp\left(\frac{C_{31} \log N}{\sqrt{\log \log N}}\right).$$

Из последнего неравенства после несложных преобразований получается требуемая оценка

$$Z \leq N^{11/15} \exp\left(\frac{C \log N}{\sqrt{\log \log N}}\right),$$

и неравенство (1.4) доказано.

§ 4. Решето Бруна с квадратными модулями

Пусть $\mathcal{P}$ – некоторое подмножество множества простых чисел. Каждому простому числу $p \in \mathcal{P}$ сопоставим множество B_p вычетов по модулю p^2 , и пусть $|B_p| = \rho(p) < p^2$. Обозначим

$$\mathcal{B} = \{B_p : p \in \mathcal{P}\}, \quad \gamma = \gamma(\mathcal{B}) = \prod_{p \in \mathcal{P}} \left(1 - \frac{\rho(p)}{p^2}\right),$$

и положим для конечного множества $D \subset \mathbb{N}$

$$R(D, \mathcal{B}) = \{n \in D : \forall p \in \mathcal{P}, \forall b \in B_p \ n \not\equiv b \pmod{p^2}\}.$$

Для $D = \{1, \dots, N\}$ обозначим $R(N, \mathcal{B}) = R(D, \mathcal{B})$. Пусть $P(z)$ – произведение всех простых чисел, меньших некоторого натурального числа z . Пусть $\mu(d)$ – функция Мёбиуса. Для $d \in \mathbb{N}$ и $l \in \mathbb{Z}$ обозначим $B_{d,l}(D) = \{n \in D : n \equiv l \pmod{d^2}\}$.

ЛЕММА 5. Пусть $\varepsilon > 0$, числа $\alpha_1 > 0$ и $\delta_1 > 0$ удовлетворяют условию

$$\left(\frac{2\delta_1}{\alpha_1}\right)^{\alpha_1} e^{\delta_1} < 1, \quad (4.1)$$

натуральные числа $N \geq N(\varepsilon)$, ρ и $z_1 \geq z_1(\varepsilon) \geq 2$ – условиям

$$\rho \leq \frac{z_1^2}{2}, \quad \frac{\rho}{z_1 \log z_1} \leq \frac{\delta_1}{2} \frac{\log N}{\log \log N}, \quad (4.2)$$

натуральное число $z_2 > z_1$ и число $\alpha_2 > 0$ – условию

$$\frac{\alpha_1 \log z_2}{\log \log N} < \alpha_2. \quad (4.3)$$

Пусть $|B(p)| = \rho(p) \leq \rho$ для каждого простого $p \in \mathcal{P} = \{p \in [z_1, z_2]\}$. Пусть множество $D \subset \{1, \dots, N\}$ и числа $\delta_2 > 0$, $\delta_3 \geq 0$ удовлетворяют условиям

$$|D| > N^{1-\delta_2}, \quad (4.4)$$

$$\forall d, \forall l (d \leq N^{\alpha_2}, d|P(z_2), (d, P(z_1)) = 1) \rightarrow \left| |B_{d,l}(D)| - \frac{|D|}{d^2} \right| \leq N^{\delta_3}, \quad (4.5)$$

$$\frac{\log(z_1^2 z_2)}{\log \log N} \alpha_1 + \delta_2 + \delta_3 < 1 - \varepsilon. \quad (4.6)$$

Тогда

$$|R(D, \mathcal{B})| \sim \gamma |D|, \quad N \rightarrow \infty. \quad (4.7)$$

ДОКАЗАТЕЛЬСТВО. Пусть $z_1 \leq p_1 < \dots < p_k < z_2$. Обозначим

$$\gamma_k = \sum_{p_1, \dots, p_k} \prod_{j=1}^k \frac{\rho(p_j)}{p_j^2}.$$

При этом мы полагаем $\gamma_0 = 1$. Возьмем произвольное множество $D' \subset \mathbb{Z}$. Обозначим

$$\Gamma_k(D') = \sum_{p_1, \dots, p_k} \sum_{\substack{b_j \in B_{p_j} \\ 1 \leq j \leq k}} |\{n \in D' : n \equiv b_j \pmod{p_j^2}\}|,$$

полагая $\Gamma_0(D') = |D'|$. Из простейшего варианта метода Бруна (см. [10, с. 14]) имеем

$$(-1)^K \left(|R(D, \mathcal{B})| - \sum_{k=0}^K (-1)^k \Gamma_k(D') \right) \leq 0,$$

откуда

$$\left| |R(D', \mathcal{B})| - \sum_{k=0}^{K-1} (-1)^k \Gamma_k(D') \right| \leq \Gamma_K(D'). \quad (4.8)$$

Возьмем $D' = \{1, \dots, P(z_2)\}$. Тогда легко видеть, что $|R(D', \mathcal{B})| = \gamma |D'|$, $\Gamma_k(D') = \gamma_k |D'|$, поэтому неравенство (4.8) принимает вид

$$\left| \gamma - \sum_{k=0}^{K-1} (-1)^k \gamma_k \right| \leq \gamma_K. \quad (4.9)$$

Оценим γ_K . Имеем

$$\gamma_K \leq \frac{1}{K!} \sum_{z_1 \leq p_1 < z_2} \cdots \sum_{z_1 \leq p_K < z_2} \prod_{j=1}^K \frac{\rho(p_j)}{p_j^2} = \frac{1}{K!} \left(\sum_{z_1 \leq p < z_2} \frac{\rho(p)}{p^2} \right)^K. \quad (4.10)$$

Мы будем пользоваться известным неравенством

$$\frac{1}{K!} < \left(\frac{e}{K} \right)^K \quad (4.11)$$

(см., например, [7, с. 371]). Далее,

$$\sum_{z_1 \leq p < z_2} \frac{\rho(p)}{p^2} \leq \rho \sum_{p \geq z_1} \frac{1}{p^2}.$$

Используя асимптотический закон распределения простых чисел и преобразование Абеля, получаем

$$\sum_{p \geq z} \frac{1}{p^2} \sim \frac{1}{z \log z}, \quad z \rightarrow \infty. \quad (4.12)$$

Отсюда и из условий (4.2) для достаточно большого z_1 вытекает неравенство

$$\sum_{z_1 \leq p < z_2} \frac{\rho(p)}{p^2} \leq 0.6\delta_1 \frac{\log N}{\log \log N}. \quad (4.13)$$

Подставляя неравенства (4.11) и (4.13) в (4.10), получаем

$$\gamma_K \leq \left(\frac{1.7\delta_1 \log N}{K \log \log N} \right)^K. \quad (4.14)$$

Будем предполагать, что K удовлетворяет условию

$$z_2^K \leq N^{\alpha_2}. \quad (4.15)$$

В силу неравенств (4.15), (4.5) и (4.2) для всех $k \leq K$ справедлива оценка

$$|\Gamma_k(D') - \gamma_k|D'| \leq \sum_{z_1 \leq p_1 < \cdots < p_k < z_2} \sum_{\substack{b_j \in B_{p_j} \\ 1 \leq j \leq k}} N^{\delta_3} \leq \frac{(\rho\pi(z_2))^k}{k!} N^{\delta_3} \leq \frac{(z_1^2 z_2)^k}{2^k k!} N^{\delta_3}. \quad (4.16)$$

Записывая неравенство (4.8) для $D' = D$ и используя (4.16), получаем

$$\left| |R(D, \mathcal{B})| - \sum_{k=0}^{K-1} (-1)^k \Gamma_k(D) \right| \leq \gamma_K |D| + N^{\delta_3} (z_1^2 z_2)^K.$$

Осюда и из (4.14) следует, что

$$||R(D, \mathcal{B})| - \gamma|D|| \leq 2 \left(\frac{1.7\delta_1 \log N}{K \log \log N} \right)^K |D| + N^{\delta_3} (z_1^2 z_2)^K. \quad (4.17)$$

Оценим снизу γ . Воспользовавшись неравенством

$$-\log(1-u) \leq 1.5u, \quad 0 \leq u \leq 0.5,$$

и учитывая (4.2) и (4.13), получаем

$$-\log \gamma \leq 1.5 \sum_{z_1 \leq p < z_2} \frac{\rho(p)}{p^2} \leq 0.9\delta_1 \frac{\log N}{\log \log N}. \quad (4.18)$$

Возьмем $K = [\alpha_1 \log N / \log \log N]$; тогда в силу (4.3) требование (4.15) выполнено. При $N \rightarrow \infty$ имеем

$$\left(\frac{1.7\delta_1 \log N}{K \log \log N} \right)^K \leq \left(\frac{1.7\delta_1}{\alpha_1} + o(1) \right)^{\alpha_1 \log N / \log \log N}.$$

Из последнего неравенства, (4.1) и (4.18) следует, что

$$\left(\frac{1.7\delta_1 \log N}{K \log \log N} \right)^K = o(\gamma), \quad N \rightarrow \infty. \quad (4.19)$$

При $N \rightarrow \infty$ в силу (4.6) и определения K

$$N^{\delta_3} (z_1^2 z_2)^K \leq N^{1-\varepsilon-\delta_2+o(1)}.$$

С другой стороны, из неравенств (4.4) и (4.18) следует, что

$$\gamma|D| \geq N^{1-\delta_2+o(1)}.$$

Значит,

$$N^{\delta_3} (z_1^2 z_2)^K \leq N^{1-\varepsilon-\delta_2+o(1)} = o(\gamma|D|), \quad N \rightarrow \infty. \quad (4.20)$$

Утверждение леммы вытекает из (4.17), (4.19) и (4.20).

ЛЕММА 6. Пусть положительные числа ε , α_1 , α_2 , δ_1 , натуральные числа $N \geq N(\varepsilon)$, ρ , $z_1 \geq z_1(\varepsilon) \geq 2$, z_2 удовлетворяют условиям (4.1)–(4.3), а также условию

$$z_2 \geq \max(\rho, \log N). \quad (4.21)$$

Пусть $\alpha_3 > 0$, $z_3 > z_2$ – натуральное число, удовлетворяющее условию

$$z_3 \leq \frac{N^{\alpha_3}}{2}. \quad (4.22)$$

Пусть $|B(p)| = \rho(p) \leq \rho$ для каждого простого $p \in \mathcal{P} = \{p \in [z_1, z_3]\}$,

$$\gamma_0 = \prod_{z_1 \leq p < z_2} \left(1 - \frac{\rho(p)}{p^2}\right),$$

и пусть множество $D \subset \{1, \dots, N\}$ и числа $\delta_2 > 0$, $\delta_3 \geq 0$ удовлетворяют условиям (4.4),

$$\forall d, \forall l \left(d \leq N^{\alpha_2 + \alpha_3}, d|P(z_3), (d, P(z_1)) = 1 \right) \rightarrow \left| |B_{d,l}(D)| - \frac{|D|}{d^2} \right| \leq N^{\delta_3}, \quad (4.23)$$

$$\frac{\log(z_1^2 z_2)}{\log \log N} \alpha_1 + 2\alpha_3 + \delta_2 + \delta_3 < 1 - \varepsilon. \quad (4.24)$$

Тогда

$$|R(D, \mathcal{B})| \sim \gamma_0 |D|, \quad N \rightarrow \infty. \quad (4.25)$$

ДОКАЗАТЕЛЬСТВО. Положим $\mathcal{P}_0 = \{p \in [z_1, z_2]\}$, $\mathcal{B}_0 = \{B_p : p \in \mathcal{P}_0\}$. Из леммы 5 следует, что

$$|R(D, \mathcal{B}_0)| \sim \gamma_0 |D|, \quad N \rightarrow \infty. \quad (4.26)$$

Наша цель – показать, что множество $R(D, \mathcal{B})$ мало отличается от множества $R(D, \mathcal{B}_0)$. Имеем

$$0 \leq |R(D, \mathcal{B}_0)| - |R(D, \mathcal{B})| \leq \sum_{z_2 \leq p < z_3} \sum_{b \in B_p} |R(D, \mathcal{B}_0) \cap B_{p,b}|. \quad (4.27)$$

В силу предположения (4.23) при $N \rightarrow \infty$ и условия $z_2 \leq p < z_3$

$$|D \cap B_{p,b}| \sim \frac{|D|}{p^2}, \quad (4.28)$$

и, значит, для достаточно большого N справедливо неравенство $|D \cap B_{p,b}| \geq |D|/(2p^2)$. Пользуясь (4.4) и (4.22), получаем $|D \cap B_{p,b}| \geq N^{1-\delta_2-2\alpha_3}$. Условия (4.23) и (4.24) показывают, что ко множествам $D \cap B_{p,b}$ применима лемма 5 с заменой δ_2 на $\delta_2 + 2\alpha_3$. Значит, при $N \rightarrow \infty$

$$|R(D, \mathcal{B}_0) \cap B_{p,b}| \sim \gamma_0 |D \cap B_{p,b}|,$$

и вследствие (4.28)

$$|R(D, \mathcal{B}_0) \cap B_{p,b}| \sim \gamma_0 \frac{|D|}{p^2}.$$

Далее,

$$\begin{aligned} \sum_{z_2 \leq p < z_3} \sum_{b \in B_p} |R(D, \mathcal{B}_0) \cap B_{p,b}| &\leq (1 + o(1)) \gamma_0 |D| \sum_{z_2 \leq p < z_3} \sum_{b \in B_p} \frac{1}{p^2} \\ &= (1 + o(1)) \gamma_0 |D| \sum_{z_2 \leq p < z_3} \frac{\rho(p)}{p^2} \leq (1 + o(1)) \gamma_0 |D| \rho \sum_{p \geq z_2} \frac{1}{p^2}. \end{aligned} \quad (4.29)$$

Из условия (4.21) и соотношения (4.12) следует, что

$$\rho \sum_{p \geq z_2} \frac{1}{p^2} \ll \frac{z_2}{z_2 \log z_2} = o(1), \quad N \rightarrow \infty.$$

Подставляя последнюю оценку в (4.29), получаем

$$\sum_{z_2 \leq p < z_3} \sum_{b \in B_p} |R(D, \mathcal{B}_0) \cap B_{p,b}| = o(\gamma_0 |D|), \quad N \rightarrow \infty.$$

Отсюда и из неравенств (4.26), (4.27) вытекает утверждение леммы 6.

ЛЕММА 7. Пусть выполнены все условия леммы 6, кроме определения множества $\mathcal{P}$. Пусть теперь $\mathcal{P} = \{p \in [z_1, \sqrt{N}]\}$ и, кроме того, выполнены условия

$$z_1^2 \leq z_3 N^{-\delta_2 - \varepsilon}, \quad (4.30)$$

$$z_1^2 \sqrt{N} \leq N^{1 - \delta_2 - \varepsilon}. \quad (4.31)$$

Тогда выполнено асимптотическое равенство (4.25).

ДОКАЗАТЕЛЬСТВО. Положим $\mathcal{P}_1 = \{p \in [z_1, z_3]\}$, $\mathcal{B}_1 = \{B_p : p \in \mathcal{P}_1\}$. Из леммы 6 следует, что

$$|R(D, \mathcal{B}_1)| \sim \gamma_0 |D|, \quad N \rightarrow \infty. \quad (4.32)$$

Наша цель – показать, что множество $R(D, \mathcal{B})$ мало отличается от множества $R(D, \mathcal{B}_1)$. Учитывая (4.2), имеем

$$\begin{aligned} 0 \leq |R(D, \mathcal{B}_1)| - |R(D, \mathcal{B})| &\leq \sum_{z_3 \leq p \leq \sqrt{N}} \sum_{b \in B_p} |B_{p,b}| \\ &\leq \sum_{z_3 \leq p \leq \sqrt{N}} \rho(p) \left(1 + \frac{N}{p^2}\right) \leq z_1^2 N \sum_{p \geq z_3} \frac{1}{p^2} + z_1^2 \sqrt{N}. \end{aligned}$$

В силу (4.12) и (4.30) для достаточно большого N

$$z_1^2 N \sum_{p \geq z_3} \frac{1}{p^2} \leq N^{1 - \delta_2 - \varepsilon}.$$

Отсюда и из предположения (4.31) вытекает, что

$$0 \leq |R(D, \mathcal{B}_1)| - |R(D, \mathcal{B})| \ll N^{1-\delta_2-\varepsilon}. \quad (4.33)$$

С другой стороны, в силу неравенства (4.18), в обозначениях леммы 7, $\gamma_0 \gg N^{-\varepsilon/2}$. Отсюда и из (4.4) получаем

$$\gamma_0 |D| \gg N^{1-\delta_2-\varepsilon/2}. \quad (4.34)$$

Требуемое неравенство (4.25) немедленно следует из (4.32)–(4.34), и лемма 7 доказана.

§5. Доказательство теоремы 4

Оценка сверху. В силу асимптотического закона распределения простых чисел, при $z \geq C_{51} \log N$ справедливо неравенство $P(z) > N$ (напомним, что $P(z)$ – произведение всех простых чисел, меньших z). Значит, для любого натурального $d \leq N$ найдется такое простое p , что

$$p < C_{51} \log N, \quad d \not\equiv 0 \pmod{p}. \quad (5.1)$$

Пусть $\mathcal{A} \subset \mathcal{S}_0 \cap \{1, \dots, N\}$ – арифметическая прогрессия, d – ее разность. Возьмем p , удовлетворяющее условиям (5.1). Тогда если $|\mathcal{A}| \geq p^2$, то элементы $\mathcal{A}$ представляют полную систему вычетов по модулю p^2 и, в частности, $\mathcal{A}$ содержит элемент, делящийся на p^2 , что противоречит предположению $\mathcal{A} \subset \mathcal{S}_0$. Значит, $|\mathcal{A}| < p^2 < C_{51}^2 \log^2 N$, и оценка сверху доказана для $C_4 = C_{51}^2$.

Оценка снизу. Не ограничивая общности, можно полагать, что N достаточно велико. Идея доказательства оценки снизу состоит в том, чтобы для подходящего малого, но фиксированного $\delta > 0$ и для

$$z_1 = \left\lceil \frac{\delta \log N}{2} \right\rceil, \quad d = P(z_1), \quad \rho = \left\lceil \frac{z_1^2}{2} \right\rceil \quad (5.2)$$

показать, что при некотором целом n все члены прогрессии $\{(n+j)d+1 : 0 \leq j < \rho\}$ содержатся в $\mathcal{S}_0 \cap \{1, \dots, N\}$.

Положим $\alpha_1 = 1/5$, $\alpha_2 = 1/4$, $\alpha_3 = 1/20$ и $\delta_1 = \delta_2 = \delta_3 = \varepsilon = \delta > 0$, причем δ выберем настолько малым, чтобы выполнялись неравенства (4.1) и

$$4\alpha_1 + 2\alpha_3 + 3\delta < 1. \quad (5.3)$$

Заметим, что неравенство (5.3) можно переписать в виде

$$\delta < \frac{1}{30}. \quad (5.4)$$

Положим также

$$z_2 = \lceil \log^2 N \rceil, \quad z_3 = \left\lceil \frac{N^{\alpha_3}}{2} \right\rceil. \quad (5.5)$$

В силу (5.2) первое неравенство (4.2) выполняется, а второе вытекает из асимптотической формулы

$$\frac{\rho}{z_1 \log z_1} \sim \frac{\delta_1}{4} \frac{\log N}{\log \log N}, \quad N \rightarrow \infty.$$

Неравенство (4.3) также выполнено, поскольку $\log z_2 / \log \log N \leq 2$ вследствие (5.5). Далее, $z_1^2 z_2 < \log^4 N$, т. е.

$$\frac{\log(z_1^2 z_2)}{\log \log N} < 4.$$

Отсюда и из неравенства (5.3) получаем справедливость (4.24). Легко видеть, что условия (4.21) и (4.22) также выполнены. Учитывая (5.4), мы получаем справедливость условий (4.30) и (4.31).

Положим $D = \{1, \dots, [N/(2d)]\}$. В силу асимптотического закона распределения простых чисел и (5.2) имеем при $N \rightarrow \infty$

$$\log d \sim z_1 \sim \frac{\delta \log N}{2}, \quad (5.6)$$

что влечет справедливость неравенства (4.4). Наконец, условие (4.5) выполнено, поскольку всегда

$$\left| B_{d,l}(D) - \frac{|D|}{d^2} \right| \leq 1.$$

Для каждого $p \geq z_1$ через B_p обозначим множество вычетов a по модулю p^2 таких, что для некоторого j , $0 \leq j < \rho$, имеем $(a+j)d+1 \equiv 0 \pmod{p^2}$. Ясно, что $|B(p)| \leq \rho$ для каждого простого p . Поэтому можно воспользоваться леммой 4.7, утверждающей выполнение асимптотического равенства (4.25), в силу которого $|R(D, \mathcal{B})| > 0$ при достаточно большом N (мы учли, что $\gamma_0 > 0$ в силу (4.2)).

Итак, пусть $n \in R(D, \mathcal{B})$. Тогда для $j < \rho$ в силу (5.6)

$$(n+j)d+1 < nd+\rho d \leq \frac{N}{2} + (\log^2 N)d < N. \quad (5.7)$$

Следовательно,

$$\{(n+j)d+1: 0 \leq j < \rho\} \subset \{1, \dots, N\}.$$

Далее, по определению множеств B_p условие $n \in R(D, \mathcal{B})$ влечет, что числа $(n+j)d+1$, $0 \leq j < \rho$, не делятся на p^2 при $z_1 \leq p \leq \sqrt{N}$. Поскольку $d = P(z_1)$, то они не делятся на p^2 и при $p < z_1$. Учитывая (5.7), мы видим, что все они свободны от квадратов. Следовательно, арифметическая прогрессия $\{(n+j)d+1: 0 \leq j < \rho\}$ действительно содержится в $\mathcal{S}_0 \cap \{1, \dots, N\}$. Замечая, что ее длина $\rho > \delta^2 \log^2 N/9$ при достаточно большом N , мы завершаем доказательство теоремы.

§ 6. Сбалансированное просеивание

Будем пользоваться обозначениями, введенными в § 4. Следующая лемма идейно близка к лемме 5.

ЛЕММА 8. *Существует такая функция $\Theta(N)$, что выполнены условия:*

$$\Theta(N) \ll N^\varepsilon \quad \forall \varepsilon > 0; \quad (6.1)$$

для любых $N \geq 3$ и $z \leq \log N \log \log N$, $\mathcal{P} = \{p: p < z\}$, для любых $\mathcal{B}$ таких, что $\rho(p) \leq 1$ для всех $p > 2$, и для любых натуральных $M \leq N$ имеет место неравенство

$$||R(M, \mathcal{B})| - \gamma M| \leq \Theta(N). \quad (6.2)$$

ДОКАЗАТЕЛЬСТВО. Очевидно, интерес представляет лишь случай $z > 2$. Положим $z_1 = 2$, $z_2 = z$,

$$K = \left\lceil \frac{\log N}{(\log \log N)^{1/2}} \right\rceil.$$

Так же, как при доказательстве леммы 5, мы применяем решето Бруна для $D = \{1, \dots, M\}$. Заметим, что

$$\sum_{z_1 \leq p < z_2} \frac{\rho(p)}{p^2} \leq \frac{3}{4} + \sum_{p > 2} \frac{1}{p^2} < \frac{3}{4} + \sum_{j \geq 1} \frac{1}{(2j+1)^2} < \frac{3}{4} + \sum_{j \geq 1} \frac{1}{4j(j+1)} = 1.$$

Поэтому в силу неравенств (4.9) и (4.10) имеем

$$\gamma_K \leq \left(\frac{e}{K} \right)^K = o(N^{-1}), \quad N \rightarrow \infty. \quad (6.3)$$

Заметим, что для любых $p_1 < \dots < p_K$, $b_j \in B_{p_j}$

$$\left| |\{n \in D: n \equiv b_j \pmod{p_j^2}\}| - M \prod_{j=1}^K \frac{1}{p_j^2} \right| \leq 1,$$

откуда, вновь учитывая, что $\rho(2) \leq 3$, $\rho(p) \leq 1$ при $p > 2$, и используя (4.10), аналогично (4.16) получаем для всех $k \leq K$

$$\begin{aligned} |\Gamma_k(D) - \gamma_k|D|| &\leq \sum_{p_1 < \dots < p_k < z} 3 \leq 3 \frac{(\rho\pi(z))^k}{k!} \\ &\leq 3 \frac{(C_{61} \log N)^k}{k!} \leq 3 \left(\frac{C_{61} e \log N}{k} \right)^k. \end{aligned} \quad (6.4)$$

При достаточно большом N правая часть последнего неравенства из (6.4) возрастает по k при $k \leq K$, поэтому

$$|\Gamma_k(D) - \gamma_k|D|| \leq 3 \left(\frac{C_{61} e \log N}{K} \right)^K \leq (C_{62} (\log \log N)^{1/2})^K = O(N^{\varepsilon/2}).$$

Отсюда и из неравенств (4.8) для $D' = D$, (4.9) и (6.3) вытекает утверждение леммы.

Через $\omega(d)$ обозначаем количество различных простых делителей натурального числа d .

ЛЕММА 9. Пусть $N \geq 3$ и $z \leq \log N \log \log N$, $E = \{d \leq N : d|P(z)\}$. Тогда для любого $\varepsilon > 0$ справедливо неравенство

$$|E| = O(N^\varepsilon).$$

Лемма легко следует из [5], но для полноты изложения мы приведем ее доказательство.

ДОКАЗАТЕЛЬСТВО. Из условия $d \leq N$ следует, что

$$\omega(d) \leq K = \left\lceil \frac{C_{63} \log N}{\log \log N} \right\rceil,$$

а из ограничений на z и теоремы о простых числах вытекает неравенство $\pi(z) \leq L = [C_{64} \log N]$. Следовательно,

$$|E| \leq \sum_{k=0}^K \binom{L}{k}.$$

Поскольку при достаточно большом N выполнено неравенство $K < L/2$, то $\binom{L}{k}$ возрастает по k при $k \leq K$, откуда имеем

$$|E| \leq (K+1) \binom{L}{K}. \quad (6.5)$$

В силу неравенства (4.11) получаем

$$\binom{L}{K} \leq \left(\frac{eL}{K} \right)^K.$$

Осюда и из неравенства (6.5) вытекает утверждение леммы.

Выберем теперь $z_1 \sim \delta_4 \log N \log \log N$, $\delta_4 \in (0, 1)$. Пусть

$$\begin{aligned} \mathcal{P}_1 &= \{p : 2 < p < z_1\}, \\ S_1 &= \{n \leq N : n \equiv 1 \pmod{4}, \forall p \in \mathcal{P}_1 \ n \not\equiv 0 \pmod{p^2}\}, \\ \gamma_1 &= \frac{1}{4} \prod_{p \in \mathcal{P}_1} \left(1 - \frac{1}{p^2}\right). \end{aligned}$$

Будем неоднократно пользоваться тем, что число γ_1 ограничено сверху и снизу положительными константами. В силу леммы 8 существует функция $\Theta(N)$ такая, что $\Theta(N) = O(N^\varepsilon)$ для любого $\varepsilon > 0$ и

$$||S_1| - \gamma_1 N| \leq \Theta(N). \quad (6.6)$$

Идея доказательства теоремы 3 состоит в следующем. Рассмотрим семейство независимых одинаково распределенных случайных величин $\xi_{p,j}$, $p > 2$,

$1 \leq j < p^2/2$, каждая из которых принимает значения $+1$ и -1 с вероятностью $1/2$. Для $p \in \mathcal{P}_1$ обозначим

$$B(p) = \left\{ \xi_{p,j} : 1 \leq j < \frac{p^2}{2} \right\}.$$

Таким образом, $B(p)$ – случайное подмножество во множестве $\mathbb{Z}_p$ вычетов по модулю p^2 , причем каждый ненулевой вычет попадает в $B(p)$ с вероятностью $1/2$ и, кроме того, $b_1 + b_2 \not\equiv 0 \pmod{p}$ для любых $b_1, b_2 \in B(p)$. Обозначим

$$S_2 = \{n \in S_1 : \forall p \in \mathcal{P}_1 \exists b \in B_p \ n \equiv b \pmod{p^2}\}.$$

Пусть $t = |P_1|$; тогда, поскольку каждый элемент множества S_1 попадает в S_2 с вероятностью $1/2^t$, это позволяет вычислить математическое ожидание случайной величины $|S_2|$:

$$\mathbb{E}|S_2| = 2^{-t}|S_1|.$$

Заметим, что $t \sim \delta_4 \log N$ и, значит,

$$2^t = N^{\delta_5 + o(1)}, \quad \delta_5 = (\log 2)\delta_4. \quad (6.7)$$

Наша цель – доказать, что множество S_2 с большой вероятностью является “сбалансированным”, т.е. его размер близок к $2^{-t}|S_1|$, и, более того, для любого небольшого натурального числа d , $(d, P(z_1)) = 1$, множество S_2 почти равномерно распределено по вычетам $\pmod{d^2}$. Заметим, что для любых $s_1, s_2 \in S_2$ число $s_1 + s_2$ не делится на p^2 ни при каком $p < z_1$. Докажем, что из “сбалансированного” множества можно выбрать достаточно большое подмножество, сумма любых двух элементов которого свободна от квадратов.

Напомним, что $B_{d,l}(D) = \{n \in D : n \equiv l \pmod{d^2}\}$.

ЛЕММА 10. Если $(d, P(z_1)) = 1$, $d^2 \leq N$, то для любого $\varepsilon > 0$

$$\mathbb{E}|B_{d,l}(S_2)| = \left(\frac{\gamma_1 N}{d^2} + O(N^\varepsilon) \right) 2^{-t}, \quad (6.8)$$

$$\mathbb{E}|B_{d,l}(S_2)|^2 \leq (\mathbb{E}|B_{d,l}(S_2)|)^2 + O\left(2^{-t} N^\varepsilon \frac{N}{d^2}\right). \quad (6.9)$$

ДОКАЗАТЕЛЬСТВО. Без ограничения общности можно считать, что $-d^2 < l \leq 0$. Пусть $M = \lfloor (N - l)/d^2 \rfloor$. Множество чисел вида $(n - l)/q^2$, $n \in B_{d,l}(S_1)$, представляет собой отрезок натурального ряда $[1, M]$, из которого удалены числа, лежащие в трех классах вычетов по модулю 4 и (для каждого p , $2 < p < p_1$) лежащие в одном из классов вычетов по модулю p^2 . Отсюда по лемме 8 имеем

$$|B_{d,l}(S_1)| = \gamma_1 M + O(N^\varepsilon) = \frac{\gamma_1 N}{d^2} + O(N^\varepsilon). \quad (6.10)$$

Вновь пользуясь тем, что каждый элемент множества S_1 попадает в S_2 с вероятностью $1/2^t$, получаем

$$\mathbb{E}|B_{d,l}(S_2)| = 2^{-t}|B_{d,l}(S_1)|. \quad (6.11)$$

Отсюда и из (6.10) вытекает утверждение (6.8).

Для любых двух элементов n_0, n из $B_{d,l}(S_1)$ рассмотрим следующее событие $\Omega(n_0, n)$: оба элемента n_0, n принадлежат S_2 . Ясно, что

$$\mathbb{E}|B_{d,l}(S_2)|^2 = \sum_{n_0, n \in B_{d,l}(S_1)} \Pr \Omega(n_0, n). \quad (6.12)$$

Далее, для любых n_0, n из $B_{d,l}(S_1)$ вероятность события $\Omega(n_0, n)$ равна нулю, если $n \equiv -n_0 \pmod{p^2}$ для некоторого $p \in P_1$. В противном случае

$$\Pr \Omega(n_0, n) = \prod_{\substack{p \in P_1 \\ n \equiv n_0 \pmod{p^2}}} \frac{1}{2} \prod_{\substack{p \in P_1 \\ n \not\equiv n_0 \pmod{p^2}}} \frac{1}{4} = 4^{-t} 2^{\omega(n, n_0)}, \quad (6.13)$$

где $\omega(n, n_0)$ – количество $p \in P_1$ таких, что $n \equiv n_0 \pmod{p^2}$. Через $Q_1(n_0, n)$ обозначим наибольшее q такое, что $q|P(z_1)/2$ и $q^2|(n_0 - n)$, а через $Q_2(n_0, n)$ – наибольшее q такое, что $q|P(z_1)/2$ и $q^2|(n_0 + n)$.

Заметим, что $(Q_1(n_0, n), Q_2(n_0, n)) = 1$, поскольку в силу определения множества S_1 числа n и n_0 не делятся на квадрат ни одного числа $p|P(z_1)/2$ (т. е. $p \in P_1$). Имеем

$$2^{\omega(n, n_0)} = \sum_{q_1 | Q_1(n_0, n)} 1,$$

а сумма

$$\sum_{q_2 | Q_2(n_0, n)} \mu(q_2)$$

равна единице, если $n + n_0$ не делится на квадрат никакого простого $p \in P_1$, и равна нулю в противном случае. Поэтому из (6.13) следует, что

$$\Pr \Omega(n_0, n) = 4^{-t} \sum_{q_1 | Q_1(n_0, n)} \sum_{q_2 | Q_2(n_0, n)} \mu(q_2). \quad (6.14)$$

Объединяя соотношения (6.12) и (6.14), получаем

$$\mathbb{E}|B_{d,l}(S_2)|^2 = \Sigma_1 + \sum_{q|P(z_1)/2} \Sigma_{2,q}, \quad (6.15)$$

где

$$\begin{aligned} \Sigma_1 &= \sum_{n \in B_{d,l}(S_1)} \Pr \Omega(n, n), \\ \Sigma_{2,q} &= 4^{-t} \sum_{q=q_1 q_2} \mu(q_2) \sum_{\substack{n, n_0 \in B_{d,l}(S_1), n \neq n_0 \\ q_1^2 | (n_0 - n), q_2^2 | (n_0 + n)}} 1. \end{aligned}$$

Первое слагаемое в правой части (6.15) легко вычисляется:

$$\Sigma_1 = \sum_{n \in B_{d,l}(S_1)} 2^{-t} = 2^{-t} |B_{d,l}(S_1)|. \quad (6.16)$$

Так же нетрудно проверить, что $\Sigma_{2,1} = 4^{-t} |B_{d,l}(S_1)|^2$, откуда, учитывая равенство (6.11), получаем

$$\Sigma_{2,1} = (\mathbb{E} |B_{d,l}(S_2)|)^2. \quad (6.17)$$

Фактически $\Sigma_{2,1}$ можно рассматривать как главный член в $\mathbb{E} |B_{d,l}(S_2)|^2$, а Σ_1 и $\Sigma_{2,q}$ при $q > 1$ – как остаточные члены. Из (6.15)–(6.17) следует, что

$$\mathbb{E} |B_{d,l}(S_2)|^2 - (\mathbb{E} |B_{d,l}(S_2)|)^2 = 2^{-t} |B_{d,l}(S_1)| + \sum_{\substack{q > 1 \\ q | P(z_1)/2}} \Sigma_{2,q}. \quad (6.18)$$

Остается оценить сверху суммарный вклад $\Sigma_{2,q}$ при $q > 1$.

Прежде всего заметим, что условия $q = q_1 q_2$, $n \neq n_0$, $q_1^2 | (n_0 - n)$, $q_2^2 | (n_0 + n)$ влекут $n^2 \equiv n_0^2 \pmod{q^2}$, откуда следует, что в (6.16) достаточно ограничиться $q \leq N$. По лемме 9 количество таких q есть $O(N^\varepsilon)$. Далее, при фиксированных q, q_1, q_2, n_0 условия $n \equiv l \pmod{d^2}$, $n \equiv n_0 \pmod{q_1^2}$, $n \equiv -n_0 \pmod{q_2^2}$ означают, что n принадлежит некоторому вычету $l' \pmod{(dq)^2}$. Применяя лемму 8 ко множеству $\{(n - l')/(dq)^2\}$, как это было сделано в начале доказательства леммы, находим, что количество таких n равно

$$\gamma_q N(dq)^2 + O(N^\varepsilon), \quad (6.19)$$

где

$$\gamma_q = 14 \prod_{p \in P_1, p \nmid q} (1 - p^2).$$

Суммируя (6.19) при фиксированных q, n_0 по всем q_1 , мы получаем

$$\gamma_q N(dq)^2 \sum_{q_2 | q} \mu(q_2) + \sum_{q_2 | q} O(N^\varepsilon).$$

Однако

$$\sum_{q_2 | q} \mu(q_2) = 0,$$

так как $q > 1$, а количество делителей q есть $O(N^\varepsilon)$ в силу леммы 9 (можно также воспользоваться неравенством $q \leq N$). Значит,

$$\gamma_q N(dq)^2 \sum_{q_2 | q} \mu(q_2) + \sum_{q_2 | q} O(N^\varepsilon) = O(N^{2\varepsilon}).$$

Отсюда, учитывая (6.10), мы получаем

$$\Sigma_{2,q} = 4^{-t} N^{2\varepsilon} \left(O\left(\frac{N}{d^2}\right) + O(N^\varepsilon) \right).$$

Взяв теперь сумму по всем q , мы имеем

$$\sum_{q > 1} \Sigma_{2,q} = O(4^{-t} N^{3\varepsilon} N d^2) + O(4^{-t} N^{4\varepsilon}).$$

Отсюда и из соотношений (6.18) и (6.10) следует, что

$$\begin{aligned} \mathbb{E}|B_{d,l}(S_2)|^2 - (\mathbb{E}|B_{d,l}(S_2)|)^2 &= O\left(2^{-t}\frac{N}{d^2}\right) + O(2^{-t}N^\varepsilon) \\ &+ O\left(4^{-t}N^{3\varepsilon}\frac{N}{d^2}\right) + O(4^{-t}N^{4\varepsilon}) = O\left(2^{-t}N^{4\varepsilon}\frac{N}{d^2}\right). \end{aligned}$$

Поскольку последняя оценка верна для произвольного $\varepsilon > 0$, то неравенство (6.9) также установлено для любого $\varepsilon > 0$. Лемма доказана.

ЛЕММА 11. *При выполнении условий леммы 10 имеем*

$$\mathbb{E} \sum_{l \pmod{d^2}} \left(|B_{d,l}(S_2)| - \frac{|S_2|}{d^2} \right)^2 = O(2^{-t}N^{1+\varepsilon}).$$

ДОКАЗАТЕЛЬСТВО. Имеем

$$\begin{aligned} &\mathbb{E} \sum_{l \pmod{d^2}} \left(|B_{d,l}(S_2)| - \frac{|S_2|}{d^2} \right)^2 \\ &\leq 4 \sum_{l \pmod{d^2}} \mathbb{E}(|B_{d,l}(S_2)| - \mathbb{E}|B_{d,l}(S_2)|)^2 \\ &\quad + 4 \sum_{l \pmod{d^2}} \left(\mathbb{E}|B_{d,l}(S_2)| - \frac{2^{-t}\gamma_1 N}{d^2} \right)^2 \\ &\quad + 4 \sum_{l \pmod{d^2}} \left(\frac{2^{-t}\gamma_1 N}{d^2} - \frac{\mathbb{E}|S_2|}{d^2} \right)^2 + 4 \sum_{l \pmod{d^2}} \mathbb{E} \left(\frac{\mathbb{E}|S_2|}{d^2} - \frac{|S_2|}{d^2} \right)^2 \\ &= 4 \sum_{l \pmod{d^2}} \mathbb{E}(|B_{d,l}(S_2)| - \mathbb{E}|B_{d,l}(S_2)|)^2 \\ &\quad + 4 \sum_{l \pmod{d^2}} \left(\mathbb{E}|B_{d,l}(S_2)| - \frac{2^{-t}\gamma_1 N}{d^2} \right)^2 \\ &\quad + \frac{4}{d^2} (2^{-t}\gamma_1 N - \mathbb{E}|S_2|)^2 + \frac{4}{d^2} \mathbb{E}(\mathbb{E}|S_2| - |S_2|)^2. \end{aligned} \tag{6.20}$$

Однако

$$\mathbb{E}(|B_{d,l}(S_2)| - \mathbb{E}|B_{d,l}(S_2)|)^2 = \mathbb{E}|B_{d,l}(S_2)|^2 - (\mathbb{E}|B_{d,l}(S_2)|)^2$$

(обе части последнего равенства равны дисперсии случайной величины $|B_{d,l}(S_2)|$), и в силу (6.9)

$$\sum_{l \pmod{d^2}} \mathbb{E}(|B_{d,l}(S_2)| - \mathbb{E}|B_{d,l}(S_2)|)^2 = O(2^{-t}N^{1+\varepsilon}). \tag{6.21}$$

Далее, из равенства (6.8) мы получаем, что

$$\sum_{l \pmod{d^2}} \left(\mathbb{E}|B_{d,l}(S_2)| - \frac{2^{-t}\gamma_1 N}{d^2} \right)^2 = O(4^{-t}N^{2\varepsilon}d^2) = O(4^{-t}N^{1+2\varepsilon}). \tag{6.22}$$

В силу (6.8) при $d = 1$ имеем

$$(2^{-t}\gamma_1 N - \mathbb{E}|S_2|)^2 = O(4^{-t}N^{2\varepsilon}). \quad (6.23)$$

Наконец, используя (6.9) при $d = 1$ и равенство

$$\mathbb{E}(\mathbb{E}|S_2| - |S_2|)^2 = \mathbb{E}|S_2|^2 - (\mathbb{E}|S_2|)^2,$$

получаем

$$\mathbb{E}(\mathbb{E}|S_2| - |S_2|)^2 = O(2^{-t}N^{1+\varepsilon}). \quad (6.24)$$

Подставляя соотношения (6.21)–(6.24) в (6.20), приходим к оценке

$$\mathbb{E} \sum_{l \pmod{d^2}} \left(|B_{d,l}(S_2)| - \frac{|S_2|}{d^2} \right)^2 = O(2^{-t}N^{1+2\varepsilon}).$$

Ввиду произвольности $\varepsilon > 0$ лемма доказана.

Теперь докажем существование искомого “сбалансированного” множества S_2 .

ЛЕММА 12. Пусть число $\delta_5 \in (0, 1)$ определяется соотношением (6.7), а положительные числа α и δ_3 удовлетворяют неравенству

$$1 + \alpha - \delta_5 - 2\delta_3 < 0. \quad (6.25)$$

Тогда для достаточно большого N можно выбрать знаки $\xi_{p,j}$, $p \in \mathcal{P}_1$, $1 \leq j < p^2/2$, так, что для множества S_2 выполнены условия

$$\frac{1}{2} 2^{-t}\gamma_1 N \leq |S_2| \leq \frac{3}{2} 2^{-t}\gamma_1 N, \quad (6.26)$$

$$\forall d, \forall l \ (d \leq N^\alpha, \ (d, P(z_1)) = 1) \rightarrow \left| |B_{d,l}(S_2)| - \frac{|S_2|}{d^2} \right| \leq N^{\delta_3}. \quad (6.27)$$

ДОКАЗАТЕЛЬСТВО. Через E_0 обозначим событие

$$||S_2| - 2^{-t}\gamma_1 N| > \frac{1}{2} 2^{-t}\gamma_1 N,$$

а через $E_{d,l}$ – событие

$$\left| |B_{d,l}(S_2)| - \frac{|S_2|}{d^2} \right| > N^{\delta_3}.$$

Как только мы проверим, что

$$\Pr E_0 + \sum_{\substack{d \leq N^\alpha \\ (d, P(z_1))=1}} \sum_{l \pmod{d^2}} \Pr E_{d,l} < 1, \quad (6.28)$$

лемма будет доказана, так как из неравенства (6.28) следует, что с положительной вероятностью ни одно из событий E_0 , $E_{d,l}$ не произойдет, а тогда будут выполнены условия (6.26) и (6.27).

Запишем неравенство (6.8) для $d = 1$:

$$\mathbb{E}|S_2| = \gamma_1 N 2^{-t} + \Theta, \quad \Theta = O(2^{-t} N^\varepsilon). \quad (6.29)$$

Через E'_0 обозначим событие

$$||S_2| - \mathbb{E}|S_2|| > \frac{1}{2} 2^{-t} \gamma_1 N - \Theta.$$

В силу (6.29) имеем $\Pr E_0 \leq \Pr E'_0$. Отсюда и из неравенства (6.24), применяя неравенство Чебышева, получаем

$$\Pr E_0 \leq \left(\frac{1}{2} 2^{-t} \gamma_1 N - \Theta \right)^{-2} \mathbb{E}(\mathbb{E}|S_2| - |S_2|)^2 = O(2^t N^{\varepsilon-1}),$$

откуда в силу (6.7) имеем

$$\Pr E_0 = O(N^{\delta_5 + \varepsilon - 1 + o(1)}).$$

Поскольку $\delta_5 < 1$, то, подбирая достаточно малое ε , мы видим, что

$$\Pr E_0 = o(1), \quad N \rightarrow \infty. \quad (6.30)$$

Вновь применяя неравенство Чебышева, имеем

$$\Pr E_{d,l} \leq N^{-2\delta_3} \mathbb{E} \left(|B_{d,l}(S_2)| - \frac{|S_2|}{d^2} \right)^2,$$

откуда в силу леммы 11

$$\sum_{l \pmod{d^2}} \Pr E_{d,l} = N^{-2\delta_3} O(2^{-t} N^{1+\varepsilon}).$$

Учитывая (6.7), получаем

$$\sum_{l \pmod{d^2}} \Pr E_{d,l} \leq N^{1-\delta_5-2\delta_3+\varepsilon+o(1)}. \quad (6.31)$$

Суммируя (6.31) по $d \leq N^\alpha$, $(d, P(z_1)) = 1$, мы приходим к оценке

$$\sum_{\substack{d \leq N^\alpha \\ (d, P(z_1))=1}} \sum_{l \pmod{d^2}} \Pr E_{d,l} = O(N^{1+\alpha-\delta_5-2\delta_3+\varepsilon+o(1)}),$$

откуда в силу условия (6.25), подбирая достаточно малое ε , получим

$$\sum_{\substack{d \leq N^\alpha \\ (d, P(z_1))=1}} \sum_{l \pmod{d^2}} \Pr E_{d,l} = o(1), \quad N \rightarrow \infty. \quad (6.32)$$

Требуемое неравенство (6.28) для больших N немедленно вытекает из (6.30) и (6.32). Тем самым лемма доказана.

§7. Доказательство теоремы 3

Не ограничивая общности, полагаем, что N – достаточно большое натуральное число. Выберем положительные числа $\alpha_2 = \alpha_3 \leq 1/8$ и $\delta_2 = \delta_4 < \alpha_2$. Пусть $\alpha = 2\alpha_2 = \alpha_2 + \alpha_3$, $\delta_3 = \frac{1}{2} + \alpha_2$. В качестве ε возьмем малое положительное число и при этом предположим, что $N \geq N(\varepsilon)$. В соответствии с конструкцией из §6 положим $z_1 = [\delta_4 \log N \log \log N]$; множества $\mathcal{P}_1, S_1, S_2$ и число γ_1 задаются так же, как в §6. Вследствие определения α и δ_3 имеет место условие (6.25), поэтому множество S_2 выбирается так, чтобы для него выполнялись утверждения леммы 12.

Положим $z_2 = [\log^3 N]$, $z_3 = [N^{\alpha_3}/2]$. Заметим, что условия (4.22), (4.30) и (4.31) выполнены. Поскольку

$$2\alpha_3 + \delta_2 + \delta_3 = \frac{1}{2} + 3\alpha_3 + \delta_2 < \frac{1}{2} + 4\alpha_3 \leq 1,$$

то можно выбрать α_1 и ε так, чтобы выполнялось неравенство

$$8\alpha_1 + 2\alpha_3 + \delta_2 + \delta_3 < 1 - \varepsilon,$$

откуда следует (4.24), так как

$$\frac{\log z_1}{\log \log N} < 2, \quad \frac{\log z_2}{\log \log N} \leq 3.$$

Из последнего неравенства вытекает также (4.3), если потребовать дополнительно, чтобы выполнялось неравенство $\alpha_1 < \alpha_2/3$. Выберем $\delta_1 > 0$ так, чтобы выполнялось условие (4.1). Наконец, положим

$$\rho = \left\lceil \frac{\delta_1 \delta_4^2}{3} \log^2 N \log \log N \right\rceil.$$

Тогда при достаточно большом N условия (4.2) и (4.21) также выполнены. Для доказательства теоремы нам достаточно показать, что

$$ES_N \geq \rho. \quad (7.1)$$

Итак, нам нужно найти множество $\mathcal{A} \subset \{1, \dots, N\}$ такое, что $a + a' \in S_0$ для любых $a \in \mathcal{A}$, $a' \in \mathcal{A}$, и при этом $|\mathcal{A}| \geq \rho$. Будем строить $\mathcal{A}$ как подмножество множества S_2 . Элементы $a_1, \dots, a_\rho$ будем выбирать последовательно. Допустим, что $l \leq \rho$ и элементы $a_1, \dots, a_{l-1}$ из S_2 уже выбраны. Тогда элемент $a \in S_2$ может быть выбран в качестве a_l , если он отличен от $a_1, \dots, a_{l-1}$, и при этом для любого простого p выполнены условия

$$a \not\equiv 0 \pmod{p^2}, \quad a \not\equiv -a_j \pmod{p^2}, \quad j = 1, \dots, l-1. \quad (7.2)$$

Заметим, что при $p < z_1$ условия (7.2) выполняются автоматически по определению множества S_2 . Выполнены они и при $p > \sqrt{2N}$, поскольку для натуральных чисел $a \leq N$, $a_j \leq N$ числа $2a$, $a + a_j$ не превосходят $2N$ и, стало быть, не делятся

на p^2 . Более того, если $p > \sqrt{N}$, $a \leq N$, $a_j \leq N$ и $a + a_j$ делится на p^2 , то обязательно $a + a_j = p^2$, что невозможно для $a, a_j \in S_2 \subset S_1$, поскольку по определению S_1 мы имеем $a + a_1 \equiv 2 \pmod{4}$. Таким образом, условие (7.2) следует проверять только для $p \in \mathcal{P} = [z_1, \sqrt{N}]$. Для $p \in \mathcal{P}$ обозначим

$$B_p = \{0\} \cup \{-a_j\} \pmod{p^2}.$$

Условие (7.2) для $a \in S_2$ можно переписать в виде $a \in R(D, \mathcal{B})$. Для оценки $|R(D, \mathcal{B})|$ мы воспользуемся леммой 7. Для достаточно большого N условия (4.4) и (4.23) вытекают из (6.26) и (6.27). Поэтому можно применить лемму 7, и мы получаем при $N \rightarrow \infty$ асимптотическое равенство (4.25), которое можно переписать в виде

$$|R(S_2, \mathcal{B})| \sim \gamma |S_2|, \quad \gamma = \prod_{z_1 \leq p < z_2} \left(1 - \frac{\rho(p)}{p^2}\right).$$

Используя (4.18) для оценки γ , (6.26) для оценки $|S_2|$ и (6.7) для оценки 2^t , мы получаем

$$|R(S_2, \mathcal{B})| \geq N^{1-\delta_5-o(1)}, \quad N \rightarrow \infty.$$

Отсюда следует, что во множестве $R(S_2, \mathcal{B})$ имеется число, отличное от $a_1, \dots, a_{l-1}$ (напомним, что $l \leq \rho$), и его можно взять в качестве a_l . Это построение продолжается до тех пор, пока мы не получим искомое множество $\mathcal{A} = \{a_1, \dots, a_\rho\}$. Тем самым теорема 3 доказана.

Список литературы

1. *Balog A., Ruzsa I. Z.* A new lower bound for the L^1 mean of the exponential sum with the Möbius function // Bull. Lond. Math. Soc. 1999. V. 31. P. 415–418.
2. *Balog A. Ruzsa I. Z.* On the exponential sum over r -free integers // Acta Math. Hung. 2001. V. 90. P. 219–230.
3. *Бомбьеры Э., Заньне У.* О числе рациональных точек на некоторых эллиптических кривых // Изв. РАН. Сер. матем. 2004. Т. 68. №3. С. 5–14.
4. *Дэвенпорт Г.* Мультипликативная теория чисел. М.: Наука, 1989.
5. *Erdős P., Van Lint J. H.* On the number of positive integers $\leq x$ and free of prime factors $> y$ // Simon Stevin. 1966/67. V. 40. P. 73–76.
6. *Erdős P., Sárközy A.* On divisibility properties of integers of the form $a + a'$ // Acta Math. Hung. 1987. V. 50. P. 117–122.
7. *Фихтенгольц Г. М.* Курс дифференциального и интегрального исчисления. Т. 2. М.: Наука, 1969.
8. *Gorbachev D. V.* Improvement Taykov's lower bound in an inequation between C and L norms for trigonometric polynomials. <http://www.arxiv.org/math.CA/0212037>.
9. *Gyarmati K.* On divisibility properties of integers of the form $ab + 1$ // Period. Math. Hung. 2001. V. 43. P. 71–79.
10. *Хооли К.* Применение методов решета в теории чисел. М.: Наука, 1987.
11. *Konyagin S. V.* On squarefree numbers of the form $a + a'$ // Colloquium on Number Theory in honor of the 60th birthday of Professors Kálmán Györy and András Sárközy. Debrecen, 2000.

12. *Коробов Н. М.* Тригонометрические суммы и их приложения. М.: Наука, 1971.
13. *Монтгомери Г.* Мультипликативная теория чисел. М.: Мир, 1971.
14. *Прахар К.* Распределение простых чисел. М.: Мир, 1967.
15. *Sárközy A.* On a problem of Erdős // *Acta Math. Hung.* 1992. V. 60. P. 271–282.
16. *Тайков Л. В.* Один круг экстремальных задач для тригонометрических полиномов // *УМН.* 1965. Т. 20. С. 205–211.
17. *Тайков Л. В.* О наилучшем приближении ядер Дирихле // *Матем. заметки.* 1993. Т. 53. С. 116–121.

Московский государственный университет
им. М. В. Ломоносова

Поступило в редакцию
15.08.2003