Math-Net.Ru

Общероссийский математический портал

Ж. Бургейн, М. З. Гараев, Сумма множеств, образованных обратными элементами в полях простого порядка, и полилинейные суммы Клоостермана, *Изв. РАН. Сер. матем.*, 2014, том 78, выпуск 4, 19–72

DOI: <https://doi.org/10.4213/im8070>

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: 3.85.73.92

26 апреля 2023 г., 09:04:23

УДК 511.33+517

Ж. Бургейн, М. З. Гараев

Сумма множеств, образованных обратными элементами в полях простого порядка, и полилинейные суммы Клоостермана

Получены новые результаты об аддитивных свойствах множества $I^{-1} = \{x^{-1}; x \in I\}$, где I – произвольный интервал в поле классов вычетов по модулю большого простого числа p . С помощью этих результатов и оценок полилинейных экспоненциальных сумм получены новые результаты по неполным полилинейным суммам Клоостермана.

Библиография: 36 наименований.

Ключевые слова: сравнения по простому модулю, сумма множеств, полилинейные экспоненциальные суммы, полилинейные суммы Клоостермана, распределение простых чисел.

DOI: 10.4213/im8070

§ 1. Введение

На протяжении всей статьи p – большое простое число, $\mathbb{F}_p$ – поле классов вычетов по модулю p . Каждый класс вычетов часто будем отождествлять с его конкретным представителем. Для конечного множества X через $|X|$ будем обозначать его мощность. Если обратное не оговорено, то через ε обозначается малая положительная константа. Для данного целого числа x , взаимно простого с p (или для данного элемента x из $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$), через x^* или x^{-1} обозначаем обратный к x элемент по модулю p .

Пусть I – ненулевой интервал в $\mathbb{F}_p$. Аддитивные свойства обратного к I множества

$$I^{-1} = \{x^{-1}; x \in I\}$$

с последующим применением к суммам Клоостермана были рассмотрены в работе [1]. Было доказано, что для любого $\delta > 0$ существует $k \in \mathbb{Z}_+$ такое, что для мощности суммы множеств

$$k(I^{-1}) = \{x_1^{-1} + \cdots + x_k^{-1}; x_i \in I\}$$

имеет место оценка

$$|k(I^{-1})| > p^{-\delta} \min\{|I|^2, p\}.$$

В самом интересном случае $|I| < p^{\frac{1}{2}}$ последний результат дает оценку $|k(I^{-1})| > |I|^2 p^{-\delta}$. Из результатов недавней работы [2] (см. лемму 10 далее) следует, что

$$|I^{-1} + I^{-1}| > \min\{|I|^2, \sqrt{p|I|}\} |I|^{o(1)}. \quad (1)$$

В частности, если $|I| < p^{1/3}$, то $|I^{-1} + I^{-1}| > |I|^{2+o(1)}$.

В настоящей работе мы устанавливаем новые аддитивные свойства множества I^{-1} . Затем мы соединяем наши результаты с недавними оценками полилинейных экспоненциальных сумм из работы [3] и получаем новые оценки полилинейных сумм Клоостермана.

Статья организована следующим образом. В § 2 формулируются результаты по аддитивным свойствам множества I^{-1} и по оценкам сумм Клоостермана. В § 3 приводятся основные предварительные факты, которые используются далее в статье. В § 4–6 приводятся некоторые вспомогательные утверждения и доказываются предварительные леммы. Доказательство наших результатов об аддитивных свойствах обратных к интервалам множеств (теоремы 1–6) приведено в § 7. Доказательства теорем 7–13 и доказательство теоремы 14 о непрерывном аналоге оценки Карацубы даны в § 8. В § 9 содержатся доказательства теоремы 15 о $\pi(x) - \pi(x - y)$, теоремы 16 о линейных суммах Клоостермана и теоремы 17, относящейся к оценке Бруна–Тичмарша.

В настоящей статье мы рассматриваем только случай простого модуля. Случай составного модуля будет рассмотрен в нашей последующей статье.

§ 2. Формулировки результатов

2.1. Суммы обратных элементов интервала. Напомним, что I – произвольный ненулевой интервал поля $\mathbb{F}_p$. Сначала сформулируем результаты об аддитивных свойствах множества I^{-1} .

ТЕОРЕМА 1. *Для любой целой положительной константы k имеет место оценка*

$$J_{2k} < \left(|I|^{\frac{2k^2}{k+1}} + \frac{|I|^{2k}}{p} \right) |I|^{o(1)}, \quad (2)$$

где J_{2k} – число решений сравнения $x_1^{-1} + \dots + x_k^{-1} = x_{k+1}^{-1} + \dots + x_{2k}^{-1}$, $x_1, \dots, x_{2k} \in I$.

Напомним, что оценка (2) эквивалентна тому, что для любого $\varepsilon > 0$ существует $c = c(k; \varepsilon) > 0$ такое, что

$$J_{2k} < c \left(|I|^{\frac{2k^2}{k+1}} + \frac{|I|^{2k}}{p} \right) |I|^\varepsilon.$$

СЛЕДСТВИЕ 1. *Пусть $|I| < p^{\frac{1}{2}}$. Тогда для любой целой положительной константы k имеет место оценка*

$$|k(I^{-1})| > |I|^{\frac{2k}{k+1} + o(1)}.$$

Заметим, что при $k = 3$ имеет место более сильная оценка

$$|I^{-1} + I^{-1} + I^{-1}| > |I|^{1.55 + o(1)}$$

(см. § 10). Следующий результат относится к тернарному аддитивному сравнению с множеством I^{-1} .

ТЕОРЕМА 2. Пусть $|I| < p^{\frac{3}{46}}$. Тогда для любого элемента $\lambda \in \mathbb{F}_p$ с условием

$$\lambda \notin I^{-1} \cup \{0\} \quad (3)$$

имеет место оценка

$$J < |I|^{\frac{2}{3}+o(1)},$$

где J – число решений сравнения $x^{-1} + y^{-1} + z^{-1} = \lambda$, $x, y, z \in I$.

Ограничение (3) мотивировано тем, что в противном случае сравнение из теоремы 2 может иметь порядка $|I|^{1+o(1)}$ решений (например, $z = \lambda^{-1}$ и $x + y = 0$).

Из теоремы 2 легко вытекает, что при $|I| < p^{\frac{3}{46}}$ имеет место оценка

$$|I^{-1} + I^{-1} + I^{-1}| > |I|^{\frac{7}{3}+o(1)}.$$

Следующее утверждение показывает, что при малых I имеет место оптимальная оценка.

ТЕОРЕМА 3. Пусть $|I| < p^{\frac{1}{18}}$. Тогда имеет место оценка

$$J_6 < |I|^{3+o(1)},$$

где J_6 – число решений сравнения $x_1^{-1} + x_2^{-1} + x_3^{-1} = x_4^{-1} + x_5^{-1} + x_6^{-1}$, $x_1, \dots, x_6 \in I$. В частности, при $|I| < p^{\frac{1}{18}}$ имеем

$$|I^{-1} + I^{-1} + I^{-1}| > |I|^{3+o(1)}.$$

ТЕОРЕМА 4. Существует абсолютная константа $c > 0$ такая, что для любой целой положительной константы k и любого интервала $I \subset \mathbb{F}_p$ мощности $|I| < p^{\frac{c}{k^2}}$ имеет место оценка

$$J_{2k} < |I|^{k+o(1)},$$

где J_{2k} – число решений сравнения $x_1^{-1} + \dots + x_k^{-1} = x_{k+1}^{-1} + \dots + x_{2k}^{-1}$, $x_1, \dots, x_{2k} \in I$. В частности, для таких интервалов I имеем

$$|k(I^{-1})| > |I|^{k+o(1)}.$$

ЗАМЕЧАНИЕ 1. Из доказательства теоремы 4 следует, что в этой теореме можно брать $c = 1/4$.

ТЕОРЕМА 5. Пусть $I = [1, N]$. Тогда имеет место оценка

$$J_{2k} < (2k)^{90k^3} (\log N)^{4k^2} \left(\frac{N^{2k-1}}{p} + 1 \right) N^k,$$

где J_{2k} – число решений сравнения $x_1^* + \dots + x_k^* \equiv x_{k+1}^* + \dots + x_{2k}^* \pmod{p}$, $x_1, \dots, x_{2k} \in I$.

Приведем вариант теоремы 5, в котором переменные x_j будут простыми числами. Через $\mathcal{P}$ обозначим множество простых чисел.

ТЕОРЕМА 6. Пусть $I = [1, N]$. Тогда имеет место оценка

$$J_{2k} < (2k)^k \left(\frac{N^{2k-1}}{p} + 1 \right) N^k,$$

где J_{2k} – число решений сравнения $x_1^* + \dots + x_k^* \equiv x_{k+1}^* + \dots + x_{2k}^* \pmod{p}$, $x_1, \dots, x_{2k} \in I \cap \mathcal{P}$.

2.2. Неполные полилинейные суммы Клоостермана. Далее пользуемся сокращением $e_p(z) = e^{2\pi iz/p}$. Неполные суммы Клоостермана

$$\sum_{x=M+1}^{M+N} e_p(ax^* + bx),$$

где a и b – целые числа, $(a, p) = 1$, хорошо известны и имеют много применений в различных задачах теории чисел. Как следствие оценок Вейля, эти суммы оцениваются величиной порядка $O(p^{\frac{1}{2}} \log p)$. При $M = 0$ и очень малых N (порядка $N = p^{o(1)}$) эти суммы были оценены М. А. Королёвым [4].

Неполные билинейные суммы Клоостермана

$$S = \sum_{x_1=M_1+1}^{M_1+N_1} \sum_{x_2=M_2+1}^{M_2+N_2} \alpha_1(x_1) \alpha_2(x_2) e_p(ax_1^* x_2^*),$$

где $\alpha_i(x_i) \in \mathbb{C}$, $|\alpha_i(x_i)| \leq 1$, также хорошо известны. Заметим, что если один из параметров N_1, N_2 намного больше, чем $p^{\frac{1}{2}}$, то сумма S может быть легко оценена. Например, если, скажем, $N_1^{1-c} > p^{\frac{1}{2}}$ для некоторой константы $c > 0$, то из оценок Вейля следует, что

$$\begin{aligned} |S|^2 &\leq N_1 \sum_{x_1=M_1+1}^{M_1+N_1} \left| \sum_{x_2=M_2+1}^{M_2+N_2} \alpha_2(x_2) e_p(ax_1^* x_2^*) \right|^2 \\ &\leq N_1 \sum_{y=M_2+1}^{M_2+N_2} \sum_{z=M_2+1}^{M_2+N_2} \left| \sum_{x_1=M_1+1}^{M_1+N_1} e_p(ax_1^* (y^* - z^*)) \right| \ll N_1^2 N_2 + N_1 N_2^2 \sqrt{p} (\log p), \end{aligned}$$

откуда имеем

$$|S| < (N_2^{-\frac{1}{2}} + N_1^{-\frac{c}{2}}) (N_1 N_2)^{1+o(1)}.$$

Таким образом, наиболее нетривиальным будет случай, когда $N_i < p^{\frac{1}{2}}$. Если $M_1 = M_2 = 0$, то сумма S (в более общей форме) была оценена А. А. Карацубой [5], [6] для малых величин N_1 и N_2 и Ж. Бургейном [1] для произвольных M_1, M_2 при условии $N_1 N_2 > p^{\frac{1}{2}+\varepsilon}$. Явная версия результата Бургейна получена Р. Бейкером [7].

Неполные n -линейные суммы Клоостермана

$$\sum_{x_1=M_1+1}^{M_1+N_1} \dots \sum_{x_n=M_n+1}^{M_n+N_n} e_p(a_1 x_1 + \dots + a_n x_n + a_{n+1} (x_1 \dots x_n)^*),$$

где $a_i \in \mathbb{Z}$, $(a_{n+1}, p) = 1$, для произвольных n были изучены В. Люо [8] и И. Е. Шпарлинским [9]. Основными их инструментами являлись оценки Берджесса [10] неполных сумм Гаусса.

В настоящей работе мы соединяем наши теоремы 1–5 с оценкой полилинейных экспоненциальных сумм из [3] (см. далее лемму 1) и получаем новые оценки сумм Клоостермана.

Везде далее $\alpha_1(x_1), \dots, \alpha_n(x_n)$ являются произвольными комплексными числами такими, что $|\alpha_i(x_i)| \leq 1$.

ТЕОРЕМА 7. *Для любых интервалов I_1, I_2 с условием $|I_1| > p^{\frac{1}{18}}, |I_2| > p^{\frac{5}{12} + \varepsilon}$ имеет место оценка*

$$\max_{(a,p)=1} \left| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1) \alpha_2(x_2) e_p(ax_1^* x_2^*) \right| < p^{-\delta} |I_1| |I_2|$$

для некоторого $\delta = \delta(\varepsilon) > 0$.

Заметим, что если мощности $|I_1|$ и $|I_2|$ имеют порядок соответственно $p^{\frac{1}{18}}$ и $p^{\frac{5}{12} + \varepsilon}$, то $|I_1| |I_2|$ будет иметь порядок $p^{\frac{1}{2} - \frac{1}{36} + \varepsilon}$.

ЗАМЕЧАНИЕ 2. Утверждение теоремы 7 остается справедливым для более общей суммы

$$\sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1) \alpha_2(x_2) e_p(ax_1^* x_2^* + bx_1 x_2).$$

Это можно показать, соединяя нашу теорему 3 с леммой А.8 из работы [1].

В случае $M_1 = M_2 = 0$ мы докажем следующий результат, который улучшает область нетривиальности оценки Карацубы [6].

ТЕОРЕМА 8. *Пусть $I_1 = [1, N_1]$, $I_2 = [1, N_2]$. Тогда равномерно по всем натуральным числам k_1 и k_2 имеет место оценка*

$$\begin{aligned} \max_{(a,p)=1} \left| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1) \alpha_2(x_2) e_p(ax_1^* x_2^*) \right| &< (2k_1)^{\frac{45k_1^2}{k_2}} (2k_2)^{\frac{45k_2^2}{k_1}} (\log p)^{2(\frac{k_1}{k_2} + \frac{k_2}{k_1})} \\ &\times \left(\frac{N_1^{k_1-1}}{p^{\frac{1}{2}}} + \frac{p^{\frac{1}{2}}}{N_1^{k_1}} \right)^{\frac{1}{2k_1 k_2}} \left(\frac{N_2^{k_2-1}}{p^{\frac{1}{2}}} + \frac{p^{\frac{1}{2}}}{N_2^{k_2}} \right)^{\frac{1}{2k_1 k_2}} N_1 N_2. \end{aligned}$$

Для данных N_1, N_2 если взять k_1, k_2 так, чтобы выполнялись условия

$$N_1^{2(k_1-1)} < p \leq N_1^{2k_1}, \quad N_2^{2(k_2-1)} < p \leq N_2^{2k_2},$$

то оценка будет нетривиальной, за исключением случая, когда каждая из N_1 и N_2 будет находиться внутри p^ε -пропорции некоторого числа из множества $\{p^{\frac{1}{2l}}, l \in \mathbb{Z}_+\}$. Таким образом, имеем

СЛЕДСТВИЕ 2. *Пусть $I_1 = [1, N_1]$, $I_2 = [1, N_2]$, где либо для $i = 1$, либо для $i = 2$ выполняется условие*

$$N_i \notin \bigcup_{j \geq 1} [p^{\frac{1}{2j} - \varepsilon}, p^{\frac{1}{2j} + \varepsilon}].$$

Тогда для некоторого $\delta = \delta(\varepsilon) > 0$ имеет место оценка

$$\max_{(a,p)=1} \left| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1) \alpha_2(x_2) e_p(ax_1^* x_2^*) \right| < p^{-\delta} N_1 N_2.$$

ТЕОРЕМА 9. Для любых интервалов $I_1, I_2 \subset \mathbb{F}_p$ мощности соответственно N_1, N_2 имеет место оценка

$$\begin{aligned} \max_{(a,p)=1} \left| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1) \alpha_2(x_2) e_p(ax_1^* x_2^*) \right| \\ \ll p^{\frac{1}{8}} N_1^{\frac{3}{4}} N_2^{\frac{3}{4}} \left(\frac{N_1^3}{p} + 1 \right)^{\frac{1}{16}} \left(\frac{N_2^3}{p} + 1 \right)^{\frac{1}{16}}. \end{aligned}$$

Результаты, подобные теореме 9, для интервалов, начинающихся от нуля, содержатся в работах [7], [11], [12].

ТЕОРЕМА 10. Пусть k_1, k_2 – целые положительные константы, и пусть $I_1, I_2 \subset \mathbb{F}_p$ – интервалы мощности соответственно N_1, N_2 . Предположим, что

$$N_1 < p^{\frac{k_1+1}{2k_1}}, \quad N_2 < p^{\frac{k_2+1}{2k_2}}.$$

Тогда имеет место оценка

$$\begin{aligned} \max_{(a,p)=1} \left| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1) \alpha_2(x_2) e_p(ax_1^* x_2^*) \right| \\ < \left(p^{\frac{1}{2k_1 k_2}} N_1^{-\frac{1}{k_2(k_1+1)}} N_2^{-\frac{1}{k_1(k_2+1)}} \right) (N_1 N_2)^{1+o(1)}. \end{aligned}$$

Перейдем к рассмотрению полилинейных сумм Клоостермана.

ТЕОРЕМА 11. Пусть $n \geq 7$ и $N^n > p^{\frac{1}{3}+\varepsilon}$. Тогда для любых интервалов $I_1, \dots, I_n$ мощности N имеет место оценка

$$\max_{(a,p)=1} \left| \sum_{x_1 \in I_1} \cdots \sum_{x_n \in I_n} \alpha_1(x_1) \cdots \alpha_n(x_n) e_p(ax_1^* \cdots x_n^*) \right| < p^{-\delta} N^n$$

при некотором $\delta = \delta(\varepsilon, n) > 0$.

ТЕОРЕМА 12. Существует абсолютная константа $C > 0$ такая, что для любого натурального числа n и любых интервалов $I_1, \dots, I_n$ мощности $N > p^{\frac{C}{n^2}}$ имеем

$$\max_{(a,p)=1} \left| \sum_{x_1 \in I_1} \cdots \sum_{x_n \in I_n} \alpha_1(x_1) \cdots \alpha_n(x_n) e_p(ax_1^* \cdots x_n^*) \right| < p^{-\delta} N^n$$

при некотором $\delta = \delta(n) > 0$.

ЗАМЕЧАНИЕ 3. Можно показать, что теорема 12 имеет место с константой $C = 4$. Для этого можно использовать геометрию чисел в стиле работы [13] и получить подходящий для этой цели вариант нашей теоремы 4.

ТЕОРЕМА 13. Пусть $I_1, \dots, I_n$ – интервалы в $[1, p-1]$, удовлетворяющие условию

$$|I_1| \cdots |I_n| > p^{\frac{1}{2} + \varepsilon}.$$

Тогда для произвольных целых чисел $a, a_1, \dots, a_n$ с условием $(a, p) = 1$ и некоторого $\delta = \delta(\varepsilon, n) > 0$ выполняется оценка

$$\left| \sum_{x_1 \in I_1} \cdots \sum_{x_n \in I_n} e_p(ax_1^* \cdots x_n^* + a_1 x_1 + \cdots + a_n x_n) \right| < p^{-\delta} |I_1| \cdots |I_n|.$$

Имеет место следующий непрерывный аналог оценки Карацубы.

ТЕОРЕМА 14. Пусть $\xi \in \mathbb{R}$, $|\xi| > N_1 N_2$ и $k_1, k_2 \in \mathbb{Z}_+$. Тогда

$$\left| \sum_{n_1=N_1+1}^{2N_1} \sum_{n_2=N_2+1}^{2N_2} \alpha_1(n_1) \alpha_2(n_2) e^{i \frac{1}{n_1} \frac{1}{n_2} \xi} \right| < c(k_1, k_2, \varepsilon) \gamma(N_1 N_2)^{1+\varepsilon}, \quad (4)$$

где

$$\gamma = \left\{ \left(\frac{|\xi|}{N_1 N_2} N_1^{-2k_1} + \frac{N_1 N_2}{|\xi|} N_1^{2(k_1-1)} \right) \left(\frac{|\xi|}{N_1 N_2} N_2^{-2k_2} + \frac{N_1 N_2}{|\xi|} N_2^{2(k_2-1)} \right) \right\}^{\frac{1}{4k_1 k_2}}.$$

При данном $|\xi| > N_1 N_2$ выбираем k_1, k_2 так, чтобы

$$N_i^{2(k_i-1)} \leq \frac{|\xi|}{N_1 N_2} < N_i^{2k_i}.$$

Тогда при предельных значениях каждый множитель в выражении для γ в теореме 14 будет являться $O(1)$.

Экспоненциальные суммы вида (4) появляются, например, в [14, доказательство теоремы 13.8], именно

$$\pi(x) - \pi(x-y) \leq (2-\delta) \frac{y}{\log y}, \quad x^\theta < y < x, \quad (5)$$

где, как обычно, $\pi(z)$ – количество простых чисел, не превосходящих z , а $\delta = \delta(\theta) > 0$. Здесь $\theta > 0$ может быть малым, $x > x_0(\theta)$ достаточно большое. В [14] доказательство (5) основано на оценках экспоненциальных сумм вида $\sum_{n \sim N} e(\frac{\xi}{n})$ при использовании либо метода Вейля, либо метода Виноградова, где θ мало. Используя теорему 14, можно улучшить оценку.

ТЕОРЕМА 15. Оценка (5) имеет место при

$$\delta < \frac{2(1-\theta)}{12(\theta^{-1}+1)(\theta^{-1}+0.5)+1-\theta} \sim \theta^2.$$

Мы будем применять оценки трилинейных экспоненциальных сумм из работы [3] (см. далее лемму 1) к линейным суммам Клоостермана и задаче, связанной с теоремой Бруна–Титчмарша.

ТЕОРЕМА 16. *Имеет место оценка*

$$\max_{(a,p)=1} \left| \sum_{n \leq N} e_p(an^*) \right| \ll \frac{(\log \log p)^3 \log p}{(\log N)^{\frac{3}{2}}} N,$$

где константа в знаке $\ll$ является абсолютной.

Из теоремы 16 следует, что при $N = p^\varepsilon$ с фиксированным ε имеем понижение порядка $O((\log \log p)^3 / (\log p)^{\frac{1}{2}})$. При этом оценка теоремы 16 является нетривиальной при $N > \exp((\log p)^{\frac{2}{3}} (\log \log p)^3)$. Это улучшает некоторые результаты Королёва [4] в случае простого модуля (см. также работу [15], где рассмотрены различные варианты задачи).

Заметим, что в работе [16] утверждается, что для фиксированного $\varepsilon > 0$ и $p^\varepsilon < N < p^{\frac{4}{7}}$ имеет место оценка

$$\left| \sum_{n=1}^N e_p(an^*) \right| < \frac{N}{(\log N)^{1-\varepsilon}},$$

но приведенное в [16] доказательство вызывает сомнения. Наше доказательство существенно опирается на оценки трилинейных экспоненциальных сумм из работы [3] (см. также [17, теорема 4.2]).

При $(a, q) = 1$ через $\pi(x; q, a)$ обозначено количество простых чисел $p \leq x$ с условием $p \equiv a \pmod{q}$. Мы улучшаем результат Фридландера–Иванца о $\pi(x; q, a)$ в следующей форме.

ТЕОРЕМА 17. *Пусть $x^\theta \leq q \leq 2x^\theta$, где $\theta < 1$ близко к 1. Тогда для некоторой абсолютной константы $c_1 > 0$ и всех достаточно больших $x > x_0(\theta)$ имеет место оценка*

$$\pi(x; q, a) < \frac{cx}{\varphi(q) \log(x/q)},$$

где $c = 2 - c_1(1 - \theta)^2$.

Константы в теореме 17 являются эффективными и могут быть явно выписаны. Заметим, что для небольших значений θ имеются более точные оценки. В недавней работе Дж. Майнард [19] при $q < x^{\frac{1}{8}}$ получена оценка

$$\pi(x; q, a) < \frac{2x}{\varphi(q) \log x}.$$

Также напомним результат Мотохаши (см., например, [20, (5.13)]), который утверждает, что для любой фиксированной константы $\varepsilon > 0$, если $q < x^{\frac{9}{20} - \varepsilon}$, имеет место оценка

$$\pi(x; q, a) < \frac{(2 + o(1))x}{\varphi(q) \log(x/q^{\frac{3}{8}})}.$$

Более детальную информацию можно найти в работах [19], [20] и приведенных в них библиографиях.

§ 3. Предварительные замечания

На протяжении статьи будем пользоваться хорошо известными связями между числом решений симметрических уравнений и мощностью соответствующих множеств. Пусть T – число решений уравнения

$$x_1 + \dots + x_n = y_1 + \dots + y_n,$$

где при каждом i переменные x_i, y_i независимо друг от друга пробегают некоторое множество A_i . Тогда для любого подмножества $\Omega \subset A_1 \times \dots \times A_n$ имеет место оценка

$$|\{x_1 + \dots + x_n; (x_1, \dots, x_n) \in \Omega\}| \geq \frac{|\Omega|^2}{T}.$$

Данная оценка следует из того, что если $T_n(\Omega; \lambda)$ – число решений уравнения $x_1 + \dots + x_n = \lambda$, $(x_1, \dots, x_n) \in \Omega$, и если $X = \{x_1 + \dots + x_n; (x_1, \dots, x_n) \in \Omega\}$, то

$$T \geq \sum_{\lambda \in X} T_n(\Omega; \lambda)^2 \geq \frac{1}{|X|} \left| \sum_{\lambda \in X} T_n(\Omega; \lambda) \right|^2 = \frac{|\Omega|^2}{|X|}.$$

В частности,

$$|A_1 + \dots + A_n| = \#\{a_1 + \dots + a_n; a_i \in A_i\} \geq \frac{|A_1|^2 \dots |A_n|^2}{T}.$$

Заметим, что если $A_1, \dots, A_{2n} \subset \mathbb{F}_p$, а $T_{2n}(\lambda)$ – число решений сравнения

$$x_1 + \dots + x_{2n} \equiv \lambda \pmod{p}, \quad (x_1, \dots, x_{2n}) \in A_1 \times \dots \times A_{2n},$$

то выполняется оценка

$$T_{2n}(\lambda) \leq (J_1 \dots J_{2n})^{\frac{1}{2n}},$$

где J_i – число решений сравнения

$$y_1 + \dots + y_n \equiv y_{n+1} + \dots + y_{2n} \pmod{p}, \quad y_1, \dots, y_{2n} \in A_i.$$

Действительно, имеем

$$T_{2n}(\lambda) = \frac{1}{p} \sum_{a=0}^{p-1} \sum_{x_1 \in A_1} \dots \sum_{x_{2n} \in A_{2n}} e_p(ax_1) \dots e_p(ax_{2n}) e_p(-a\lambda).$$

Применяя неравенство Гёльдера, получаем

$$T_{2n}(\lambda) \leq \prod_{j=1}^{2n} \left(\frac{1}{p} \sum_{a=0}^{p-1} \left| \sum_{x_j \in A_j} e_p(ax_j) \right|^{2n} \right)^{\frac{1}{2n}} = (J_1 \dots J_{2n})^{\frac{1}{2n}}.$$

При доказательстве некоторых наших результатов будем использовать следующее наблюдение: если $X, Y \subset \mathbb{F}_p$, то число решений сравнения

$$\frac{1}{y + x_1} + \dots + \frac{1}{y + x_n} = \frac{1}{y + x_{n+1}} + \dots + \frac{1}{y + x_{2n}}, \quad x_i \in X, \quad y \in Y,$$

ограничено величиной $O(|X|^n Y + |X|^{2n})$, где константа в знаке O может зависеть только от n . Действительно, вклад тех $(x_1, \dots, x_{2n}) \in X^{2n}$, для которых последовательность $x_1, \dots, x_{2n}$ содержит не более чем n различных элементов, ограничен величиной $O(|X|^n |Y|)$. С другой стороны, если в этой последовательности имеется более чем n различных элементов, то можем предположить, что $x_1 \notin \{x_2, \dots, x_{2n}\}$. Для каждого такого $(x_1, \dots, x_{2n}) \in X^{2n}$ многочлен

$$P(Z) = \prod_{i \neq 1} (Z + x_i) + \dots + \prod_{i \neq n} (Z + x_i) - \prod_{i \neq n+1} (Z + x_i) - \dots - \prod_{i \neq 2n} (Z + x_i)$$

является ненулевым ($P(-x_1) \neq 0$), а так как $P(y) = 0$, то получаем, что для y имеется не более чем $2n - 1$ возможностей (см. также [7, леммы 2, 3] для более общих утверждений).

§ 4. Вспомогательные факты

Следующая лемма доказана Бургейном [3]. Доказательство основано на результатах из аддитивной комбинаторики, в частности оценок сумм и произведений множеств. Эта лемма будет использована в доказательстве наших результатов о суммах Клоостермана.

ЛЕММА 1. Пусть $\gamma_1(x_1), \dots, \gamma_n(x_n)$ – неотрицательные действительные числа такие, что

$$\|\gamma_i\|_1 = \sum_{x=0}^{p-1} |\gamma_i(x)| \leq 1, \quad \|\gamma_i\|_2 = \left(\sum_{x=0}^{p-1} |\gamma_i(x)|^2 \right)^{\frac{1}{2}} < p^{-\delta}.$$

Предположим, что $\prod_{i=1}^n \|\gamma_i\|_2 < p^{-\frac{1}{2}-\delta}$, где $0 < \delta < 1/4$. Тогда имеет место оценка

$$\left| \sum_{x_1=0}^{p-1} \dots \sum_{x_n=0}^{p-1} \gamma_1(x_1) \dots \gamma_n(x_n) e_p(x_1 \dots x_n) \right| < p^{-\delta'}$$

для некоторого $\delta' > (\delta/n)^{Cn}$.

Далее будет нужна следующая лемма об оценке результатов из работы [13].

ЛЕММА 2. Пусть $N \geq 1$, $\sigma, \vartheta \in \mathbb{R}$, и пусть $m, n \geq 2$ – фиксированные целые числа. Предположим, что имеет место какое-нибудь из следующих условий: (i) $\sigma \geq 0$; (ii) $\vartheta \geq 0$; (iii) $\sigma + \vartheta \geq -1$. Пусть $P_1(Z)$ и $P_2(Z)$ – многочлены, не являющиеся константами, с целыми коэффициентами,

$$P_1(Z) = \sum_{i=0}^{m-1} a_i Z^{m-1-i}, \quad P_2(Z) = \sum_{i=0}^{n-1} b_i Z^{n-1-i},$$

такие, что для некоторого A выполняются условия

$$\begin{aligned} |a_i| &< AN^{i+\sigma}, & i = 0, \dots, m-1, \\ |b_i| &< AN^{i+\vartheta}, & i = 0, \dots, n-1. \end{aligned}$$

Тогда имеет место оценка

$$\text{Res}(P_1, P_2) \ll N^{(m-1+\sigma)(n-1+\vartheta)-\sigma\vartheta},$$

где константа в знаке $\ll$ зависит только от A, m и n .

Нам понадобятся некоторые факты из геометрии чисел. Напомним, что решетка в $\mathbb{R}^n$ – это аддитивная подгруппа $\mathbb{R}^n$, порожденная n линейно независимыми векторами. Возьмем произвольное симметричное относительно нуля выпуклое компактное тело $D \subset \mathbb{R}^n$. Для данной решетки $\Gamma \subset \mathbb{R}^n$ и $i = 1, \dots, n$ через $\lambda_i(D, \Gamma)$ обозначим i -й последовательный минимум множества D относительно решетки Γ . Напомним, что $\lambda_i(D, \Gamma)$ определяется как минимальное число λ такое, что множество λD содержит i линейно независимых векторов решетки Γ . Очевидно, что $\lambda_1(D, \Gamma) \leq \dots \leq \lambda_n(D, \Gamma)$. Будем пользоваться следующим результатом из [21, предложение 2.1] (см. также [22, упражнение 3.5.6] для более простой формы, которая, впрочем, достаточна для наших целей).

ЛЕММА 3. *Имеет место оценка*

$$|D \cap \Gamma| \leq \prod_{i=1}^n \left(\frac{2i}{\lambda_i(D, \Gamma)} + 1 \right).$$

Обозначая, как обычно, через $(2n+1)!!$ произведение всех положительных нечетных чисел, не превосходящих $2n+1$, получаем

СЛЕДСТВИЕ 3. *Имеет место оценка*

$$\prod_{i=1}^n \min\{\lambda_i(D, \Gamma), 1\} \leq \frac{(2n+1)!!}{|D \cap \Gamma|}.$$

§ 5. Уравнения со многими переменными

Следующая лемма принадлежит А. А. Карацубе [6].

ЛЕММА 4. *Имеет место оценка*

$$\left| \left\{ (x_1, \dots, x_{2k}) \in [1, N]^{2k}; \frac{1}{x_1} + \dots + \frac{1}{x_k} = \frac{1}{x_{k+1}} + \dots + \frac{1}{x_{2k}} \right\} \right| < (2k)^{80k^3} (\log N)^{4k^2} N^k.$$

Следующее элементарное утверждение будет использовано при доказательстве леммы 6 для исключения некоторых вырождающихся случаев. Рассуждение, подобное нашему доказательству этого утверждения, впервые было использовано в работе Ю. В. Линника [23, лемма 4].

ЛЕММА 5. *Пусть $c \in \mathbb{C}$, $c_1, \dots, c_r \in \mathbb{C}^*$, S – конечное подмножество в $\mathbb{C}$. Пусть T_r обозначает число решений уравнения*

$$c_1 x_1 + \dots + c_r x_r = c, \quad x_1, \dots, x_r \in S,$$

а J_{2s} – число решений уравнения

$$x_1 + \dots + x_s = x_{s+1} + \dots + x_{2s}, \quad x_1, \dots, x_{2s} \in S.$$

Если $r = 2k$ для некоторого целого k , то $T_{2k} \leq J_{2k}$. Если $r = 2k - 1$ для некоторого целого k , то $T_{2k-1}^2 \leq J_{2k-2}J_{2k}$.

ДОКАЗАТЕЛЬСТВО. Пусть $r = 2k$. Среди всех наборов $(l_1, \dots, l_{2k}, l)$ с условием

$$l_i \in \{\pm c_1, \dots, \pm c_{2k}\}, \quad l \in \{0, c\},$$

рассмотрим тот набор, для которого число решений уравнения

$$l_1x_1 + \dots + l_{2k}x_{2k} = l, \quad x_1, \dots, x_{2k} \in S, \quad (6)$$

будет максимальным. Если существуют несколько таких наборов с этим свойством, то выбираем один из наборов, для которого последовательность $l_1, \dots, l_{2k}$ содержит максимальное количество элементов из $\{-l_1, l_1\}$. Зафиксируем один такой набор $(l_1, \dots, l_{2k}, l)$ так, чтобы $l_i \in \{-l_1, l_1\}$, $i = 1, \dots, s$, и при этом либо $s = 2k$, либо $l_t \notin \{-l_1, l_1\}$ при $t > s$. Обозначим через L_{2k} число решений уравнения (6), которое перепишем в виде

$$l_1x_1 + \dots + l_kx_k = l - (l_{k+1}x_{k+1} + \dots + l_{2k}x_{2k}), \quad x_1, \dots, x_{2k} \in S.$$

Заметим, что

$$L_{2k} = \sum_{\lambda} I_1(\lambda)I_2(\lambda),$$

где $I_1(\lambda)$ – число решений уравнения $l_1x_1 + \dots + l_kx_k = \lambda$, $x_1, \dots, x_k \in S$, а $I_2(\lambda)$ – число решений уравнения $l - (l_{k+1}x_{k+1} + \dots + l_{2k}x_{2k}) = \lambda$, $x_{k+1}, \dots, x_{2k} \in S$.

Применяя неравенство Коши–Буняковского, получим

$$L_{2k}^2 \leq \left(\sum_{\lambda} I_1^2(\lambda) \right) \left(\sum_{\lambda} I_2^2(\lambda) \right).$$

Величина, содержащаяся внутри второй скобки, равна числу решений уравнения

$$l_{k+1}x_1 + \dots + l_{2k}x_k = l_{k+1}x_{k+1} + \dots + l_{2k}x_{2k}, \quad x_1, \dots, x_{2k} \in S.$$

Следовательно, из максимальнойности L_{2k} имеем

$$L_{2k} \leq \sum_{\lambda} I_1^2(\lambda).$$

Правая часть последней оценки выражает число решений уравнения

$$l_1x_1 + \dots + l_kx_k = l_1x_{k+1} + \dots + l_kx_{2k}, \quad x_1, \dots, x_{2k} \in S. \quad (7)$$

Ясно, что последовательность $l_1, \dots, l_k, l_1, \dots, l_k$ содержит $\min\{2s, 2k\}$ элементов из $\{-l_1, l_1\}$. Следовательно, по свойству максимальнойности s имеем $s = 2k$.

Таким образом, при всех i имеем $l_i \in \{-l_1, l_1\}$, откуда получаем, что число решений уравнения (7) равно J_{2k} . Поэтому $L_{2k} \leq J_{2k}$, откуда следует, что $T_{2k} \leq J_{2k}$. Это доказывает первое утверждение леммы.

Для доказательства второго утверждения леммы запишем уравнение, соответствующее величине T_{2k-1} , в виде

$$c_1 x_1 + \dots + c_k x_k = l - (c_{k+1} x_{k+1} + \dots + c_{2k-1} x_{2k-1})$$

и, как ранее, применим неравенство Коши–Буняковского. Тогда получим

$$T_{2k-1}^2 \leq \left(\sum_{\lambda} I_{11}^2(\lambda) \right) \left(\sum_{\lambda} I_{22}^2(\lambda) \right),$$

где $I_{11}(\lambda)$ – число решений уравнения $c_1 x_1 + \dots + c_k x_k = \lambda$, $x_1, \dots, x_k \in S$, а $I_{22}(\lambda)$ – число решений уравнения $-(c_{k+1} x_{k+1} + \dots + c_{2k-1} x_{2k-1}) = \lambda$, $x_{k+1}, \dots, x_{2k-1} \in S$.

Остается применить первое утверждение леммы, которое влечет

$$\sum_{\lambda} I_{11}^2(\lambda) \leq J_{2k}, \quad \sum_{\lambda} I_{22}^2(\lambda) \leq J_{2k-2},$$

что завершает доказательство леммы.

Пусть ξ – целое алгебраическое число степени d , а $O_{\mathbb{K}}$ – кольцо целых чисел поля $\mathbb{K} = \mathbb{Q}(\xi)$. Далее, при доказательстве леммы 6, будем пользоваться понятием идеалов в дедекиндовом кольце $O_{\mathbb{K}}$ (более подробно см. [24, гл. 3], [25, гл. 12]). Все рассматриваемые идеалы предполагаются целыми. В частности, мы говорим, что идеал I_2 делит I_1 , если для некоторого идеала I_3 имеет место $I_1 = I_2 I_3$.

Будем пользоваться хорошо известными свойствами идеалов. Например, если I_1 и I_2 являются идеалами и $I_1 \subset I_2$, то идеал I_2 делит I_1 (см., например, [25, предложение 12.2.7]).

Ясно, что единственность разложения идеалов на простые множители влечет, что если I_1, I_2, I_3 – идеалы в $O_{\mathbb{K}}$ такие, что I_3 делит $I_1 I_2$, то $I_3 = J_1 J_2$ для некоторых идеалов J_1 и J_2 , делящих I_1 и I_2 соответственно.

Мы будем пользоваться тем фактом, что число целых идеалов в $O_{\mathbb{K}}$ нормы n не превосходит $\tau(n)^d$, где $\tau(n)$ – число делителей n . В частности, если число d является константой, то для больших n эта величина имеет порядок $n^{o(1)}$. Заметим, что число натуральных чисел, не превосходящих $m^{O(1)}$, простые делители которых делят m , ограничено сверху величиной $m^{o(1)}$ (это легко следует, например, из основных свойств гладких чисел и распределения простых чисел).

Напомним, что *логарифмической высотой многочлена* $P \in \mathbb{Z}[Z]$ называется логарифм максимума абсолютных величин коэффициентов P . *Логарифмическая высота алгебраического числа* α определяется как логарифмическая высота его минимального многочлена. Из основных свойств меры Махлера известно, что если $P, Q \in \mathbb{Z}[Z]$ – многочлены от одной переменной, $Q \mid P$ и P имеет логарифмическую высоту, не превосходящую H , то Q имеет логарифмическую высоту, не превосходящую $H + O(1)$, где константа в знаке $O(1)$ зависит только от $\deg P$ (см., например, [26, теорема 4.2.2]).

В частности, если многочлен $P \in \mathbb{Z}[Z]$ не является константой и его коэффициенты по абсолютной величине не превосходят числа M , то каждый корень σ этого многочлена может быть представлен в виде ξ/q , где ξ – целое алгебраическое число логарифмической высоты $O(\log M)$, а q – натуральное число с условием $q < M^{O(1)}$, где константа в знаке $O(1)$ зависит только от $\deg P$.

ЛЕММА 6. *Для любой фиксированной целой положительной константы r и всех значений $\sigma \in \mathbb{C}$ величина $T_r(\sigma, N)$, равная числу решений уравнения*

$$\frac{1}{\sigma + x_1} + \cdots + \frac{1}{\sigma + x_r} = \frac{1}{\sigma + x_{r+1}} + \cdots + \frac{1}{\sigma + x_{2r}} \quad (8)$$

в натуральных числах $x_1, \dots, x_{2r} \leq N$, удовлетворяет оценке

$$T_r(a, N) < N^{r+o(1)}.$$

ДОКАЗАТЕЛЬСТВО. Для краткости обозначим $T_r = T_r(a, N)$. Докажем лемму индукцией по r . Для $r = 1$ утверждение тривиально. Пусть $r \geq 2$.

Из леммы 5 следует, что число решений с условием $x_i = x_j$ при некоторых $i \neq j$ вносит вклад в T_r величину порядка $O(\sqrt{T_{r-1}T_r})$. Значит, по индуктивному предположению достаточно доказать, что

$$T'_r < N^{r+o(1)},$$

где T'_r – число решений уравнения (8) с условием $x_i \neq x_j$ при всех $i \neq j$. Также можем предположить, что $T'_r > N^r$, так как в противном случае доказательство очевидно. Перепишем уравнение (8) в виде

$$\prod_{i \neq 1} (\sigma + x_i) + \cdots + \prod_{i \neq r} (\sigma + x_i) = \prod_{i \neq r+1} (\sigma + x_i) + \cdots + \prod_{i \neq 2r} (\sigma + x_i)$$

и рассмотрим многочлен

$$P(Z) = \prod_{i \neq 1} (Z + x_i) + \cdots + \prod_{i \neq r} (Z + x_i) - \prod_{i \neq r+1} (Z + x_i) - \cdots - \prod_{i \neq 2r} (Z + x_i).$$

Ясно, что $\deg P \leq 2r - 1$. Заметим, что $P(-x_1) \neq 0$. В частности, $P(Z)$ не равно тождественно нулю. Более того, из $P(\sigma) = 0$ следует, что многочлен $P(Z)$ не является константой. Следовательно, можем предположить, что σ является алгебраическим числом степени d для некоторого $1 \leq d \leq 2r - 1$ и имеет логарифмическую высоту $O(\log N)$. Запишем σ в виде ξ/q , где ξ – целое алгебраическое число высоты $O(\log N)$ и q – целое число, удовлетворяющее $q = N^{O(1)}$. Тогда уравнение (8) принимает форму

$$\prod_{i \neq 1} (\xi + qx_i) + \cdots + \prod_{i \neq r} (\xi + qx_i) = \prod_{i \neq r+1} (\xi + qx_i) + \cdots + \prod_{i \neq 2r} (\xi + qx_i). \quad (9)$$

Пусть $O_{\mathbb{K}}$ – кольцо целых чисел поля $\mathbb{K} = \mathbb{Q}(\xi)$. Идея состоит в использовании следующего наблюдения: для каждого $i = 1, \dots, 2r$ имеем

$$\xi + qx_i \mid q^{2r-1} \prod_{j \neq i} (x_j - x_i). \quad (10)$$

Стратегия оценки числа решений уравнения (9) состоит в последовательном введении переменных $x_1, x_2, \dots$, при этом на каждом шаге будут использоваться сравнения, которые появляются при фиксировании предыдущих переменных.

Через $\nu(I)$ обозначим норму данного идеала I . Разложим главный идеал $(\xi + qx_1)$ на множители:

$$(\xi + qx_1) = I_1 J_1,$$

где простые множители идеала I_1 делят q , а идеал J_1 взаимно прост с q . Согласно (10) норма $\nu(J_1)$ делит $\prod_{j \geq 2} (x_j - x_1)^d$. Следовательно,

$$x_j \equiv x_1 \pmod{r_j}, \quad 2 \leq j \leq 2r, \quad (11)$$

для некоторых $r_j \in \mathbb{Z}_+$ таких, что $\nu(J_1) \mid \nu_1^d$, где $\nu_1 = \prod_{j \geq 2} r_j$ и $\nu_1 \mid \nu(J_1)$. Ограничим ν_1 на диадический интервал, т. е. существует фиксированное число $\mu_1 \geq 1$ такое, что если мы ограничим величину ν_1 на интервал

$$\mu_1 \leq \nu_1 \leq 2\mu_1, \quad (12)$$

то число решений уравнения (9) с этим ограничением будет меняться не более чем в $N^{o(1)}$ раз.

Для каждого x_1 рассматриваем $N^{o(1)}$ различных случаев и в соответствии с (11) относим $x_j, j \geq 2$, в арифметические прогрессии $L_{2,j} \in [1, N]$, где, таким образом,

$$\prod_{j \geq 2} |L_{2,j}| < \frac{N^{2r-1+o(1)}}{\mu_1}. \quad (13)$$

На следующем шаге для каждого $x_2 \in L_{2,2}$ мы разлагаем $(\xi + qx_2)$ на множители:

$$(\xi + qx_2) = I_2 J_2,$$

где простые делители I_2 делят q или $\nu(\xi + qx_1)$, а идеал J_2 взаимно прост с q и $\nu(\xi + qx_1)$. Таким образом, J_2 взаимно прост с $(x_2 - x_1)$, и снова согласно (10) норма $\nu(J_2)$ делит $\prod_{j \geq 3} (x_j - x_2)^d$. Рассуждая, как и на предыдущем шаге, находим ν_2 такое, чтобы $\nu(J_2) \mid \nu_2^d$ и $\nu_2 \mid \nu(J_2)$. Как и ранее, мы можем ограничить ν_2 на диадический интервал, т. е. существует фиксированное число $\mu_2 \geq 1$ (которое, в частности, не зависит от переменных x_i) такое, что если мы ограничим ν_2 на интервал

$$\mu_2 \leq \nu_2 \leq 2\mu_2, \quad (14)$$

то число решений уравнения (9) с этим ограничением будет изменяться не более чем в $N^{o(1)}$ раз. Для каждого $x_2 \in L_{2,2}$ рассматриваем $N^{o(1)}$ возможностей и относим $x_j, j \geq 3$, в арифметические прогрессии $L_{3,j} \subset L_{2,j}$, где

$$\prod_{j \geq 3} |L_{3,j}| \leq \frac{1}{\mu_2} \prod_{j \geq 3} |L_{2,j}|, \quad \nu(J_2) \mid \nu_2^d. \quad (15)$$

Заметим, что, действительно, прогрессии $L_{2,j}$ определены по некоторым модулям $r_j \mid \nu_1$, и так как $\nu(J_1), \nu(J_2)$ являются взаимно простыми, то r_j и $\nu(J_2)$ также будут взаимно простыми.

На следующем шаге для каждого $x_3 \in L_{3,3}$ мы разлагаем $(\xi + qx_3)$ на множители:

$$(\xi + qx_3) = I_3 J_3,$$

где простые делители I_3 делят (q) , $\nu(\xi + qx_1)$ или $\nu(\xi + qx_2)$, а J_3 взаимно прост с (q) , $\nu(\xi + qx_1)$ и $\nu(\xi + qx_2)$. Так же, как и в предыдущих случаях, мы находим ν_3 из диадического интервала $\mu_3 \leq \nu_3 \leq 2\mu_3$, где μ_3 не зависит от переменных.

Продолжение процесса вполне очевидно. Мы теперь последовательно фиксируем $x_1 \leq N$, $x_2 \in L_{2,2}$, $\dots$, $x_{2r} \in L_{2r,2r}$, т. е. фиксируем x_1 и, рассматривая $N^{o(1)}$ возможностей для арифметических прогрессий $L_{2,j}$, $j \geq 3$, фиксируем $x_2 \in L_{2,2}$, затем, рассматривая $N^{o(1)}$ возможностей для арифметических прогрессий $L_{3,j}$, $j \geq 3$, фиксируем $x_3 \in L_{3,3}$ и итерируем этот процесс до тех пор, пока не зафиксируем $x_{2r} \in L_{2r,2r}$. Таким образом, мы оцениваем число решений уравнения (9) как $N^{o(1)}$ вкладов величин размера

$$N|L_{2,2}||L_{3,3}|\cdots|L_{2r,2r}|.$$

Из (13), (15) и итерационного процесса получаем

$$\begin{aligned} N^{2r-1} &\gtrsim \mu_1|L_{2,2}|\prod_{j \geq 3}|L_{2,j}| \gtrsim \mu_1\mu_2|L_{2,2}||L_{3,3}|\prod_{j \geq 4}|L_{3,j}| \gtrsim \cdots \\ &\cdots \gtrsim \mu_1 \cdots \mu_{2r-1}|L_{2,2}|\cdots|L_{2r,2r}|. \end{aligned}$$

Здесь $A \gtrsim B$ означает, что $A > BN^{o(1)}$. Таким образом, число решений уравнения (9) ограничено величиной

$$\frac{N^{2r+o(1)}}{\mu_1 \cdots \mu_{2r-1}}. \quad (16)$$

Далее, в силу нашей конструкции понятно, что $\nu(I_1) = N^{O(1)}$, а так как простые множители I_1 делят q , то число возможных значений для I_1 не превосходит величины $N^{o(1)}$. Фиксируя I_1 и обозначая через $\xi_1 = \xi, \xi_2, \dots, \xi_d$ сопряженные к ξ , получим

$$\prod_{s=1}^d (\xi_s + qx_1) = \nu(I_1)\nu(J_1).$$

Поскольку $\nu(J_1) \mid \nu_1^d$, при заданном ν_1 для $\nu(J_1)$ имеется не более чем $N^{o(1)}$ возможных значений. Таким образом, при заданном ν_1 для x_1 имеется не более чем $N^{o(1)}$ возможных значений. Отсюда следует, что в интервале (12) число возможных значений для x_1 не превосходит $N^{o(1)}\mu_1$. Далее, при фиксированном x_1 имеется не более чем $N^{o(1)}$ возможных значений для идеала I_2 и, аналогично, не более $N^{o(1)}\mu_2$ возможных значений для x_2 . Продолжая эти рассуждения, мы видим, что число возможных значений для $x_1, x_2, \dots, x_{2r-1}$ не превосходит $\mu_1\mu_2 \cdots \mu_{2r-1}N^{o(1)}$. Таким образом, число решений уравнения (9) ограничено величиной $\mu_1\mu_2 \cdots \mu_{2r-1}N^{o(1)}$. Поскольку число решений уравнения (9) также ограничено величиной (16), получаем требуемый результат.

ЛЕММА 7. Пусть $x, y, z, a_1, a_2, b_1, b_2$ – комплексные числа такие, что

$$\begin{aligned}xyz &= a_1(x + y + z) + b_1, \\xy + yz + zx &= a_2(x + y + z) + b_2.\end{aligned}$$

Тогда

$$(x^2 - a_2x + a_1)(y^2 - a_2y + a_1)(z^2 - a_2z + a_1) = (b_1 - \alpha_1b_2 - \alpha_1^3)(b_1 - \alpha_2b_2 - \alpha_2^3),$$

где

$$\alpha_1 = \frac{a_2 + \sqrt{a_2^2 - 4a_1}}{2}, \quad \alpha_2 = \frac{a_2 - \sqrt{a_2^2 - 4a_1}}{2}.$$

ДОКАЗАТЕЛЬСТВО. Действительно, поскольку $\alpha_i^2 - a_2\alpha_i + a_1 = 0$, имеем

$$(x - \alpha_i)(y - \alpha_i)(z - \alpha_i) = b_1 - \alpha_i b_2 - \alpha_i^3, \quad i = 1, 2.$$

Умножив эти равенства между собой, получим требуемое.

ЛЕММА 8. Пусть A, B – целые числа такие, что $AB \neq 0$ и $|A|, |B| < N^{O(1)}$. Тогда диофантово уравнение

$$Axy + Bx + By = 0 \tag{17}$$

имеет не более чем $N^{o(1)}$ решений в целых числах x, y , удовлетворяющих условию $|x|, |y| \leq N^{O(1)}$.

ДОКАЗАТЕЛЬСТВО. Действительно, имеем равенство

$$(Ax + B)(Ay + B) = B^2,$$

откуда утверждение следует согласно известной оценке для числа делителей.

ЛЕММА 9. Пусть a_0, b_0, u_0, v_0 – целые числа такие, что $b_0u_0v_0 \neq 0$ и

$$|a_0|, |b_0|, |u_0|, |v_0| < N^{O(1)}.$$

Предположим, что

$$\frac{u_0}{v_0} \notin \left\{ \frac{b_0}{a_0 + b_0x}; 1 \leq x \leq N \right\}.$$

Тогда для числа решений J диофантового уравнения

$$\begin{aligned}u_0(a_0 + b_0x_1)(a_0 + b_0x_2)(a_0 + b_0x_3) &= v_0b_0 \\&\times ((a_0 + b_0x_1)(a_0 + b_0x_2) + (a_0 + b_0x_2)(a_0 + b_0x_3) + (a_0 + b_0x_3)(a_0 + b_0x_1))\end{aligned}$$

в целых числах x_1, x_2, x_3 с условием $1 \leq x_i \leq N$, $a_0 + b_0x_i \neq 0$, имеет место оценка

$$J < N^{\frac{2}{3} + o(1)}.$$

ДОКАЗАТЕЛЬСТВО. Можно предположить, что $b_0 > 0$, $v_0 > 0$, $(a_0, b_0) = 1$. Заметим, что если одна из переменных x_1 , x_2 , x_3 определена, то для двух других переменных остается не более чем $N^{o(1)}$ возможных значений. Действительно, пусть x_1 уже зафиксировано. Тогда, обозначая

$$X_i = a_0 + b_0 x_i, \quad A = u_0 X_1 - v_0 b_0, \quad B = -v_0 b_0 X_1,$$

получим

$$AX_2X_3 + BX_2 + BX_3 = 0.$$

По условию леммы имеем $AB \neq 0$ и $|A|, |B| < N^{O(1)}$. Следовательно, согласно лемме 8 для X_2 , X_3 (а значит, и для x_2 , x_3) имеют место не более чем $N^{o(1)}$ возможных значений.

Обозначим

$$u'_0 = \frac{u_0}{(u_0, b_0 v_0)}, \quad \frac{b_0 v_0}{(u_0, b_0 v_0)} = w_0 \geq 1.$$

Имеем

$$\begin{aligned} u'_0(a_0 + b_0 x_1)(a_0 + b_0 x_2)(a_0 + b_0 x_3) \\ = w_0((a_0 + b_0 x_1)(a_0 + b_0 x_2) + (a_0 + b_0 x_2)(a_0 + b_0 x_3) + (a_0 + b_0 x_3)(a_0 + b_0 x_1)). \end{aligned}$$

Поскольку $(u'_0, w_0) = 1$, существует представление

$$w_0 = w_1 w_2 w_3 \quad (18)$$

такое, что

$$a_0 + b_0 x_i = w_i y_i, \quad i = 1, 2, 3, \quad (19)$$

для некоторых ненулевых целых чисел y_1 , y_2 , y_3 . В частности,

$$u'_0 y_1 y_2 y_3 = w_1 w_2 y_1 y_2 + w_2 w_3 y_2 y_3 + w_3 w_1 y_3 y_1. \quad (20)$$

Мы можем предположить, что $w_1 \geq w_2 \geq w_3 \geq 1$. Из оценки числа делителей и представления (18) следует, что имеется не более чем $N^{o(1)}$ возможных значений для w_1 , w_2 , w_3 . Зафиксируем одно такое представление. Тогда заметим, что условие $(a_0, b_0) = 1$ и равенство

$$a_0 + b_0 x_1 = w_1 y_1 \quad (21)$$

влекут $(b_0, w_1) = 1$. Следовательно, равенство (21) однозначно определяет $x_1 \pmod{w_1}$. Отсюда следует, что имеется не более чем $N^{1+o(1)} w_1^{-1} + 1$ возможных значений для x_1 . Тогда мы восстанавливаем x_2 , x_3 и получаем оценку

$$J < N^{1+o(1)} w_1^{-1} + N^{o(1)}. \quad (22)$$

Далее, из (20) и $w_1 \geq w_2 \geq w_3 \geq 1$ имеем

$$|u'_0| \min\{|y_1|, |y_2|, |y_3|\} \leq 3w_1^2.$$

Таким образом,

$$\min\{|y_1|, |y_2|, |y_3|\} \leq 3w_1^2.$$

Следовательно, для одной из переменных y_1, y_2, y_3 имеются $O(w_1^2)$ возможных значений. Поэтому согласно (19) мы можем определить одну из переменных x_1, x_2, x_3 и таким образом получить, что

$$J < w_1^2 N^{o(1)}.$$

Сравнивая эту оценку с (22), заключаем, что $J < N^{\frac{2}{3}+o(1)}$. Лемма доказана.

§ 6. Сравнения

Далее N – большой параметр, $N < p$. Приведем следующий результат из работы [2], доказательство которого основано на идеях Хиз-Брауна [27].

ЛЕММА 10. Пусть $\lambda \not\equiv 0 \pmod{p}$. Тогда для числа решений J сравнения

$$xy \equiv \lambda \pmod{p}, \quad L+1 \leq x, y \leq L+N,$$

имеет место оценка

$$J < \frac{N^{\frac{3}{2}+o(1)}}{p^{\frac{1}{2}}} + N^{o(1)}.$$

В частности, если $N < p^{\frac{1}{3}}$, то имеет место оценка $J < N^{o(1)}$.

СЛЕДСТВИЕ 4. Пусть $\lambda \not\equiv 0 \pmod{p}$. Тогда для числа решений J сравнения

$$\frac{1}{x} + \frac{1}{y} \equiv \lambda \pmod{p}, \quad L+1 \leq x, y \leq L+N,$$

имеет место оценка

$$J < \frac{N^{\frac{3}{2}+o(1)}}{p^{\frac{1}{2}}} + N^{o(1)}.$$

В частности, если $N < p^{\frac{1}{3}}$, то имеет место оценка $J < N^{o(1)}$.

ДОКАЗАТЕЛЬСТВО. Действительно, имеем

$$(x - \lambda^{-1})(y - \lambda^{-1}) \equiv \lambda^{-2} \pmod{p}.$$

Применяя лемму 10, получаем требуемое.

Следующее утверждение доказано в работе [2] (см. также [28], где аналог этого утверждения доказан для многих переменных).

ЛЕММА 11. Пусть $\lambda \not\equiv 0 \pmod{p}$ и $N < p^{\frac{1}{8}}$. Тогда для числа решений J сравнения

$$xyz \equiv \lambda \pmod{p}, \quad L+1 \leq x, y \leq L+N,$$

имеет место оценка

$$J < N^{o(1)}.$$

Следующая лемма вытекает из работы [29] (а также из леммы 10 для малых значений $|I_1||I_2|$). Заметим, что эту лемму мы применим только в случае, когда один из интервалов начинается с единицы (этот частный случай был ранее установлен в [30]).

ЛЕММА 12. Пусть I_1, I_2 – интервалы в $\mathbb{F}_p^*$ с условием $|I_1||I_2| < p$. Тогда сравнение

$$xy = zt, \quad (x, z) \in I_1 \times I_1, \quad (y, t) \in I_2 \times I_2,$$

имеет не более чем $(|I_1||I_2|)^{1+o(1)}$ решений.

Следующая лемма будет использована при доказательстве теорем 2, 3. Она приведена с явными константами для того, чтобы утверждение имело более прозрачный вид (не следует воспринимать эти константы слишком серьезно).

ЛЕММА 13. Пусть $I = \{a+1, \dots, a+N\}$ и $\lambda \not\equiv 0 \pmod{p}$, $\lambda \notin \{x^{-1} \pmod{p} : x \in I\}$. Предположим, что

$$|I| = N < 0.1p^{\frac{1}{18}}J^{\frac{2}{9}},$$

где J – число решений сравнения

$$x^{-1} + y^{-1} + z^{-1} \equiv \lambda \pmod{p}, \quad x, y, z \in I.$$

Пусть также $J > N^\varepsilon$ для некоторой малой фиксированной константы $\varepsilon > 0$, и пусть N – достаточно большое число. Тогда существуют целые числа $\Delta'_4, \Delta''_4, \Delta_3$, удовлетворяющие условиям

$$|\Delta'_4| < \frac{10^5 N^4}{J}, \quad |\Delta''_4| < \frac{10^5 N^4}{J}, \quad |\Delta_3| < \frac{10^5 N^3}{J}$$

и такие, что

$$a \equiv \frac{\Delta'_4}{\Delta_3} \pmod{p}, \quad \lambda^{-1} \equiv \frac{\Delta''_4}{\Delta_3} \pmod{p}.$$

ДОКАЗАТЕЛЬСТВО. Из условия следует, что величина J равна числу решений сравнения

$$\begin{aligned} & \lambda(a+x)(a+y)(a+z) \\ & \equiv (a+x)(a+y) + (a+y)(a+z) + (a+z)(a+x) \pmod{p} \end{aligned} \quad (23)$$

в натуральных числах $x, y, z \leq N$ с условием $(a+x)(a+y)(a+z) \not\equiv 0 \pmod{p}$.

Заметим, что по следствию 4 имеет место $J < N^{1+o(1)}$, откуда следует, что $N < p^{\frac{1}{13}}$. Перепишем сравнение (23) в виде

$$\begin{aligned} & xyz + (a - \lambda^{-1})(xy + yz + zx) \\ & + (a^2 - 2a\lambda^{-1})(x + y + z) + (a^3 - 3a^2\lambda^{-1}) \equiv 0 \pmod{p}. \end{aligned} \quad (24)$$

Фиксируя одно решение (x_0, y_0, z_0) , получим

$$\begin{aligned} & (a^2 - 2a\lambda^{-1})(x + y + z - A_0) \\ & + (a - \lambda^{-1})(xy + yz + zx - B_0) + (xyz - C_0) \equiv 0 \pmod{p}, \end{aligned} \quad (25)$$

где

$$A_0 = x_0 + y_0 + z_0, \quad B_0 = x_0y_0 + y_0z_0 + z_0x_0, \quad C_0 = x_0y_0z_0.$$

Будем пользоваться некоторыми идеями из работы [13]. Определим решетку

$$\Gamma = \{(u, v, w) \in \mathbb{Z}^3 : (a^2 - 2a\lambda^{-1})u + (a - \lambda^{-1})v + w \equiv 0 \pmod{p}\}$$

и тело

$$D = \{(u, v, w) \in \mathbb{R}^3: |u| \leq 3N, |v| \leq 3N^2, |w| \leq N^3\}.$$

Поскольку каждый фиксированный вектор

$$(x + y + z - A_0, xy + yz + zx - B_0, xyz - C_0)$$

определяет величины x, y, z с точностью до не более чем шести возможных значений, имеем

$$|D \cap \Gamma| \geq \frac{J}{6}.$$

Таким образом, по следствию 3 последовательные минимумы $\lambda_i = \lambda_i(D, \Gamma)$, $i = 1, 2, 3$, удовлетворяют неравенству

$$\prod_{i=1}^3 \min\{1, \lambda_i\} < 1000J^{-1}.$$

В частности, $\lambda_1 \leq 1$. По определению чисел λ_i имеются линейно независимые векторы

$$(u_i, v_i, w_i) \in \lambda_i D \cap \Gamma, \quad i = 1, 2, 3.$$

Рассмотрим отдельно следующие три случая.

Случай 1: $\lambda_3 \leq 1$. Тогда $\lambda_1 \lambda_2 \lambda_3 < 1000J^{-1}$. Рассмотрим определитель

$$\Delta = \det \begin{pmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \\ u_3 & v_3 & w_3 \end{pmatrix}.$$

Ясно, что $|\Delta| < 6N^6 \lambda_1 \lambda_2 \lambda_3 < 6000N^6/J < p$. Таким образом, $|\Delta| < p$. С другой стороны, из сравнения

$$(a^2 - 2a\lambda^{-1})u_i + (a - \lambda^{-1})v_i + w_i \equiv 0 \pmod{p}, \quad i = 1, 2, 3,$$

заключаем, что Δ делится на p . Следовательно, имеем равенство $\Delta = 0$, которое противоречит линейной независимости векторов (u_i, v_i, w_i) , $i = 1, 2, 3$. Значит, этот случай невозможен.

Случай 2: $\lambda_1 \leq 1, \lambda_2 > 1$. Поскольку $\lambda_2 > 1$, вектор $(x + y + z - A_0, xy + yz + zx - B_0, xyz - C_0)$ и вектор (u_1, v_1, w_1) являются линейно зависимыми. Следовательно, выполняется одно из двух следующих условий:

(i) $x + y + z - A_0 = 0$;

(ii) $xyz = \frac{w_1}{u_1}(x + y + z) + C_0 - \frac{w_1}{u_1}A_0$, $xy + yz + zx = \frac{v_1}{u_1}(x + y + z) + B_0 - \frac{v_1}{u_1}A_0$.

Если решение (x, y, z) удовлетворяет условию (i), то сравнение (24) может быть записано в виде

$$\left(x + a - \frac{1}{\lambda}\right) \left(y + a - \frac{1}{\lambda}\right) \left(z + a - \frac{1}{\lambda}\right) \equiv \lambda' \pmod{p}.$$

Поскольку $\lambda \notin I^{-1} \pmod{p}$, имеем $\lambda' \not\equiv 0 \pmod{p}$. Следовательно, по лемме 11 решения, удовлетворяющие условию (i), вносят в J вклад, не превосходящий величины $N^{o(1)}$.

Если решение (x, y, z) удовлетворяет условию (ii), то лемма 7 и оценка числа делителей влекут, что для одной из переменных x, y, z имеется не более чем $N^{o(1)}$ возможных значений. Таким образом, по следствию 4 получим, что решения, удовлетворяющие условию (ii), вносят в J вклад, не превосходящий величины $N^{o(1)}$.

Таким образом, получаем неравенство $J < N^{o(1)}$, которое противоречит предположению $J > N^\varepsilon$. Следовательно, этот случай невозможен.

Случай 3: $\lambda_1 \leq 1, \lambda_2 \leq 1, \lambda_3 > 1$. Тогда $\lambda_1 \lambda_2 < 1000J^{-1}$. Далее,

$$\begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \begin{pmatrix} a^2 - 2a\lambda^{-1} \\ a - \lambda^{-1} \end{pmatrix} \equiv \begin{pmatrix} -w_1 \\ -w_2 \end{pmatrix} \pmod{p}. \quad (26)$$

Пусть

$$\Delta_3 = \det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}, \quad \Delta_5 = \det \begin{pmatrix} -w_1 & v_1 \\ -w_2 & v_2 \end{pmatrix}, \quad \Delta_4 = \det \begin{pmatrix} u_1 & -w_1 \\ u_2 & -w_2 \end{pmatrix}.$$

Имеем

$$|\Delta_3| < \frac{2000N^3}{J}, \quad |\Delta_5| < \frac{2000N^5}{J}, \quad |\Delta_4| < \frac{2000N^4}{J}. \quad (27)$$

Заметим, что

$$\Delta_3 \not\equiv 0 \pmod{p}. \quad (28)$$

Действительно, предполагая противное, из сравнения (26) получим

$$\Delta_3 \equiv \Delta_5 \equiv \Delta_4 \equiv 0 \pmod{p}.$$

Учитывая неравенства (27), получим $\Delta_3 = \Delta_5 = \Delta_4 = 0$. Однако тогда ранг матрицы

$$\begin{pmatrix} u_1 & v_1 & w_1 \\ u_2 & v_2 & w_2 \end{pmatrix}$$

будет строго меньше чем 2, что противоречит линейной независимости векторов (u_i, v_i, w_i) , $i = 1, 2$. Таким образом, выполняется условие (28). Поэтому

$$a^2 - 2a\lambda^{-1} \equiv \frac{\Delta_5}{\Delta_3} \pmod{p}, \quad a - \lambda^{-1} \equiv \frac{\Delta_4}{\Delta_3} \pmod{p}. \quad (29)$$

Используя (24), мы также получим

$$a^3 - 3a^2\lambda^{-1} \equiv \frac{\Delta_6}{\Delta_3} \pmod{p} \quad (30)$$

для некоторого целого числа Δ_6 с условием $|\Delta_6| < 6000N^6/J$. Имеем

$$\lambda^{-2} \equiv \frac{\Delta_4^2}{\Delta_3^2} - \frac{\Delta_5}{\Delta_3} \equiv \frac{\Delta_4^2 - \Delta_5\Delta_3}{\Delta_3^2} \pmod{p}. \quad (31)$$

Далее, заменяя $\lambda^{-1} \equiv a - (\Delta_4/\Delta_3) \pmod{p}$ в первом сравнении из (29) и в тождестве (30), получим

$$\Delta_3 a^2 - 2\Delta_4 a + \Delta_5 \equiv 0 \pmod{p}, \quad 2\Delta_3 a^3 - 3\Delta_4 a^2 + \Delta_6 \equiv 0 \pmod{p}.$$

Отсюда следует, что

$$\Delta_4 a^2 - 2\Delta_5 a + \Delta_6 \equiv 0 \pmod{p}.$$

Рассмотрим многочлены

$$P(Z) = \Delta_4 Z^2 - 2\Delta_5 Z + \Delta_6, \quad Q(Z) = \Delta_3 Z^2 - 2\Delta_4 Z + \Delta_5.$$

Поскольку $P(a) \equiv Q(a) \equiv 0 \pmod{p}$, получим $\text{Res}(P, Q) \equiv 0 \pmod{p}$. С другой стороны,

$$|\text{Res}(P, Q)| < \frac{10^{18} N^{18}}{J^4} < p.$$

Таким образом, имеем

$$\text{Res}(P, Q) = 0,$$

но тогда многочлены $P(Z)$ и $Q(Z)$ имеют общий корень. Если $Q(Z)$ является неприводимым в $\mathbb{Q}[Z]$, то $Q(Z)$ и $P(Z)$ будут линейно зависимыми, что влечет

$$\Delta_4^2 = \Delta_5 \Delta_3.$$

Ввиду (31) это невозможно. Следовательно, $Q(Z)$ является приводимым в $\mathbb{Q}[Z]$, и его дискриминант является квадратом целого числа. Таким образом,

$$\Delta_4^2 - \Delta_5 \Delta_3 = m^2, \quad m \in \mathbb{Z}_+.$$

Тогда получим, что $m < 10^4 N^4 / J$. Далее,

$$\lambda^{-2} \equiv \frac{m^2}{\Delta_3^2} \pmod{p}.$$

Следовательно,

$$\lambda^{-1} \equiv \frac{\Delta_4''}{\Delta_3} \pmod{p}, \quad |\Delta_4''| = m < \frac{10^4 N^4}{J}.$$

Вследствие этого также имеем

$$a \equiv \frac{\Delta_4}{\Delta_3} + \lambda^{-1} \equiv \frac{\Delta_4'}{\Delta_3} \pmod{p}, \quad |\Delta_4'| < \frac{10^5 N^4}{J}.$$

Лемма доказана.

§ 7. Доказательство теорем 1–6

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1. Пусть $I = [a + 1, a + N]$. Сначала рассмотрим случай $N < p^{\frac{k+1}{2k}}$. В этом случае нашей целью является доказательство оценки

$$J_{2k} < N^{\frac{2k^2}{k+1} + o(1)}.$$

Положим

$$V = [N^{\frac{k-1}{k+1}}], \quad Y = [N^{\frac{2}{k+1}}], \quad I_1 = [a + 1, a + 2N].$$

Определим подмножество $\mathcal{V} \subset [0.5V, V]$ следующим образом. Для данного $v \in [0.5V, V]$ рассмотрим функцию $\eta_v: I_1 \rightarrow \mathbb{Z}_+$, которая определяется равенством

$$\eta_v(u') = |\{(u'_1, v_1) \in I_1 \times [0.5V, V]; u'v_1 \equiv u'_1v \pmod{p}\}|.$$

По лемме 12 имеем

$$\sum_{u' \in I_1} \sum_{v \in [0.5V, V]} \eta_v(u') < N^{1+o(1)}V.$$

Следовательно, существует подмножество $\mathcal{V} \subset [0.5V, V]$ мощности $|\mathcal{V}| \sim V$ такое, что

$$\sum_{u' \in I_1} \eta_v(u') < N^{1+o(1)} \quad \forall v \in \mathcal{V}. \quad (32)$$

При любых фиксированных целых числах $y_i \in \mathcal{Y} = [0.5Y, Y]$ и $v \in \mathcal{V}$ величина J_{2k} не превосходит количества решений сравнения

$$\frac{1}{u'_1 - vy_1} + \cdots + \frac{1}{u'_k - vy_k} \equiv \frac{1}{u'_{k+1} - vy_{k+1}} + \cdots + \frac{1}{u'_{2k} - vy_{2k}} \pmod{p}$$

в целых числах $u'_i \in I_1$. Таким образом, получим

$$Y^{2k}VJ_{2k} \ll \frac{1}{p} \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \left| \sum_{u' \in I_1} \sum_{y \in \mathcal{Y}} e_p(n(u' - vy)^{-1}) \right|^{2k}. \quad (33)$$

Для $v \in \mathcal{V}$ и числа B вида $B = 2^s < N$ обозначим

$$S_{v,B} = \{u' \in I_1; 0.5B \leq \eta_v(u') < B\}.$$

В частности, $I_1 = \bigcup_B S_{v,B}$, а так как $v \in \mathcal{V}$, то из (32) получим

$$|S_{v,B}| < \frac{N^{1+o(1)}}{B}. \quad (34)$$

Из (33) имеем

$$Y^{2k}VJ_{2k} \ll \frac{N^{o(1)}}{p} \sum_B \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \left(\sum_{u' \in S_{v,B}} \left| \sum_{y \in \mathcal{Y}} e_p(n(u' - vy)^{-1}) \right| \right)^{2k}.$$

Поэтому согласно неравенству Гёльдера и (34) получим, что для некоторого фиксированного B имеет место оценка

$$Y^{2k}VJ_{2k} \ll \frac{N^{o(1)}}{p} \left(\frac{N}{B} \right)^{2k-1} \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \sum_{u' \in S_{v,B}} \left| \sum_{y \in \mathcal{Y}} e_p(n(u' - vy)^{-1}) \right|^{2k}. \quad (35)$$

Величина

$$\frac{1}{p} \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \sum_{u' \in S_{v,B}} \left| \sum_{y \in \mathcal{Y}} e_p(n(u' - vy)^{-1}) \right|^{2k}$$

ограничена числом решений сравнения

$$\frac{1}{u' - vy_1} + \cdots + \frac{1}{u' - vy_k} \equiv \frac{1}{u' - vy_{k+1}} + \cdots + \frac{1}{u' - vy_{2k}} \pmod{p}$$

в переменных $v \in \mathcal{V}$, $u' \in S_{v,B}$, $y \in \mathcal{Y}$. Таким образом, получаем оценку

$$\frac{1}{p} \sum_{n=0}^{p-1} \sum_{v \in \mathcal{V}} \sum_{u' \in S_{v,B}} \left| \sum_{y \in \mathcal{Y}} e_p(n(u' - vy)^{-1}) \right|^{2k} \ll Y^k V \frac{N^{1+o(1)}}{B} + Y^{2k} B.$$

Поэтому из (35) получим

$$Y^{2k} V J_{2k} \ll N^{2k-1+o(1)} B^{-2k+1} \left(Y^k V \frac{N^{1+o(1)}}{B} + Y^{2k} B \right).$$

Значит,

$$J_{2k} < N^{2k+o(1)} Y^{-k} + \frac{N^{2k-1+o(1)}}{V} < N^{\frac{2k^2}{k+1}+o(1)},$$

откуда следует требуемое в случае $N < p^{\frac{k+1}{2k}}$.

Пусть теперь $N > p^{\frac{k+1}{2k}}$. Разобьем интервал $I = [a+1, a+N]$ на $K \sim Np^{-\frac{k+1}{2k}}$ подынтервалов длин, не превосходящих $N_1 = p^{\frac{k+1}{2k}}$. Тогда для некоторых интервалов $I^{(1)}, \dots, I^{(2k)}$ длин, не превосходящих N_1 , выполняется оценка

$$J_{2k} < K^{2k} R_{2k} \ll \left(\frac{N}{p^{\frac{k+1}{2k}}} \right)^{2k} R_{2k},$$

где R_{2k} – число решений сравнения

$$\frac{1}{x_1} + \cdots + \frac{1}{x_k} \equiv \frac{1}{x_{k+1}} + \cdots + \frac{1}{x_{2k}} \pmod{p}, \quad x_i \in I^{(i)}, \quad i = 1, \dots, 2k.$$

Выражая R_{2k} в терминах экспоненциальных сумм и применяя неравенство Гёльдера, получим

$$R_{2k} \leq \prod_{i=1}^{2k} (R_{2k}(i))^{\frac{1}{2k}},$$

где $R_{2k}(i)$ – число решений сравнения

$$\frac{1}{x_1} + \cdots + \frac{1}{x_k} \equiv \frac{1}{x_{k+1}} + \cdots + \frac{1}{x_{2k}} \pmod{p}, \quad x_1, \dots, x_{2k} \in I^{(i)}.$$

Таким образом, для некоторого фиксированного $i = i_0$ имеет место оценка

$$R_{2k} \leq R_{2k}(i_0).$$

Поскольку $|I^{(i_0)}| \leq N_1 = p^{\frac{k+1}{2k}}$, по уже доказанному известно, что

$$R_{2k}(i_0) < N_1^{\frac{2k^2}{k+1}+o(1)} = p^k N^{o(1)}.$$

Следовательно, имеем

$$J_{2k} < \left(\frac{N}{p^{\frac{k+1}{2k}}} \right)^{2k} p^k N^{o(1)} = \frac{N^{2k+o(1)}}{p},$$

что завершает доказательство теоремы.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2. Пусть $I = \{a + 1, \dots, a + N\}$. Можно предположить, что N – большое число и $J > N^{\frac{2}{3}} \log N$, так как в противном случае доказательство очевидно. Условия леммы 13 выполняются, поэтому существуют целые числа $\Delta'_4, \Delta''_4, \Delta_3$ с условием

$$|\Delta'_4| < N^{\frac{10}{3}}, \quad |\Delta''_4| < N^{\frac{10}{3}}, \quad |\Delta_3| < N^{\frac{7}{3}} \quad (36)$$

такие, что

$$a \equiv \frac{\Delta'_4}{\Delta_3} \pmod{p}, \quad \lambda^{-1} \equiv \frac{\Delta''_4}{\Delta_3} \pmod{p}. \quad (37)$$

Учитывая (36), (37) в сравнении

$$\begin{aligned} \lambda(a+x)(a+y)(a+z) \\ \equiv (a+x)(a+y) + (a+y)(a+z) + (a+z)(a+x) \pmod{p}, \end{aligned}$$

получим

$$\begin{aligned} (\Delta'_4 + \Delta_3 x)(\Delta'_4 + \Delta_3 y)(\Delta'_4 + \Delta_3 z) &\equiv \Delta''_4 \{ (\Delta'_4 + \Delta_3 x)(\Delta'_4 + \Delta_3 y) \\ &+ (\Delta'_4 + \Delta_3 y)(\Delta'_4 + \Delta_3 z) + (\Delta'_4 + \Delta_3 z)(\Delta'_4 + \Delta_3 x) \} \pmod{p}. \end{aligned}$$

Левая и правая части последнего сравнения имеют порядок $O(N^{10}) = o(p)$. Таким образом, это сравнение превращается в равенство

$$\begin{aligned} (\Delta'_4 + \Delta_3 x)(\Delta'_4 + \Delta_3 y)(\Delta'_4 + \Delta_3 z) &= \Delta''_4 \{ (\Delta'_4 + \Delta_3 x)(\Delta'_4 + \Delta_3 y) \\ &+ (\Delta'_4 + \Delta_3 y)(\Delta'_4 + \Delta_3 z) + (\Delta'_4 + \Delta_3 z)(\Delta'_4 + \Delta_3 x) \}, \end{aligned}$$

и утверждение следует из леммы 9.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 3. Пусть $I = \{a + 1, \dots, a + N\}$. Утверждение теоремы эквивалентно тому, что для любого $\varepsilon > 0$ имеет место оценка

$$J_6 \ll N^{3+\varepsilon},$$

где постоянная в знаке $\ll$ может зависеть только от ε .

Заметим, что для любого $j \in \mathbb{Z}$ существуют $u_j, v_j \in \mathbb{Z}$ такие, что

$$\frac{u_j}{v_j} \equiv j \pmod{p}, \quad |u_j| \leq p^{\frac{1}{2}}, \quad 0 < |v_j| \leq p^{\frac{1}{2}}. \quad (38)$$

Это следует из того, что среди более чем p чисел $u + jv$, $0 \leq u, v \leq [p^{\frac{1}{2}}]$, найдутся хотя бы два сравнимые между собой по модулю p числа. В таком виде мы также представим число a , т. е.

$$a \equiv \frac{a_0}{b_0} \pmod{p}, \quad |a_0| \leq p^{\frac{1}{2}}, \quad 0 < |b_0| \leq p^{\frac{1}{2}}. \quad (39)$$

Пусть T_j – число решений сравнения

$$\frac{1}{a+x_1} + \frac{1}{a+x_2} + \frac{1}{a+x_3} \equiv j \pmod{p}, \quad 1 \leq x_1, x_2, x_3 \leq N.$$

Имеем

$$J_6 = \sum_{j=0}^{p-1} T_j^2, \quad \sum_{j=0}^{p-1} T_j \leq N^3.$$

Из следствия 4 вытекает, что $T_j < N^{1+o(1)}$. Следовательно, вкладом в J_6 , исходящим от всех $j \in \{I^{-1} \cup 0\} \pmod{p}$, будет

$$\sum_{\substack{0 \leq j \leq p-1 \\ j \in I^{-1} \cup 0 \pmod{p}}} T_j^2 \leq (N+1) \max_j T_j^2 < N^{3+o(1)}.$$

Далее, вклад в J_6 , исходящий из тех j , для которых $T_j < N^{0.1\varepsilon}$, меньше, чем

$$N^{0.1\varepsilon} \sum_{j=0}^{p-1} T_j \leq N^{3+0.1\varepsilon}.$$

Таким образом, если мы обозначим через Ω множество целых чисел j с условием

$$1 \leq j \leq p-1, \quad j \notin I^{-1} \pmod{p}, \quad |T_j| > N^{0.1\varepsilon},$$

то

$$J_6 < N^{3+0.2\varepsilon} + \sum_{j \in \Omega} T_j^2. \quad (40)$$

Теперь для каждого j применим лемму 13 (где J заменяется на T_j , а λ – на j). Тогда существуют числа Δ'_{4j} , Δ''_{4j} , Δ_{3j} с условиями

$$\Delta'_{4j} \ll N^4, \quad \Delta''_{4j} \ll N^4, \quad \Delta_{3j} \ll N^3$$

такие, что

$$a \equiv \frac{\Delta'_{4j}}{\Delta_{3j}} \pmod{p}, \quad j^{-1} \equiv \frac{\Delta''_{4j}}{\Delta_{3j}} \pmod{p}.$$

Сравнивая последнее с (38) и (39), видим, что

$$a \equiv \frac{a_0}{b_0} \equiv \frac{\Delta'_{4j}}{\Delta_{3j}} \pmod{p}, \quad j^{-1} \equiv \frac{v_j}{u_j} \equiv \frac{\Delta''_{4j}}{\Delta_{3j}} \pmod{p}. \quad (41)$$

Принимая во внимание неравенства, которым подчиняются N , a_0 , b_0 , u_j , v_j , получим, что имеют место равенства

$$\frac{a_0}{b_0} = \frac{\Delta'_{4j}}{\Delta_{3j}}, \quad \frac{v_j}{u_j} = \frac{\Delta''_{4j}}{\Delta_{3j}}. \quad (42)$$

Теперь представим соответствующее T_j сравнение в виде

$$\begin{aligned} x_1 x_2 x_3 + (a - j^{-1})(x_1 x_2 + x_2 x_3 + x_3 x_1) \\ + (a^2 - 2a j^{-1})(x_1 + x_2 + x_3) + (a^3 - 3a^2 j^{-1}) \equiv 0 \pmod{p}. \end{aligned}$$

Используя (41), заменим a и j^{-1} и получим, что

$$\begin{aligned} x_1 x_2 x_3 + \left(\frac{\Delta'_{4j}}{\Delta_{3j}} - \frac{\Delta''_{4j}}{\Delta_{3j}} \right) (x_1 x_2 + x_2 x_3 + x_3 x_1) \\ + \left(\left(\frac{\Delta'_{4j}}{\Delta_{3j}} \right)^2 - 2 \frac{\Delta'_{4j}}{\Delta_{3j}} \frac{\Delta''_{4j}}{\Delta_{3j}} \right) (x_1 + x_2 + x_3) \\ + \left(\left(\frac{\Delta'_{4j}}{\Delta_{3j}} \right)^3 - 3 \left(\frac{\Delta'_{4j}}{\Delta_{3j}} \right)^2 \frac{\Delta''_{4j}}{\Delta_{3j}} \right) \equiv 0 \pmod{p}. \end{aligned}$$

После умножения последнего сравнения на Δ_{3j}^3 левая часть будет целым числом порядка $O(N^{12}) = o(p)$. В результате этого полученное сравнение преобразуется в равенство, а после деления на Δ_{3j}^3 получим

$$\begin{aligned} x_1 x_2 x_3 + \left(\frac{\Delta'_{4j}}{\Delta_{3j}} - \frac{\Delta''_{4j}}{\Delta_{3j}} \right) (x_1 x_2 + x_2 x_3 + x_3 x_1) \\ + \left(\left(\frac{\Delta'_{4j}}{\Delta_{3j}} \right)^2 - 2 \frac{\Delta'_{4j}}{\Delta_{3j}} \frac{\Delta''_{4j}}{\Delta_{3j}} \right) (x_1 + x_2 + x_3) \\ + \left(\left(\frac{\Delta'_{4j}}{\Delta_{3j}} \right)^3 - 3 \left(\frac{\Delta'_{4j}}{\Delta_{3j}} \right)^2 \frac{\Delta''_{4j}}{\Delta_{3j}} \right) = 0. \end{aligned}$$

Используя (42), перепишем последнее равенство в виде

$$\begin{aligned} x_1 x_2 x_3 + \left(\frac{a_0}{b_0} - \frac{v_j}{u_j} \right) (x_1 x_2 + x_2 x_3 + x_3 x_1) \\ + \left(\frac{a_0^2}{b_0^2} - 2 \frac{a_0}{b_0} \frac{v_j}{u_j} \right) (x_1 + x_2 + x_3) + \left(\frac{a_0^3}{b_0^3} - 3 \frac{a_0^2}{b_0^2} \frac{v_j}{u_j} \right) = 0. \end{aligned}$$

В результате получим

$$\frac{1}{(a_0/b_0) + x_1} + \frac{1}{(a_0/b_0) + x_2} + \frac{1}{(a_0/b_0) + x_3} = \frac{u_j}{v_j}. \quad (43)$$

Таким образом, для $j \in \Omega$ величина T_j будет равна числу решений диофантового уравнения (43) в натуральных числах $x_1, x_2, x_3 \leq N$. Поскольку u_j/v_j являются попарно различными, получим, что величина $\sum_{j \in \Omega} T_j^2$ не превосходит числа решений уравнения

$$\begin{aligned} \frac{1}{(a_0/b_0) + x_1} + \frac{1}{(a_0/b_0) + x_2} + \frac{1}{(a_0/b_0) + x_3} \\ = \frac{1}{(a_0/b_0) + x_4} + \frac{1}{(a_0/b_0) + x_5} + \frac{1}{(a_0/b_0) + x_6} \end{aligned}$$

в натуральных числах $x_1, \dots, x_6 \leq N$. Поэтому из леммы 6 следует, что

$$\sum_{j \in \Omega} T_j^2 < N^{3+o(1)}.$$

Полученная оценка вместе с (40) завершает доказательство теоремы.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 4. Пусть $I = \{a + 1, \dots, a + N\}$. Из стандартных аргументов с привлечением неравенства Гёльдера (в силу индукции) легко следует, что для доказательства достаточно показать ограниченность вклада от множества решений с попарно различными $x_1, \dots, x_{2k}$ величиной $N^{k+o(1)}$. Итак, далее предполагаем, что $x_1, \dots, x_{2k}$ являются попарно различными.

Для каждого решения $\vec{x} = (x_1, \dots, x_{2k})$ рассмотрим многочлен

$$P_{\vec{x}}(Z) = \prod_{i \neq 1} (Z + x_i) + \dots + \prod_{i \neq k} (Z + x_i) - \prod_{i \neq k+1} (Z + x_i) - \dots - \prod_{i \neq 2k} (Z + x_i).$$

Ясно, что $\deg P_{\vec{x}}(Z) \leq 2k - 2$. Заметим, что $P_{\vec{x}}(-x_1) \neq 0$. В частности, многочлен $P_{\vec{x}}(Z)$ не равен тождественно нулю, а так как $P_{\vec{x}}(a) \equiv 0 \pmod{p}$, то этот многочлен не является константой. Ясно, что $P_{\vec{x}}(Z)$ имеет вид

$$P_{\vec{x}}(Z) = \sum_{i=0}^{2k-2} a_i Z^{2k-2-i},$$

где $|a_i| \ll N^{i+1}$. Зафиксируем одно решение

$$(x_1, \dots, x_{2k}) = (c_1, \dots, c_{2k})$$

и рассмотрим соответствующий решению $\vec{c} = (c_1, \dots, c_{2k})$ многочлен $P_{\vec{c}}(Z)$. Поскольку

$$P_{\vec{x}}(a) \equiv P_{\vec{c}}(a) \equiv 0 \pmod{p},$$

имеем

$$\text{Res}(P_{\vec{x}}(Z), P_{\vec{c}}(Z)) \equiv 0 \pmod{p}.$$

С другой стороны, многочлены $P_{\vec{x}}(Z)$ и $P_{\vec{c}}(Z)$ удовлетворяют условию леммы 2 при

$$\sigma = \theta = 1, \quad m = n = 2k - 1,$$

поэтому

$$\text{Res}(P_{\vec{x}}(Z), P_{\vec{c}}(Z)) \ll N^{4k^2 - 4k}.$$

Следовательно, предполагая, что $N < p^{\frac{1}{4k^2}}$, получим

$$|\text{Res}(P_{\vec{x}}(Z), P_{\vec{c}}(Z))| < p,$$

откуда имеем

$$\text{Res}(P_{\vec{x}}(Z), P_{\vec{c}}(Z)) = 0.$$

Таким образом, для каждого решения $\vec{x} = (x_1, \dots, x_{2k})$ многочлен $P_{\vec{x}}(Z)$ имеет общий корень с многочленом $P_{\vec{c}}(Z)$. Поскольку x_i являются попарно различными, условие $P_{\vec{x}}(\sigma) = 0$ влечет, что $x_i + \sigma \neq 0$. Тогда из леммы 6 следует, что при каждом фиксированном корне σ многочлена $P_{\vec{c}}(Z)$ уравнение $P_{\vec{x}}(\sigma) = 0$ имеет не более чем $N^{k+o(1)}$ решений в натуральных числах $x_i \leq N$. Теорема доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 5. Достаточно рассмотреть случай $kN^{k-1} < p$, так как иначе утверждение становится тривиальным. Для $\lambda = 0, 1, \dots, p-1$ обозначим

$$J(\lambda) = \{(x_1, \dots, x_k) \in I^k; x_1^* + \dots + x_k^* \equiv \lambda \pmod{p}\}.$$

Пусть $\Omega = \{\lambda \in [1, p-1]; |J(\lambda)| \geq 1\}$. Поскольку $J(0) = 0$, имеем

$$J_{2k} = \sum_{\lambda \in \Omega} |J(\lambda)|^2.$$

Рассмотрим решетку

$$\Gamma_\lambda = \{(u, v) \in \mathbb{Z}^2; \lambda u \equiv v \pmod{p}\}$$

и тело

$$D = \{(u, v) \in \mathbb{R}^2; |u| \leq N^k, |v| \leq kN^{k-1}\}.$$

Обозначая через μ_1, μ_2 последовательные минимумы тела D по отношению к решетке Γ_λ , по следствию 3 получим

$$\prod_{i=1}^2 \min\{\mu_i, 1\} \leq \frac{15}{|\Gamma_\lambda \cap D|}.$$

Заметим, что для $(x_1, \dots, x_k) \in J(\lambda)$ имеет место сравнение

$$\lambda x_1 \cdots x_k \equiv x_2 \cdots x_k + \dots + x_1 \cdots x_{k-1} \pmod{p},$$

откуда

$$(x_1 \cdots x_k, x_2 \cdots x_k + \dots + x_1 \cdots x_{k-1}) \in \Gamma_\lambda \cap D.$$

Таким образом, для $\lambda \in \Omega$ мы имеем $\mu_1 \leq 1$. Разобьем множество Ω на два подмножества:

$$\Omega' = \{\lambda \in \Omega; \mu_2 \leq 1\}, \quad \Omega'' = \{\lambda \in \Omega; \mu_2 > 1\}.$$

Имеем

$$J_{2k} = \sum_{\lambda \in \Omega'} |J(\lambda)|^2 + \sum_{\lambda \in \Omega''} |J(\lambda)|^2. \quad (44)$$

Случай 1: $\lambda \in \Omega'$, т.е. $\mu_2 \leq 1$. Пусть $(u_i, v_i) \in \mu_i D \cap \Gamma_\lambda$, $i = 1, 2$, являются линейно независимыми. Тогда

$$0 \neq \det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \equiv 0 \pmod{p},$$

откуда имеем

$$\left| \det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \right| \geq p,$$

и также получим

$$\left| \det \begin{pmatrix} u_1 & v_1 \\ u_2 & v_2 \end{pmatrix} \right| \leq 2k\mu_1\mu_2 N^{2k-1} \leq \frac{30kN^{2k-1}}{|\Gamma_\lambda \cap D|}.$$

Таким образом, при $\lambda \in \Omega'$ величина $|\Gamma_\lambda \cap D|$, равная числу решений сравнения

$$\lambda u \equiv v \pmod{p}$$

в целых числах u, v с условиями $|u| \leq N^k, |v| \leq kN^{k-1}$, ограничена величиной

$$|\Gamma_\lambda \cap D| \leq \frac{30kN^{2k-1}}{p}. \quad (45)$$

Следовательно, если обозначим через $S(u, v)$ множество наборов $(x_1, \dots, x_k)$ натуральных чисел $x_1, \dots, x_k \leq N$ с условиями

$$x_1 \cdots x_k = u, \quad x_2 \cdots x_k + \cdots + x_1 \cdots x_{k-1} = v,$$

то получим, что

$$\sum_{\lambda \in \Omega'} |J(\lambda)|^2 = \sum_{\lambda \in \Omega'} \left(\sum_{(u,v) \in \Gamma_\lambda \cap D} \sum_{(x_1, \dots, x_k) \in S(u,v)} 1 \right)^2.$$

Применяя неравенство Коши–Буняковского и учитывая (45), получим

$$\sum_{\lambda \in \Omega'} |J(\lambda)|^2 \leq \frac{30kN^{2k-1}}{p} \sum_{\lambda \in \Omega'} \sum_{(u,v) \in \Gamma_\lambda \cap D} \left(\sum_{(x_1, \dots, x_k) \in S(u,v)} 1 \right)^2.$$

Величина в правой части последнего неравенства, очевидно, ограничена числом решений системы уравнений

$$\begin{aligned} x_1 \cdots x_k &= y_1 \cdots y_k, \\ x_1 \cdots x_{k-1} + \cdots + x_2 \cdots x_k &= y_2 \cdots y_k + \cdots + y_1 \cdots y_{k-1} \end{aligned}$$

в натуральных числах $x_i, y_j \leq N$. Следовательно, из леммы 4 вытекает, что

$$\sum_{\lambda \in \Omega'} |J(\lambda)|^2 < 30k(2k)^{80k^3} (\log N)^{4k^2} \frac{N^{3k-1}}{p}. \quad (46)$$

Случай 2: $\lambda \in \Omega''$, т.е. $\mu_2 > 1$. Тогда векторы в $\Gamma_\lambda \cap D$ будут линейно зависимыми и, в частности, существует число $\hat{\lambda} \in \mathbb{Q}$ такое, что $\hat{\lambda}x_1 \cdots x_k = x_2 \cdots x_k + \cdots + x_1 \cdots x_{k-1}$ при $(x_1, \dots, x_k) \in J(\lambda)$. Таким образом, имеем

$$\begin{aligned} \sum_{\lambda \in \Omega''} |J(\lambda)|^2 &\leq \sum_{\hat{\lambda} \in \mathbb{Q}} \left| \left\{ (x_1, \dots, x_k) \in I^k; \frac{1}{x_1} + \cdots + \frac{1}{x_k} = \hat{\lambda} \right\} \right|^2 \\ &= \left| \left\{ (x_1, \dots, x_{2k}) \in [1, N]^{2k}; \frac{1}{x_1} + \cdots + \frac{1}{x_k} = \frac{1}{x_{k+1}} + \cdots + \frac{1}{x_{2k}} \right\} \right| \\ &< (2k)^{80k^3} (\log N)^{4k^2} N^k. \end{aligned}$$

Учитывая последнее и оценку (46) в (44), получим

$$J_{2k} < (2k)^{90k^3} (\log N)^{4k^2} \left(\frac{N^{2k-1}}{p} + 1 \right) N^k.$$

Теорема доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 6 проводим по той же схеме, единственное отличие состоит в том, что вместо леммы 4 следует применять оценку

$$\left| \left\{ (x_1, \dots, x_{2k}) \in ([1, N] \cap \mathcal{P})^{2k}; \frac{1}{x_1} + \dots + \frac{1}{x_k} = \frac{1}{x_{k+1}} + \dots + \frac{1}{x_{2k}} \right\} \right| < (2k)^k \left(\frac{N}{\log N} \right)^k.$$

Теорема доказана.

§ 8. Доказательство теорем 7–14

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 7. Достаточно установить утверждение в случае $|I_1| = [p^{\frac{1}{18}}]$, $|I_2| = [p^{\frac{5}{12} + \varepsilon}]$ и $0 < \varepsilon < 0.1$. Пусть

$$W_2 = \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1) \alpha_2(x_2) e_p(ax_1^* x_2^*).$$

Полагая $k = [1/\varepsilon]$ и применяя неравенство Гёльдера, получим

$$\begin{aligned} |W_2|^k &\leq |I_1|^{k-1} \sum_{x_1 \in I_1} \left| \sum_{x_2 \in I_2} \alpha_2(x_2) e_p(ax_1^* x_2^*) \right|^k \\ &= |I_1|^{k-1} \sum_{x_1 \in I_1} \left| \sum_{y_1, \dots, y_k \in I_2} \alpha_2(y_1) \cdots \alpha_2(y_k) e_p(ax_1^* (y_1^* + \dots + y_k^*)) \right| \\ &= |I_1|^{k-1} \sum_{x_1 \in I_1} \theta(x_1) \left(\sum_{y_1, \dots, y_k \in I_2} \alpha_2(y_1) \cdots \alpha_2(y_k) e_p(ax_1^* (y_1^* + \dots + y_k^*)) \right) \\ &\leq |I_1|^{k-1} \sum_{y_1, \dots, y_k \in I_2} \left| \sum_{x_1 \in I_1} \theta(x_1) e_p(ax_1^* (y_1^* + \dots + y_k^*)) \right|, \end{aligned}$$

где $\theta(x)$ – комплексные числа с условием $|\theta(x)| \leq 1$. Снова применяя неравенство Гёльдера, получим

$$\begin{aligned} |W_2|^{3k} &\leq |I_1|^{3k-3} |I_2|^{2k} \sum_{y_1, \dots, y_k \in I_2} \left| \sum_{x_1 \in I_1} \theta(x_1) e_p(ax_1^* (y_1^* + \dots + y_k^*)) \right|^3 \\ &= |I_1|^{3k-3} |I_2|^{2k} \sum_{\lambda=0}^{p-1} T(\lambda) \left| \sum_{x_1 \in I_1} \theta(x_1) e_p(ax_1^* \lambda) \right|^3, \end{aligned}$$

где $T(\lambda)$ – число решений сравнения

$$y_1^* + \dots + y_k^* \equiv \lambda \pmod{p}, \quad y_i \in I_2.$$

Применяя неравенство Коши–Буняковского, получим

$$|W_2|^{6k} \leq |I_1|^{6k-6} |I_2|^{4k} \left(\sum_{\lambda=0}^{p-1} T^2(\lambda) \right) \sum_{\lambda=0}^{p-1} \left| \sum_{x_1 \in I_1} \theta(x_1) e_p(ax_1^* \lambda) \right|^6.$$

По теореме 1 имеем

$$\sum_{\lambda=0}^{p-1} T^2(\lambda) < |I_2|^{2k-2+\frac{1}{k+1}+o(1)} < |I_2|^{2k-2+\varepsilon}.$$

Далее,

$$\sum_{\lambda=0}^{p-1} \left| \sum_{x_1 \in I_1} \theta(x_1) e_p(ax_1^* \lambda) \right|^6 \leq p J_6,$$

где J_6 – число решений сравнения

$$y_1^* + y_2^* + y_3^* \equiv y_4^* + y_5^* + y_6^* \pmod{p}, \quad y_i \in I_1.$$

По теореме 3 имеем $J_6 = |I_1|^{3+o(1)}$. Таким образом,

$$|W_2|^{6k} \leq p |I_1|^{6k-3+o(1)} |I_2|^{6k-2+\varepsilon}.$$

Поскольку $p \ll |I_1|^3 |I_2|^2 p^{-2\varepsilon}$, теорема доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 8. Пусть

$$S = \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1) \alpha_2(x_2) e_p(ax_1^* x_2^*).$$

Тогда по неравенству Гёльдера имеем

$$|S|^{k_2} \leq N_1^{k_2-1} \sum_{x_1 \in I_1} \left| \sum_{x_2 \in I_2} \alpha_2(x_2) e_p(ax_1^* x_2^*) \right|^{k_2}.$$

Поэтому для некоторых $\sigma(x_1) \in \mathbb{C}$, $|\sigma(x_1)| = 1$, получаем

$$|S|^{k_2} \leq N_1^{k_2-1} \sum_{y_1, \dots, y_{k_2} \in I_2} \left| \sum_{x_1 \in I_1} \sigma(x_1) e_p(ax_1^* (y_1^* + \dots + y_{k_2}^*)) \right|.$$

Снова по неравенству Гёльдера имеем

$$|S|^{k_1 k_2} \leq N_1^{k_1 k_2 - k_1} N_2^{k_1 k_2 - k_2} \sum_{\lambda=0}^{p-1} J_{k_2}(\lambda; N_2) \left| \sum_{x_1 \in I_1} \sigma(x_1) e_p(ax_1^* \lambda) \right|^{k_1},$$

где $J_k(\lambda; N)$ – число решений сравнения

$$x_1^* + \dots + x_k^* \equiv \lambda \pmod{p}, \quad x_i \in [1, N].$$

Тогда, применяя неравенство Коши–Буняковского и используя

$$\sum_{\lambda=0}^{p-1} J_{k_2}(\lambda; N_2)^2 = J_{2k_2}(N_2), \quad \sum_{\lambda=0}^{p-1} \left| \sum_{x_1 \in I_1} \sigma(x_1) e_p(ax_1^* \lambda) \right|^{2k_1} \leq p J_{2k_1}(N_1),$$

получим

$$|S|^{2k_1 k_2} \leq p N_1^{2k_1 k_2 - 2k_1} N_2^{2k_1 k_2 - 2k_2} J_{2k_1}(N_1) J_{2k_2}(N_2). \quad (47)$$

Здесь $J_{2k}(N)$ обозначает число решений сравнения

$$x_1^{-1} + \dots + x_k^{-1} \equiv x_{k+1}^{-1} + \dots + x_{2k}^{-1} \pmod{p}, \quad x_i \in [1, N].$$

Применяя теорему 5, получим

$$\begin{aligned} |S|^{2k_1 k_2} &\leq (2k_1)^{90k_1^3} (2k_2)^{90k_2^3} (\log N_1)^{4k_1^2} (\log N_2)^{4k_2^2} \\ &\quad \times N_1^{2k_1 k_2} N_2^{2k_1 k_2} \left(\frac{N_1^{k_1-1}}{p^{\frac{1}{2}}} + \frac{p^{\frac{1}{2}}}{N^{k_1}} \right) \left(\frac{N_2^{k_2-1}}{p^{\frac{1}{2}}} + \frac{p^{\frac{1}{2}}}{N^{k_2}} \right). \end{aligned}$$

Таким образом, имеем неравенство

$$\begin{aligned} |S| &< (2k_1)^{\frac{45k_1^2}{k_2}} (2k_2)^{\frac{45k_2^2}{k_1}} (\log p)^{2(\frac{k_1}{k_2} + \frac{k_2}{k_1})} \\ &\quad \times \left(\frac{N_1^{k_1-1}}{p^{\frac{1}{2}}} + \frac{p^{\frac{1}{2}}}{N^{k_1}} \right)^{\frac{1}{2k_1 k_2}} \left(\frac{N_2^{k_2-1}}{p^{\frac{1}{2}}} + \frac{p^{\frac{1}{2}}}{N^{k_2}} \right)^{\frac{1}{2k_1 k_2}} N_1 N_2, \end{aligned}$$

которое завершает доказательство теоремы.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 9. Заметим, что если $1 \leq N < p$, то, как результат следствия 4, число решений сравнения

$$\frac{1}{x_1} + \frac{1}{x_2} \equiv \frac{1}{x_3} + \frac{1}{x_4} \pmod{p}, \quad L+1 \leq x_1, x_2, x_3, x_4 \leq L+N,$$

ограничено величиной $N^{2+o(1)}(N^{\frac{3}{2}}p^{-\frac{1}{2}} + 1)$. Следуя доказательству теоремы 8 при $k_1 = k_2 = 2$ и применяя эту оценку для $[L+1, L+N] = I_i$, завершим доказательство теоремы.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 10. Будем использовать (47), в этом случае $J_{2k}(N_i)$ обозначает число решений сравнения

$$x_1^{-1} + \dots + x_k^{-1} \equiv x_{k+1}^{-1} + \dots + x_{2k}^{-1} \pmod{p}, \quad (x_1, \dots, x_{2k}) \in I_i^{2k}.$$

Поскольку

$$N_1 < p^{\frac{k_1+1}{2k_1}}, \quad N_2 < p^{\frac{k_2+1}{2k_2}},$$

по теореме 1 имеем

$$J_{2k_1}(N_1) < N_1^{\frac{2k_1^2}{k_1+1}}, \quad J_{2k_2}(N_2) < N_2^{\frac{2k_2^2}{k_2+1}}.$$

Объединяя последнее с неравенством (47), завершим доказательство теоремы.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 11. Можно предположить, что $0 < \varepsilon < 0.01$ и $N^n \sim p^{\frac{1}{3}+\varepsilon}$. Обозначим

$$W_n = \left| \sum_{x_1 \in I_1} \dots \sum_{x_n \in I_n} \alpha_1(x_1) \dots \alpha_n(x_n) e_p(ax_1^* \dots x_n^*) \right|.$$

Применяя n раз неравенство Гёльдера и используя тот факт, что при $|\alpha(v)| \leq 1$ имеет место оценка

$$\sum_u \left| \sum_v \alpha(v) e_p(auv) \right|^6 \leq \sum_{v_1, \dots, v_6} \left| \sum_u e_p(a(v_1 + v_2 + v_3 - v_4 - v_5 - v_6)u) \right|,$$

получим

$$W_n^{6^n} \leq N^{n6^n-6n} \times \sum_{x_{11}, \dots, x_{16} \in I_1} \cdots \sum_{x_{n1}, \dots, x_{n6} \in I_n} e_p(a(x_{11}^* + \cdots - x_{16}^*) \cdots (x_{n1}^* + \cdots - x_{n6}^*)).$$

Мы можем фиксировать x_{j4} , x_{j5} , x_{j6} так, что для некоторых целых чисел c_j будет выполняться оценка

$$W_n^{6^n} \leq N^{n6^n-3n} \left| \sum_{x_{11}, x_{12}, x_{13} \in I_1} \cdots \sum_{x_{n1}, x_{n2}, x_{n3} \in I_n} \{ \cdots \} \right|,$$

где $\{ \cdots \}$ обозначает выражение

$$e_p(a(x_{11}^* + x_{12}^* + x_{13}^* - c_1) \cdots (x_{n1}^* + x_{n2}^* + x_{n3}^* - c_n)).$$

Пусть $T_j(\lambda)$, $j = 1, \dots, n$, — число решений сравнения

$$x_1^* + x_2^* + x_3^* - c_j \equiv \lambda \pmod{p}, \quad x_1, x_2, x_3 \in I_j.$$

Тогда получим, что

$$W_n^{6^n} \leq N^{n6^n-3n} \left| \sum_{\lambda_1=0}^{p-1} \cdots \sum_{\lambda_n=0}^{p-1} T_1(\lambda_1) \cdots T_n(\lambda_n) e_p(a\lambda_1 \cdots \lambda_n) \right|. \quad (48)$$

Теперь заметим, что $\sum_{\lambda=0}^{p-1} \frac{T_j(\lambda)}{N^3} \leq 1$. По теореме 3 также имеем

$$\sum_{\lambda} \left(\frac{T_j(\lambda)}{N^3} \right)^2 < N^{-3+o(1)}.$$

Далее, для некоторого $\delta = \delta(\varepsilon, n) > 0$ будем иметь

$$\prod_{j=1}^n \left(\sum_{\lambda} \left(\frac{T_j(\lambda)}{N^3} \right)^2 \right)^{\frac{1}{2}} < N^{-\frac{3n}{2}+o(1)} < p^{-\frac{1}{2}-\delta}.$$

Таким образом, мы можем применить лемму 1 с данными $\gamma_j(x) = \frac{T_j(x)}{N^3}$. Это влечет, что

$$\left| \sum_{\lambda_1=0}^{p-1} \cdots \sum_{\lambda_n=0}^{p-1} T_1(\lambda_1) \cdots T_n(\lambda_n) e_p(a\lambda_1 \cdots \lambda_n) \right| < N^{3n} p^{-\delta'}.$$

Подставляя последнюю оценку в (48), завершаем доказательство теоремы.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 12. Пусть $C = 9c^{-2}$, где $c \leq \frac{1}{4}$ — константа из теоремы 4. В частности, можно предположить, что $n > 3c^{-1}$. Ясно, что можно предположить, что $N = [p^{\frac{9}{cn^2}}]$. При $k = [\frac{cn}{3}]$ имеем

$$p^{\frac{c}{k^2}} \geq p^{\frac{9}{cn^2}} \geq N.$$

Таким образом, при данном j число решений сравнения

$$y_1^* + \dots + y_k^* \equiv y_{k+1}^* + \dots + y_{2k}^* \pmod{p}, \quad y_1, \dots, y_{2k} \in I_j,$$

ограничено величиной $N^{k+o(1)}$. Полагая

$$W_n = \left| \sum_{x_1 \in I_1} \dots \sum_{x_n \in I_n} \alpha_1(x_1) \dots \alpha_n(x_n) e_p(ax_1^* \dots x_n^*) \right|,$$

получаем

$$W_n^{(2k)^n} \leq N^{n(2k)^n - 2kn} \sum_{x_{11}, \dots, x_{(2k)1} \in I_1} \dots \sum_{x_{1n}, \dots, x_{(2k)n} \in I_n} e_p(a\{\dots\}),$$

где $\{\dots\}$ обозначает выражение

$$\prod_{j=1}^n (x_{1j}^* + \dots + x_{kj}^* - x_{(k+1)j}^* - \dots - x_{(2k)j}^*).$$

Фиксируем $x_{(k+i)j}$ для всех $i = 1, \dots, k$ и $j = 1, \dots, n$ таким образом, что при некоторых целых числах $c_1, \dots, c_n$ будет иметь место оценка

$$W_n^{(2k)^n} \leq N^{n(2k)^n - kn} \left| \sum_{x_{11}, \dots, x_{k1} \in I_1} \dots \sum_{x_{1n}, \dots, x_{kn} \in I_n} e_p(a\{\dots\}) \right|,$$

где $\{\dots\}$ обозначает выражение

$$(x_{11}^* + \dots + x_{k1}^* - c_1) \dots (x_{1n}^* + \dots + x_{kn}^* - c_n).$$

Следовательно, имеем

$$W_n^{(2k)^n} \leq N^{n(2k)^n - kn} \left| \sum_{\lambda_1=0}^{p-1} \dots \sum_{\lambda_n=0}^{p-1} T_1(\lambda_1) \dots T_n(\lambda_n) e_p(a\lambda_1 \dots \lambda_n) \right|, \quad (49)$$

где $T_j(\lambda_j)$ – число решений сравнения

$$y_1^* + \dots + y_k^* - c_j \equiv \lambda_j \pmod{p}, \quad (y_1, \dots, y_k) \in I_j^k.$$

Имеем

$$\sum_{\lambda_j=0}^{p-1} \frac{T_j(\lambda_j)}{N^k} \leq 1.$$

Далее, по теореме 4 получаем

$$\sum_{\lambda_j=0}^{p-1} \left(\frac{T_j(\lambda_j)}{N^k} \right)^2 < \frac{N^{k+o(1)}}{N^{2k}} < N^{-k+o(1)} < p^{-\delta},$$

а также для некоторого $\delta = \delta(\varepsilon, n) > 0$ имеем

$$\prod_{j=1}^n \left(\sum_{\lambda_j=0}^{p-1} \left(\frac{T_j(\lambda_j)}{N^k} \right)^2 \right)^{\frac{1}{2}} < N^{-\frac{kn}{2}} p^{o(1)} < p^{-\frac{1}{2}-\delta}.$$

Здесь мы учли то, что $N = [p^{\frac{9}{cn^2}}]$, $N^{\frac{kn}{2}} > N^{\frac{cn^2}{12}} \gg p^{\frac{3}{4}}$. Следовательно, мы можем применить лемму 1, которая приводит к оценке

$$\sum_{\lambda_1=0}^{p-1} \cdots \sum_{\lambda_n=0}^{p-1} T_1(\lambda_1) \cdots T_n(\lambda_n) e_p(a\lambda_1 \cdots \lambda_n) < N^{kn} p^{-\delta'}$$

при некотором $\delta' = \delta'(\varepsilon, n) > 0$. Объединяя последнее с оценкой (49), завершаем доказательство теоремы.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 13. Положим $N_j = |I_j|$. Удаляя (в случае необходимости) интервалы I_j , для которых $N_j \leq p^{\frac{\varepsilon}{2n}}$, мы легко сводим утверждение к случаю, когда $N_j > p^{\frac{\varepsilon}{2n}}$ для всех j , а также $N_1 \cdots N_n \geq p^{\frac{1}{2}+\varepsilon}$. Далее, заметим, что если $N_j \geq p^{\frac{1}{2}+\frac{\varepsilon}{10n}}$ для некоторого j , то утверждение следует из оценки Вейля неполных сумм Клоостермана. Поэтому мы также можем предполагать, что для всех j выполнено условие $N_j < p^{\frac{1}{2}+\frac{\varepsilon}{10n}}$. Тогда те интервалы I_j , для которых $N_j > p^{\frac{1}{2}}$, можно разбить на подынтервалы размера $\approx p^{\frac{1}{2}}$ и, таким образом, предположить, что $p^{\frac{\varepsilon}{2n}} < N_j < p^{\frac{1}{2}}$ для всех j . Наконец, некоторые интервалы можем разбить на подынтервалы и добиться того, что будут выполняться условия

$$\begin{aligned} p^{\frac{1}{2}+\varepsilon} &< N_1 \cdots N_n < 2p^{\frac{1}{2}+\varepsilon}, \\ p^{\frac{\varepsilon}{2n}} &< N_j < p^{\frac{1}{2}}, \quad j = 1, 2, \dots, n. \end{aligned}$$

Пусть $\alpha_j(x_j) = e_p(a_j x_j)$. Обозначим

$$W_n = \left| \sum_{x_1 \in I_1} \cdots \sum_{x_n \in I_n} \alpha_1(x_1) \cdots \alpha_n(x_n) e_p(ax_1^* \cdots x_n^*) \right|.$$

Полагая $k = [\frac{2}{\varepsilon}]$ и последовательно применяя неравенство Гёльдера n раз, получим

$$W_n^{(2k)^n} \leq (N_1 \cdots N_n)^{(2k)^n - 2k} \sum_{\lambda_1=0}^{p-1} \cdots \sum_{\lambda_n=0}^{p-1} T_1(\lambda_1) \cdots T_n(\lambda_n) e_p(a\lambda_1 \cdots \lambda_n), \quad (50)$$

где $T_j(\lambda_j)$ – число решений сравнения

$$(y_1^* + \cdots + y_k^*) - (y_{k+1}^* + \cdots + y_{2k}^*) \equiv \lambda_j \pmod{p}, \quad (y_1, \dots, y_{2k}) \in I_j^{2k}.$$

Теперь заметим, что

$$\sum_{\lambda_j=0}^{p-1} \frac{T_j(\lambda_j)}{N_j^{2k}} \leq 1.$$

Далее, по теореме 1 имеем

$$\sum_{\lambda_j=0}^{p-1} \left(\frac{T_j(\lambda_j)}{N_j^{2k}} \right)^2 < \frac{N_j^{4k-2+\frac{1}{2k+1}+o(1)}}{N_j^{4k}} < N_j^{-2+\frac{1}{2k+1}+o(1)} < p^{-\delta},$$

а также

$$\prod_{j=1}^n \left(\sum_{\lambda_j=0}^{p-1} \left(\frac{T_j(\lambda_j)}{N_j^{2k}} \right)^2 \right)^{\frac{1}{2}} < (N_1 \cdots N_n)^{-1} p^{0.5\varepsilon} < p^{-\frac{1}{2}-\delta}$$

для некоторого $\delta = \delta(\varepsilon, n) > 0$. Таким образом, мы можем применить лемму 1, которая приводит к оценке

$$\sum_{\lambda_1=0}^{p-1} \cdots \sum_{\lambda_n=0}^{p-1} T_1(\lambda_1) \cdots T_n(\lambda_n) e_p(a\lambda_1 \cdots \lambda_n) < (N_1 \cdots N_n)^{2k} p^{-\delta'},$$

где $\delta' = \delta'(\varepsilon, n) > 0$. Соединяя последнюю оценку с неравенством (50), завершаем доказательство теоремы.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 14. Здесь нам понадобится следующее следствие теоремы 7 работы [31]. Пусть μ, ν – положительные вероятностные меры в $\mathbb{R}$ с носителем, скажем, в $[-1, 1]$, и пусть α, β – комплекснозначные функции на $\mathbb{R}$, $|\alpha|, |\beta| \leq 1$. Пусть $\xi \in \mathbb{R}$, $|\xi| > 1$. Тогда имеет место оценка

$$\left| \int \int \alpha(x) \beta(y) e^{ixy\xi} \mu(dx) \nu(dy) \right| \ll |\xi|^{-\frac{1}{2}} \|\mu * \varphi_\delta\|_2 \|\nu * \varphi_\delta\|_2, \quad (51)$$

где $\delta = (100|\xi|)^{-1}$ и

$$\varphi_\delta(t) = \begin{cases} \delta^{-1}, & \text{если } t \in \left[-\frac{\delta}{2}, \frac{\delta}{2}\right], \\ 0 & \text{иначе.} \end{cases}$$

Заметим, что (51) является простым фактом, работа [31] содержит также полилинейные версии, но здесь они нам не понадобятся.

Приведем прямое доказательство (51). Для краткости обозначим $\varphi = \varphi_\delta$. Поскольку

$$\widehat{\varphi}(\lambda) = \frac{2}{\delta\lambda} \sin \frac{\delta\lambda}{2},$$

при $|\lambda| < (10\delta)^{-1} = 10\xi$ и $|y| \leq 1$ имеем

$$\frac{1}{2} < \widehat{\varphi}(\lambda) \leq 1, \quad \left| \frac{\beta(y)}{\widehat{\varphi}(\xi y)} \right| \leq 2.$$

Для $x, y \in [-1, 1]$ запишем

$$e^{i\xi xy} = \frac{1}{\widehat{\varphi}(\xi y)} \int \varphi(s-x) e^{i\xi sy} ds.$$

Тогда

$$\begin{aligned} \left| \int \int \alpha(x) \beta(y) e^{ixy\xi} \mu(dx) \nu(dy) \right| &\leq \int \int \left| \int \frac{\beta(y)}{\widehat{\varphi}(\xi y)} e^{i\xi sy} \nu(dy) \right| \varphi(s-x) \mu(dx) ds \\ &= \int |\widehat{\nu}_1(\xi s)| (\mu * \varphi)(s) ds, \end{aligned} \quad (52)$$

где

$$\frac{d\nu_1}{d\nu} = \frac{\beta(y)}{\widehat{\varphi}(\xi y)}.$$

Заметим, что $|\nu_1| \leq 2\nu$. Поскольку $\text{supp}(\mu * \varphi) \subset [-2, 2]$, из (52) следует, что

$$\left| \int \int \alpha(x) \beta(y) e^{ixy\xi} \mu(dx) \nu(dy) \right| \leq \|\mu * \varphi\|_2 \|\widehat{\nu}_1(\xi \cdot)\|_{L^2[-2, 2]}.$$

Далее, при $|s| \leq 2$ имеем

$$|\widehat{\nu}_1(\xi s)| \leq 2|\widehat{\nu}_1(\xi s) \widehat{\varphi}(\xi s)| = 2|(\nu_1 * \varphi)^\wedge(\xi s)|.$$

Следовательно,

$$\begin{aligned} \|\widehat{\nu}_1(\xi \cdot)\|_{L^2[-2, 2]} &\leq 2|\xi|^{-\frac{1}{2}} \|(\nu_1 * \varphi)^\wedge\|_2 = 2|\xi|^{-\frac{1}{2}} (2\pi)^{\frac{1}{2}} \|\nu_1 * \varphi\|_2 \\ &\leq 4(2\pi)^{\frac{1}{2}} |\xi|^{-\frac{1}{2}} \|\nu * \varphi\|_2. \end{aligned}$$

Из полученных оценок следует неравенство (51).

Пусть $e(z) = e^{iz}$. Обозначим

$$S = \sum_{\substack{n_1 \sim N_1 \\ n_2 \sim N_2}} \alpha_1(n_1) \alpha_2(n_2) e\left(\frac{1}{n_1} \frac{1}{n_2} \xi\right).$$

Применяя неравенство Гёльдера, легко получаем, что

$$\begin{aligned} |S|^{k_1 k_2} &\leq N_1^{k_1 k_2 - k_1} N_2^{k_1 k_2 - k_2} \\ &\times \sum_{\substack{n_{11}, \dots, n_{1k_1} \sim N_1 \\ n_{21}, \dots, n_{2k_2} \sim N_2}} \alpha_{\overline{n_1}} \beta_{\overline{n_2}} e\left(\xi \left(\frac{1}{n_{11}} + \dots + \frac{1}{n_{1k_1}}\right) \left(\frac{1}{n_{21}} + \dots + \frac{1}{n_{2k_2}}\right)\right), \end{aligned}$$

где $\overline{n_i} = (n_{i1}, \dots, n_{ik_i})$, а коэффициенты $\alpha_{\overline{n_1}}$ и $\beta_{\overline{n_2}}$ являются комплексными числами, зависящими соответственно от величин

$$\frac{1}{n_{11}} + \dots + \frac{1}{n_{1k_1}}, \quad \frac{1}{n_{21}} + \dots + \frac{1}{n_{2k_2}},$$

а также $|\alpha_{\overline{n_1}}| = |\beta_{\overline{n_2}}| = 1$. Таким образом, для некоторых комплексных чисел $\alpha(x)$ и $\beta(y)$ с условием $|\alpha(x)| = |\beta(y)| = 1$ будем иметь

$$|S|^{k_1 k_2} \leq (N_1 N_2)^{k_1 k_2} \left| \int \int \alpha(x) \beta(y) e\left(\frac{\xi}{N_1 N_2} xy\right) \mu(dx) \nu(dy) \right|,$$

где μ – нормализованная мера образа в $\mathbb{R}$ отображения

$$\{n_i \sim N_1\}^{k_1} \rightarrow \mathbb{R}: (n_{11}, \dots, n_{1k_1}) \rightarrow N_1 \left(\frac{1}{n_{11}} + \dots + \frac{1}{n_{1k_1}}\right);$$

аналогично определяется ν .

Положим $\delta = \frac{N_1 N_2}{100|\xi|}$. Из (51) следует, что

$$|S|^{k_1 k_2} \leq (N_1 N_2)^{k_1 k_2} \delta^{\frac{1}{2}} \|\mu * \varphi_\delta\|_2 \|\nu * \varphi_\delta\|_2. \quad (53)$$

Далее оценим $\|\mu * \varphi_\delta\|_2$. Заметим, что если $\{I_j\}_j$ является разбиением $\mathbb{R}$ на δ -интервалы, то

$$\begin{aligned} & \sum_j \left| (n_1, \dots, n_k); n_i \sim N, \frac{N}{n_1} + \dots + \frac{N}{n_k} \in I_j \right| \\ & \leq \left| (n_1, \dots, n_{2k}); n_i \sim N, \left| \frac{1}{n_1} + \dots + \frac{1}{n_k} - \frac{1}{n_{k+1}} - \dots - \frac{1}{n_{2k}} \right| < \frac{\delta}{N} \right|. \end{aligned}$$

Тогда имеем

$$\|\mu * \varphi_\delta\|_2^2 \sim N_1^{-2k_1} \delta^{-1} T(N_1), \quad (54)$$

где

$$T(N) = \left| (n_1, \dots, n_{2k}); n_i \sim N, \left| \frac{1}{n_1} + \dots + \frac{1}{n_k} - \frac{1}{n_{k+1}} - \dots - \frac{1}{n_{2k}} \right| < \frac{\delta}{N} \right|.$$

Докажем, что

$$T(N) < c(k)(\log N)^{4k^2} N^k (1 + \delta N^{2k-1}).$$

При $\lambda \in \mathbb{Q}$ обозначим через $J(\lambda)$ количество представлений λ в виде

$$\lambda = \frac{1}{n_1} + \dots + \frac{1}{n_k}, \quad n_i \sim N. \quad (55)$$

По лемме 4 имеем

$$\sum_{\lambda} J^2(\lambda) \leq c(k) N^k (\log N)^{4k^2}.$$

Заметим, что расстояние между различными λ по порядку не меньше N^{-2k} . Следовательно, интервал $I \subset \mathbb{R}$ длиной δ/N может содержать по порядку не более $1 + N^{2k-1} \delta$ чисел вида (55). Следовательно,

$$\begin{aligned} T(N) & \ll \sum_{n_1, \dots, n_k \sim N} J\left(\frac{1}{n_1} + \dots + \frac{1}{n_k}\right) (1 + N^{2k-1} \delta) \\ & \ll (1 + N^{2k-1} \delta) \sum_{\lambda} J^2(\lambda) < c(k) N^k (\log N)^{4k^2} (1 + N^{2k-1} \delta), \end{aligned}$$

откуда следует требуемая оценка для $T(N)$.

Таким образом, из (54) получаем, что

$$\|\mu * \varphi_\delta\|_2 \leq c(k_1)(\log N_1)^{2k_1} \delta^{-\frac{1}{2}} N_1^{-\frac{k_1}{2}} (1 + \delta N_1^{2k_1-1})^{\frac{1}{2}}.$$

Аналогично,

$$\|\nu * \varphi_\delta\|_2 \leq c(k_2)(\log N_2)^{2k_2} \delta^{-\frac{1}{2}} N_2^{-\frac{k_2}{2}} (1 + \delta N_2^{2k_2-1})^{\frac{1}{2}}.$$

Внеся эти оценки в (53), получим

$$\begin{aligned} |S|^{k_1 k_2} & \leq c(k_1) c(k_2) (\log N_1)^{2k_1} (\log N_2)^{2k_2} (N_1 N_2)^{k_1 k_2} \\ & \quad \times (\delta^{-\frac{1}{2}} N_1^{-k_1} + \delta^{\frac{1}{2}} N_1^{k_1-1})^{\frac{1}{2}} (\delta^{-\frac{1}{2}} N_2^{-k_2} + \delta^{\frac{1}{2}} N_2^{k_2-1})^{\frac{1}{2}}. \end{aligned}$$

Учитывая, что $\delta = \frac{N_1 N_2}{100|\xi|}$, завершаем доказательство.

§ 9. Некоторые применения

В настоящем параграфе применим теорему 14 для доказательства теоремы 15 о $\pi(x) - \pi(x - y)$, а также применим оценки трилинейных экспоненциальных сумм для доказательства теоремы 16 о линейных суммах Клоостермана и теоремы 17 об оценке Бруна–Титчмарша.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 15. Если $y \geq x^{\frac{7}{12}+}$, то утверждение следует из результата Хаксли [32]. Поэтому можем предположить, что $x^\theta \leq y < x^{\frac{7}{12}+}$. Заметим, что в интервале $\nu \in (0, \frac{7}{12}+)$ функция

$$f(\nu) = \frac{2(1 - \nu)}{12(\nu^{-1} + 1)(\nu^{-1} + 0.5) + 1 - \nu}$$

растет. Поэтому достаточно рассмотреть случай $y = x^\theta$, где $\theta \in (0, \frac{7}{12}+)$. Используя аргумент из [14, с. 269] и оценку (13.56) из [14], получим, что $R(M, N)$ ограничено сверху величиной порядка

$$\frac{Hy}{MN} \left| \sum_{\substack{m \sim M \\ n \sim N}} \alpha_m \beta_n e\left(\frac{hu}{mn}\right) \right|,$$

где $u \sim x$ и $1 \leq h \leq H = MNy^{-1}x^\varepsilon$. Здесь M, N могут быть выбраны произвольно с условием $MN = D > y$ (см. [14, теорема 12.21]), и необходимо убедиться в том, что $R(M, N) < yx^{-\varepsilon}$.

Тогда мы можем получить оценку сверху

$$\pi(x) - \pi(x - y) < \frac{2y}{\log D}.$$

Итак, имеем

$$\frac{Hy}{MN} \left| \sum_{\substack{m \sim M \\ n \sim N}} \alpha_m \beta_n e\left(\frac{hu}{mn}\right) \right| \leq x^\varepsilon \left| \sum_{\substack{m \sim M \\ n \sim N}} \alpha_m \beta_n e\left(\frac{\xi}{mn}\right) \right|, \quad (56)$$

где

$$D < x \leq \xi < \frac{D}{y} x^{1+\varepsilon}.$$

Возьмем целое число k , удовлетворяющее условию $k - \frac{1}{2} < \frac{1}{\theta} < k + \frac{1}{2}$, и определим M из условия

$$\frac{x}{D} = M^{2k-1}.$$

Положим $N = D/M$ и определим целое число l так, чтобы

$$N^{2(l-1)} \leq \frac{\xi}{D} < N^{2l}.$$

Тогда

$$\log N = \log D - \frac{\log \frac{x}{D}}{2k-1} \geq \log y - \frac{\log \frac{x}{y}}{2k-1} = \left(\theta - \frac{1-\theta}{2k-1} \right) \log x > \frac{\theta}{2} \log x,$$

а также $l \leq \theta^{-1} + 1$. Оценивая (56) по теореме 14, получим

$$\begin{aligned} x^\varepsilon D \left(\frac{\xi}{D} M^{-2k} + \frac{D}{\xi} M^{2(k-1)} \right)^{\frac{1}{4kl}} &\leq x^\varepsilon D \left(\frac{Dx^\varepsilon}{y} M^{-1} + M^{-1} \right)^{\frac{1}{4kl}} \\ &< x^{2\varepsilon} \left(\frac{D}{y} \right)^{\frac{5}{4}} \left(\frac{x}{D} \right)^{-\frac{1}{4k(2k-1)l}} y < x^{2\varepsilon} \left(\frac{D}{y} \right)^{\frac{3}{2}} x^{-\frac{(1-\theta)\theta}{8(\theta^{-1}+1)(\theta^{-1}+0.5)}} y. \end{aligned}$$

Следовательно, мы можем взять

$$D = y^{1 + \frac{1-\theta}{12(\theta^{-1}+1)(\theta^{-1}+0.5)}}^{-\varepsilon'}.$$

Теорема доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 16. Обозначим $\varepsilon = \frac{\log N}{\log p}$. Как следствие оценки Вейля неполных сумм Клоостермана, можем предположить, что $\varepsilon < \frac{4}{7}$. Пусть

$$\mathcal{G} = \{x < N : p_1 \geq N^\alpha, p_3 \geq N^\beta, p_1 p_2 p_3 < N^{1-\beta}\},$$

где $p_1 \geq p_2 \geq p_3$ – наибольшие простые делители числа x . Числа α, β являются параметрами и будут определены по ходу доказательства. Пока предполагаем, что

$$0.1 > \alpha > \beta > \frac{1}{\log N}.$$

Введем еще два параметра β, β_1 с условием $0.1 > \beta_1 > \beta$. Заметим, что

$$\sum_{\substack{x < N \\ p_1 p_2 > N^{1-\beta_1}}} 1 \leq \sum_{y < N^{\beta_1}} \sum_{p_1 p_2 \leq N/y} 1 \leq \sum_{y < N^{\beta_1}} \sum_{p_2 \leq N} \frac{3N}{p_2 y \log N} \leq 4\beta_1 (\log \log N) N.$$

Аналогично,

$$\sum_{\substack{x < N \\ p_1 p_2 p_3 \geq N^{1-\beta}}} 1 < \sum_{y \leq N^\beta} \sum_{p_2 p_3 < N} \frac{4N}{y p_2 p_3 \log N} < 5\beta (\log \log N)^2 N.$$

Также заметим, что количество натуральных чисел, не превосходящих N и состоящих из произведений не более чем двух простых чисел, меньше, чем

$$\frac{2N \log \log N}{\log N} < 2\beta N \log \log N.$$

Следовательно,

$$\begin{aligned} N - |\mathcal{G}| &\leq \frac{2N \log \log N}{\log N} \\ &\quad + \sum_{\substack{x < N \\ p_1 < N^\alpha}} 1 + \sum_{\substack{x < N \\ p_1 p_2 > N^{1-\beta_1}}} 1 + \sum_{\substack{x < N \\ p_1 p_2 \leq N^{1-\beta_1} \\ p_3 < N^\beta}} 1 + \sum_{\substack{x < N \\ p_1 p_2 p_3 \geq N^{1-\beta}}} 1 \\ &\leq \frac{2N \log \log N}{\log N} + \Psi(N, N^\alpha) + 4\beta_1 N \log \log N \\ &\quad + \sum_{p_1 p_2 < N^{1-\beta_1}} \Psi\left(\frac{N}{p_1 p_2}, N^\beta\right) + 5\beta N (\log \log N)^2. \end{aligned}$$

Здесь $\Psi(x, y)$, как обычно, обозначает число натуральных чисел, не превышающих x и свободных от простых делителей, больших y . По классическому результату де Брейна [33] если $y > (\log x)^{1+\delta}$, где $\delta > 0$ – положительная фиксированная константа, то

$$\Psi(x, y) \leq xu^{-u(1+o(1))} \quad \text{при} \quad u = \frac{\log x}{\log y} \rightarrow \infty.$$

Таким образом, полагая

$$\alpha = \frac{1}{\log \log p}, \quad \beta_1 = \beta \log \log p, \quad \frac{2 \log \log N}{\log N} < \beta < \frac{1}{(\log \log p)^2},$$

получим

$$\begin{aligned} N - |\mathcal{G}| &< \alpha^{\frac{1}{2\alpha}} N + \sum_{p_1 p_2 < N^{1-\beta_1}} \frac{N}{p_1 p_2} \left(\frac{\beta}{\beta_1} \right)^{\frac{\beta_1}{2\beta}} + 11\beta N (\log \log p)^2 \\ &< \left(\alpha^{\frac{1}{2\alpha}} + (\log \log N)^2 \left(\frac{\beta}{\beta_1} \right)^{\frac{\beta_1}{2\beta}} + 11\beta (\log \log p)^2 \right) N \\ &< 12\beta (\log \log p)^2 N. \end{aligned}$$

Следовательно,

$$\left| \sum_{x < N} e_p(ax^*) \right| \leq 12\beta (\log \log p)^2 N + \left| \sum_{x \in \mathcal{G}} e_p(ax^*) \right|.$$

Мы далее предполагаем, что

$$\varepsilon \beta > \frac{1}{\sqrt{\log p}}.$$

Сумму $\sum_{x \in \mathcal{G}} e_p(ax^*)$ можем оценить как

$$\sum_{p_1} \sum_{p_2} \sum_{p_3} \left| \sum_y e_p(ap_1^* p_2^* p_3^* y^*) \right|, \quad (57)$$

где суммирование проводим по всем простым числам p_1, p_2, p_3 и целым числам y , для которых

$$\begin{aligned} p_1 \geq p_2 \geq p_3, \quad p_1 \geq N^\alpha, \quad p_3 \geq N^\beta, \quad p_1 p_2 p_3 \leq N^{1-\beta}, \\ y < \frac{N}{p_1 p_2 p_3}, \quad P(y) \leq p_3. \end{aligned} \quad (58)$$

Заметим, что если числа t и T такие, что

$$\left(1 - \frac{c}{\log p} \right) p_3 < t < p_3, \quad \left(1 - \frac{c}{\log p} \right) \frac{N}{p_1 p_2 p_3} < T < \frac{N}{p_1 p_2 p_3}, \quad (59)$$

где $c > 0$ – произвольная константа, то можно заменить условие для y на условие

$$y < T, \quad P(y) \leq t; \quad (60)$$

от такой замены сумма (57) будет меняться на величину порядка, не превосходящего

$$\frac{N(\log \log p)^{O(1)}}{\log p}.$$

Таким образом, для любых t и T с условием (59) имеем

$$\left| \sum_{x \in \mathcal{G}} e_p(ax^*) \right| < \frac{N(\log \log p)^{O(1)}}{\log p} + \sum_{p_1} \sum_{p_2} \sum_{p_3} \left| \sum_y e_p(ap_1^* p_2^* p_3^* y^*) \right|,$$

где суммирование проводится по простым числам p_1, p_2, p_3 и целым числам y с условиями (58) и (60).

Теперь разобьем интервалы изменения простых чисел p_1, p_2, p_3 на подынтервалы вида $[L, L + L(\log p)^{-1}]$ и, выбирая подходящие t и T , получим, что для некоторых чисел M_1, M_2, M_3 с условием

$$M_1 > 0.5M_2 > 0.2M_3, \quad M_1 > N^\alpha, \quad M_3 \geq N^\beta, \quad M_1 M_2 M_3 < N^{1-\beta} \quad (61)$$

имеет место оценка

$$\left| \sum_{x \in \mathcal{G}} e_p(ax^*) \right| < \frac{N(\log \log p)^{O(1)}}{\log p} + (\log p)^{10} \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \sum_{p_3 \in I_3} \left| \sum_{\substack{y \leq M \\ P(y) \leq M_3}} e_p(ap_1^* p_2^* p_3^* y^*) \right|, \quad (62)$$

где

$$I_j = \left[M_j, M_j + \frac{M_j}{\log p} \right], \quad M = \frac{N}{M_1 M_2 M_3} \geq N^\beta.$$

Обозначим

$$W = \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \sum_{p_3 \in I_3} \left| \sum_{\substack{y \leq M \\ P(y) \leq M_3}} e_p(ap_1^* p_2^* p_3^* y^*) \right|.$$

Применяя неравенство Коши–Буняковского, получим

$$W^2 \leq M_1 M_2 M_3 \sum_{y \leq M} \sum_{z \leq M} \left| \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \sum_{p_3 \in I_3} e_p(ap_1^* p_2^* p_3^* (y^* - z^*)) \right|.$$

Оценивая правую часть этого неравенства при $y = z$, а затем фиксируя должным образом y, z при $y \neq z$, получим, что для некоторого $b \not\equiv 0 \pmod{p}$ имеет место оценка

$$W^2 \leq \frac{N^2}{M} + NM|S|, \quad (63)$$

где

$$|S| = \left| \sum_{p_1 \in I_1} \sum_{p_2 \in I_2} \sum_{p_3 \in I_3} e_p(bp_1^* p_2^* p_3^*) \right|.$$

Определим целые числа k_1, k_2, k_3 так, чтобы

$$p^{\frac{1}{2k_j}} \leq M_j < p^{\frac{1}{2(k_j-1)}}, \quad j = 1, 2, 3.$$

Из условий (61) и выбора чисел α и β , в частности, следует, что

$$k_1 < \frac{1}{\varepsilon\alpha} < (\log p)^{\frac{1}{2}}, \quad k_2, k_3 < \frac{1}{\varepsilon\beta} < (\log p)^{\frac{1}{2}}. \quad (64)$$

Далее, возьмем четные числа $l_j \in \{k_j, k_j + 1\}$, $j = 1, 2, 3$, и определим

$$\eta_j(\lambda) = |\{(x_1, \dots, x_{l_j}) \in (I_j \cap \mathcal{P})^{l_j} : x_1^* - x_2^* + \dots - x_{l_j}^* \equiv \lambda \pmod{p}\}|.$$

Имеем

$$\sum_{\lambda=0}^{p-1} \eta_j(\lambda) < M_j^{l_j}, \quad (65)$$

а применяя теорему 6, получим

$$\begin{aligned} \sum_{\lambda=0}^{p-1} \eta_j^2(\lambda) &< M_j^{2(l_j - k_j)} (2M_j)^{k_j} (2k_j)^{k_j} \left(\frac{(2M_j)^{2k_j - 1}}{p} + 1 \right) \\ &< (20k_j)^{k_j} M_j^{2l_j} p^{-\frac{1}{2}}. \end{aligned} \quad (66)$$

Далее последовательно применим неравенство Гёльдера. Получим

$$|S|^{l_1} < (M_2 M_3)^{l_1 - 1} \sum_{p_2 \in I_2} \sum_{p_3 \in I_3} \left| \sum_{p_1 \in I_1} e_p(bp_1^* p_2^* p_3^*) \right|^{l_1},$$

а так как l_j являются четными числами, будем иметь

$$\begin{aligned} |S|^{l_1} &< (M_2 M_3)^{l_1 - 1} \sum_{\lambda_1=0}^{p-1} \eta_1(\lambda_1) \left[\sum_{p_2 \in I_2} \sum_{p_3 \in I_3} e_p(b\lambda_1 p_2^* p_3^*) \right] \\ &< (M_2 M_3)^{l_1 - 1} \sum_{\lambda_1=0}^{p-1} \eta_1(\lambda_1) \sum_{p_3 \in I_3} \left| \sum_{p_2 \in I_2} e_p(b\lambda_1 p_2^* p_3^*) \right|. \end{aligned}$$

Применяя неравенство Гёльдера и используя (65), получим

$$\begin{aligned} |S|^{l_1 l_2} &< (M_2 M_3)^{(l_1 - 1)l_2} M_1^{(l_2 - 1)l_1} M_3^{l_2 - 1} \sum_{\lambda_1=0}^{p-1} \eta_1(\lambda_1) \sum_{p_3 \in I_3} \left| \sum_{p_2 \in I_2} e_p(b\lambda_1 p_2^* p_3^*) \right|^{l_2} \\ &= M_1^{l_1(l_2 - 1)} M_2^{l_2(l_1 - 1)} M_3^{l_1 l_2 - 1} \sum_{\lambda_1=0}^{p-1} \sum_{\lambda_2=0}^{p-1} \eta_1(\lambda_1) \eta_2(\lambda_2) \left| \sum_{p_3 \in I_3} e_p(b\lambda_1 \lambda_2 p_3^*) \right|. \end{aligned}$$

Снова применяя неравенство Гёльдера и учитывая (65), получим

$$\begin{aligned} |S|^{l_1 l_2 l_3} &< M_1^{l_1 l_3(l_2 - 1)} M_2^{l_2 l_3(l_1 - 1)} M_3^{l_3(l_1 l_2 - 1)} (M_1^{l_1} M_2^{l_2})^{l_3 - 1} \\ &\quad \times \left| \sum_{\lambda_1=0}^{p-1} \sum_{\lambda_2=0}^{p-1} \sum_{\lambda_3=0}^{p-1} \eta_1(\lambda_1) \eta_2(\lambda_2) \eta_3(\lambda_3) e_p(b\lambda_1 \lambda_2 \lambda_3) \right| \\ &= M_1^{l_1 l_2 l_3 - l_1} M_2^{l_1 l_2 l_3 - l_2} M_3^{l_1 l_2 l_3 - l_3} |S_1|, \end{aligned}$$

где

$$|S_1| = \left| \sum_{\lambda_1=0}^{p-1} \sum_{\lambda_2=0}^{p-1} \sum_{\lambda_3=0}^{p-1} \eta_1(\lambda_1) \eta_2(\lambda_2) \eta_3(\lambda_3) e_p(b\lambda_1\lambda_2\lambda_3) \right|.$$

Применим лемму 1 при $n = 3$ и $\gamma_j(\lambda) = \frac{\eta_j(\lambda)}{M^{l_j}}$. Из (65) следует, что

$$\|\gamma_i\|_1 = \sum_{\lambda=0}^{p-1} \frac{\eta_j(\lambda)}{M^{l_j}} \leq 1.$$

Из неравенств (66) и (64) следует, что

$$\|\gamma_i\|_2 = \left(\sum_{\lambda=0}^{p-1} \left(\frac{\eta_j(\lambda)}{M^{l_j}} \right)^2 \right)^{\frac{1}{2}} < p^{-\frac{1}{5}}$$

и, в частности,

$$\prod_{i=1}^n \|\gamma_i\|_2 < p^{-\frac{1}{2} - \frac{1}{10}}.$$

Таким образом, можно применить лемму 1, которая влечет оценку

$$|S_1| < M_1 M_2 M_3 p^{-c}$$

для некоторой абсолютной константы $c > 0$. Вследствие этого имеем оценку

$$|S| < M_1 M_2 M_3 p^{-\frac{c_1}{k_1 k_2 k_3}} < M_1 M_2 M_3 p^{-c_2 \varepsilon^3 \alpha \beta^2}.$$

Подставляя последнее в (63) и учитывая, что

$$M > N^\beta = p^{\varepsilon \beta} > \exp(\sqrt{\log p}),$$

получим

$$W < \frac{N}{\exp(0.5\sqrt{\log p})} + N p^{-c_3 \varepsilon^3 \alpha \beta^2}.$$

Учитывая эту оценку в (62), получим

$$\left| \sum_{x \in \mathcal{G}} e_p(ax^*) \right| < \frac{N(\log \log p)^{O(1)}}{\log p} + (\log p)^{10} N p^{-c_3 \varepsilon^3 \alpha \beta^2}.$$

Следовательно, имеем

$$\left| \sum_{x < N} e_p(ax^*) \right| \leq \frac{N(\log \log p)^{O(1)}}{\log p} + 12\beta(\log \log p)^2 N + (\log p)^{10} N p^{-c_3 \varepsilon^3 \alpha \beta^2}.$$

Таким образом, определяя

$$\beta = \frac{C \log \log p}{\varepsilon^{\frac{3}{2}} (\log p)^{\frac{1}{2}}},$$

где C – достаточно большая константа, получаем

$$\left| \sum_{x < N} e_p(ax^*) \right| \ll \frac{(\log \log p)^3}{(\log p)^{\frac{1}{2}}} \varepsilon^{-\frac{3}{2}} N.$$

Теорема доказана.

ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 17. Напомним, что мы рассматриваем только случай простого q , случай составного q будет рассмотрен в нашей последующей статье.

Будем следовать [18]. Обозначим

$$\begin{aligned}\mathcal{A} &= \{n \leq x; n \equiv a \pmod{q}\}, & \mathcal{A}_d &= \{n \in \mathcal{A}; n \equiv 0 \pmod{d}\}, \\ S(\mathcal{A}, z) &= |\{n \in \mathcal{A}; (n, p) = 1, p < z, (p, q) = 1\}|, \\ D &= \frac{x^{1-\varepsilon}}{q}.\end{aligned}$$

Пусть $D^{\frac{1}{5}} < w < y < z = (x/q)^{\frac{1}{3}}$, где w и y будут определены позже. Используя тождество Бухштаба, запишем

$$S(\mathcal{A}, z) = S(\mathcal{A}, w) - \sum_{y \leq p < z} S(\mathcal{A}_p, z) - \sum_{w \leq p < y} S(\mathcal{A}_p, w) + \sum_{w \leq p_1 < p_2 < y} S(\mathcal{A}_{p_1 p_2}, p_2). \quad (67)$$

Применение фундаментальных оценок линейного решета в равенстве (67) ведет к оценке

$$S(\mathcal{A}, z) < \frac{2x}{\varphi(q) \log D} \quad (68)$$

(см. обсуждение в [18], а также [14, с. 265]). В частности, это влечет, что

$$S(\mathcal{A}_{p_1 p_2}, p_2) < \frac{2x}{\varphi(q) p_1 p_2 \log D_{12}}, \quad D_{12} = \frac{D}{p_1 p_2}. \quad (69)$$

Здесь D_{12} – уровень распределения последовательности $\mathcal{A}_{p_1 p_2}$. Идея работы [18] состоит в улучшении оценки (69) в среднем по p_1, p_2 , увеличивая уровень распределения D_{12} к некоторому уровню D'_{12} .

Более точно, определим остатки

$$R_{p_1, p_2, d} = |\mathcal{A}_{d p_1 p_2}| - \frac{x}{q d p_1 p_2}, \quad (70)$$

которые появляются в процессе применения решета. Стратегия состоит в оценке совместных вкладов $R_{p_1, p_2, d}$ при выполнении суммирования по p_1, p_2 .

Разобьем отрезок $[w, y]$ на диадические интервалы и при фиксированных P_1, P_2 оценим

$$\sum_{\substack{p_1 \sim P_1 \\ p_2 \sim P_2}} S(\mathcal{A}_{p_1 p_2}, p_2).$$

Введем $D'_{12} = D'_{12}(P_1, P_2) > D_{12}$ так, чтобы выполнялась оценка

$$\sum_{d < D'_{12}} \left| \sum_{\substack{p_1 \sim P_1 \\ p_2 \sim P_2}} R_{p_1, p_2, d} \right| < \frac{x^{1-\varepsilon}}{q} P_1 P_2. \quad (71)$$

Если взять D'_{12} в качестве предела решета, то оценка (69) будет улучшаться до оценки

$$S(\mathcal{A}_{p_1 p_2}, p_2) < \frac{2x}{\varphi(q) p_1 p_2 \log D'_{12}}$$

в среднем по $p_1 \sim P_1$, $p_2 \sim P_2$ с условием, что $p_2^3 > D'_{12}$. Тогда выигрыш в оценке (68) будет величиной порядка

$$\begin{aligned} \frac{x}{\varphi(q)} \sum_{w \leq p_1 < p_2 < y} \frac{1}{p_1 p_2} \left(\frac{1}{\log D_{12}} - \frac{1}{\log D'_{12}} \right) \\ = \frac{x}{\varphi(q)} \sum_{w \leq p_1 < p_2 < y} \frac{1}{p_1 p_2} \frac{\log \frac{D'_{12}}{D_{12}}}{(\log D_{12})(\log D'_{12})}. \end{aligned} \quad (72)$$

Применение анализа из [18] для представления (70) в виде экспоненциальных сумм показывает, что левая часть (71) ограничена сверху величиной

$$\sum_{d < D'_{12}} \sum_{0 < |h| < H} \left| \sum_{\substack{p_1 \sim P_1 \\ p_2 \sim P_2}} (q d p_1 p_2)^{-1} \hat{f} \left(\frac{h}{q d p_1 p_2} \right) e_q(-a h d^* p_1^* p_2^*) \right| \quad (73)$$

с допустимой погрешностью. Здесь

$$H = q d P_1 P_2 x^{2\varepsilon-1},$$

функция $f \geq 0$ имеет носитель в $x^{1-\varepsilon} < t < x + x^{1-\varepsilon}$ и удовлетворяет условиям $\hat{f}(0) = x$ и $t^j f^{(j)}(t) \ll x^{2\varepsilon j}$ при $j \geq 0$. Стандартные манипуляции позволяют выражать (73) в виде трilinearных экспоненциальных сумм ($D_{12} \leq \tilde{D} < D'_{12}$)

$$\frac{x}{q \tilde{D} P_1 P_2} H \left| \sum_{\substack{d \in I_0 \\ p_1 \in I_1, p_2 \in I_2}} \alpha_d \beta_{p_1} \gamma_{p_2} e_q(-a h d^* p_1^* p_2^*) \right|,$$

где $|\alpha_d|, |\beta_{p_1}|, |\gamma_{p_2}| \leq 1$, а I_0, I_1, I_2 являются интервалами,

$$I_0 \subset [\tilde{D}, 2\tilde{D}], \quad I_1 \subset [P_1, 2P_1], \quad I_2 \subset [P_2, 2P_2].$$

Заметим, что эти интервалы всегда могут быть дополнены до интервалов

$$I_0 = [\tilde{D}, 2\tilde{D}], \quad I_1 = [P_1, 2P_1], \quad I_2 = [P_2, 2P_2].$$

Возьмем теперь $\delta = (1 - \theta)/5$ и $w = x^\delta$, $y = x^{2\delta}$. Заметим, что

$$\tilde{D} > D_{12} > \frac{D}{y^2} > x^{0.9\delta}.$$

Используя аргумент Карацубы, связанный с применением неравенства Гёльдера, а затем применяя оценки трilinearных экспоненциальных сумм, приходим к оценке с понижающим множителем $x^{c'\delta^3}$. Следовательно,

$$\frac{x}{q \tilde{D} P_1 P_2} H \left| \sum_{\substack{d \in I_0 \\ p_1 \in I_1, p_2 \in I_2}} \alpha_d \beta_{p_1} \gamma_{p_2} e_q(-a h d^* p_1^* p_2^*) \right| < \frac{x^{1-c'\delta^3}}{q} H < x^{2\varepsilon-c'\delta^3} D'_{12} P_1 P_2. \quad (74)$$

При

$$D'_{12} = \frac{x^{1+c''\delta^3}}{qP_1P_2} \sim D_{12}x^{c''\delta^3}$$

правая часть в (74) не превосходит $x^{1-\varepsilon}q^{-1}$. Условие $w^5 > D'_{12}$ выполняется. Таким образом, возвращаясь к (72), видим, что выигрыш имеет порядок

$$\frac{x}{\varphi(q)} \sum_{x^\delta < p_1 < p_2 < x^{2\delta}} \frac{1}{p_1 p_2} \frac{\log(x^{c''\delta^3})}{\delta^2 (\log x)^2} \gg \frac{x\delta}{\varphi(q) \log x} \sim \frac{x\delta^2}{\varphi(q) \log \frac{x}{q}},$$

а так как ε является малым, то получаем требуемый результат.

§ 10. Комментарии

Как мы заметили во введении, если интервал $I \subset \mathbb{F}_p^*$ имеет мощность $|I| < p^{\frac{1}{2}}$, то выполнено

$$|I^{-1} + I^{-1} + I^{-1}| > |I|^{1.55+o(1)}. \quad (75)$$

Эта оценка лучше, чем оценка в следствии 1 для $k = 3$. Теперь докажем оценку (75). Можем предположить, что $|I| = N > p^{\frac{1}{3}}$, так как иначе следствие 4 влечет более сильную оценку

$$|I^{-1} + I^{-1}| > |I|^{2+o(1)}.$$

Пусть J_6 – число решений сравнения

$$\frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} \equiv \frac{1}{x_4} + \frac{1}{x_5} + \frac{1}{x_6} \pmod{p}, \quad x_1, \dots, x_6 \in I.$$

Величина J_6 может быть ограничена:

$$J_6 \leq (J_4 J_8)^{\frac{1}{2}}.$$

Из теоремы 1 следует, что $J_8 < N^{\frac{32}{5}+o(1)}$, а из следствия 4 имеем

$$J_4 < \frac{N^{\frac{7}{2}+o(1)}}{p^{\frac{1}{2}}}.$$

Таким образом,

$$J_6 < \frac{N^{\frac{99}{20}+o(1)}}{p^{-\frac{1}{4}}}.$$

Используя связи между числом решений сравнения и мощностью соответствующего множества, заключаем, что

$$|I^{-1} + I^{-1} + I^{-1}| \geq N^{\frac{21}{20}+o(1)} p^{\frac{1}{4}} > N^{1.55+o(1)}.$$

Заметим, что аргументы, используемые при доказательстве теоремы 1, также влекут следующее

ПРЕДЛОЖЕНИЕ 1. Для любых фиксированных положительных целых констант r и k величина $J_{2k}^{(r)}$, равная числу решений сравнения

$$\frac{1}{x_1^r} + \dots + \frac{1}{x_k^r} \equiv \frac{1}{x_{k+1}^r} + \dots + \frac{1}{x_{2k}^r} \pmod{p}, \quad x_1, \dots, x_{2k} \in I,$$

удовлетворяет оценке

$$J_{2k}^{(r)} < \left(|I|^{\frac{2k^2}{k+1}} + \frac{|I|^{2k}}{p} \right) |I|^{o(1)}.$$

В частности, получаем

СЛЕДСТВИЕ 5. Пусть r_1, r_2, k_1, k_2 – фиксированные положительные целые константы, $I_1 = [a_1 + 1, a_1 + N_1]$, $I_2 = [a_2 + 1, a_2 + N_2]$ и

$$N_1 < p^{\frac{k_1+1}{2k_1}}, \quad N_2 < p^{\frac{k_2+1}{2k_2}}.$$

Тогда для любых комплексных коэффициентов $\alpha_1(x_1), \alpha_2(x_2)$ с условием $|\alpha_i(x_i)| \leq 1$ имеет место оценка

$$\begin{aligned} \max_{(a,p)=1} \left| \sum_{x_1 \in I_1} \sum_{x_2 \in I_2} \alpha_1(x_1) \alpha_2(x_2) e_p(ax_1^{-r_1} x_2^{-r_2}) \right| \\ < \left(p^{\frac{1}{2k_1 k_2}} N_1^{-\frac{1}{k_2(k_1+1)}} N_2^{-\frac{1}{k_1(k_2+1)}} \right) (N_1 N_2)^{1+o(1)}. \end{aligned}$$

Можно применить билинейные суммы следствия 5 вместе с тождеством Вона [34] и оценить соответствующие суммы по простым числам подобно теоремам A1, A9 из работы [1] и следствию 1.5 из работы [35].

СЛЕДСТВИЕ 6. Пусть $r \in \mathbb{Z}_+$ и $p > N > p^{\frac{1}{2}+\varepsilon}$ для некоторого $\varepsilon > 0$. Тогда

$$\max_{(a,p)=1} \left| \sum_{\substack{x < N \\ x \text{ простое}}} e_p(ax^{-r}) \right| < N^{1-\delta},$$

где $\delta = \delta(\varepsilon; r) > 0$.

Далее, заметим, что результат из работы [12] влечет оценку

$$\max_{(a,p)=1} \left| \sum_{\substack{x < p \\ x \text{ простое}}} e_p(ax^{-1}) \right| < p^{\frac{15}{16}+o(1)}.$$

Следствие 5 приводит к следующему утверждению.

СЛЕДСТВИЕ 7. Для любой фиксированной положительной целой константы r имеет место оценка

$$\max_{(a,p)=1} \left| \sum_{\substack{x < p \\ x \text{ простое}}} e_p(ax^{-r}) \right| < p^{\frac{23}{24}+o(1)}.$$

ДОКАЗАТЕЛЬСТВО. Достаточно доказать, что

$$\left| \sum_{n \leq p} \Lambda(n) e_p(an^{-r}) \right| < p^{\frac{23}{24} + o(1)},$$

и тогда результат будет следовать из формулы частного суммирования. Здесь $\Lambda(n)$ обозначает функцию Мангольдта.

Далее выражение вида $A \lesssim B$ означает, что $A < Bp^{o(1)}$. Из тождества Вона (см. [36, гл. 24]) имеем

$$\sum_{n \leq p} \Lambda(n) e_p(an^{-r}) \lesssim W_1 + W_2 + W_3 + W_4,$$

где

$$\begin{aligned} W_1 &= \left| \sum_{n \leq U} \Lambda(n) e_p(an^{-r}) \right|, \quad W_2 = \sum_{n \leq UV} \left| \sum_{m \leq p/n} e_p(an^{-r} m^{-r}) \right|, \\ W_3 &= \sum_{n \leq V} \left| \sum_{m \leq p/n} (\log m) e_p(an^{-r} m^{-r}) \right|, \\ W_4 &= \sum_{U < n \leq p/V} \left| \sum_{V < m \leq p/n} \beta_m e_p(an^{-r} m^{-r}) \right|. \end{aligned}$$

Здесь $U \geq 2$, $V \geq 2$ являются параметрами, которые определяются по нашему выбору с условием $UV \leq p$,

$$\beta_m = \sum_{\substack{d|m \\ d \leq V}} \mu(d).$$

Далее будем использовать также оценку Вейля в форме

$$\left| \sum_{x=1}^{p-1} e_p(ax^{-r} + bx) \right| \ll p^{\frac{1}{2}}.$$

Более точно, мы будем пользоваться следствием этой оценки, а именно для любого интервала $I \subset \mathbb{F}_p$ имеет место оценка

$$\left| \sum_{x \in I} e_p(ax^{-r}) \right| \lesssim p^{\frac{1}{2}}.$$

Возьмем $U = V = p^{\frac{1}{3}}$ и оценим W_1 тривиально:

$$W_1 \lesssim U = p^{\frac{1}{3}}.$$

Для оценки W_2 разобьем интервал суммирования по n на диадические интервалы, и тогда для некоторого $L \leq p^{\frac{2}{3}}$ получим оценку

$$W_2 \lesssim \sum_{L \leq n \leq 2L} \left| \sum_{m \leq p/n} e_p(an^{-r} m^{-r}) \right|.$$

Если $L < p^{\frac{1}{3}}$, то применим оценку Вейля к сумме по m и получим

$$W_2 \lesssim Lp^{\frac{1}{2}} \lesssim p^{\frac{5}{6}}.$$

Если $p^{\frac{1}{3}} < L < p^{\frac{2}{3}}$, то, используя стандартный сглаживающий аргумент, распространим суммирование по m до $m \leq p/L$ и применим следствие 5 при $k_1 = k_2 = 2$. Тогда получим

$$W_2 \lesssim p^{\frac{23}{24}}.$$

Для оценки W_3 применим формулу частного суммирования к сумме по m и оценку Вейля. Тогда получим, что

$$W_3 \lesssim \sum_{n < p^{1/3}} p^{\frac{1}{2}} \lesssim p^{\frac{5}{6}}.$$

Для оценки W_4 разобьем интервал суммирования по n на диадические интервалы и получим при некотором $p^{\frac{1}{3}} < L \leq p^{\frac{2}{3}}$ оценку

$$W_4 \lesssim \sum_{L \leq n < 2L} \left| \sum_{p^{1/3} < m \leq p/n} \beta_m e_p(an^{-r}m^{-r}) \right|.$$

Применяя сглаживающий аргумент, дополняем пределы суммирования по m до $m < p/L$ и, используя следствие 5 при $k_1 = k_2 = 2$, получаем

$$W_4 \lesssim p^{\frac{23}{24}}.$$

Следствие доказано.

Список литературы

1. J. Bourgain, “More on the sum-product phenomenon in prime fields and its applications”, *Int. J. Number Theory*, **1**:1 (2005), 1–32.
2. J. Cilleruelo, M. Z. Garaev, “Concentration of points on two and three dimensional modular hyperbolas and applications”, *Geom. Funct. Anal.*, **21**:4 (2011), 892–904.
3. J. Bourgain, “Multilinear exponential sums in prime fields under optimal entropy condition on the sources”, *Geom. Funct. Anal.*, **18**:5 (2009), 1477–1502.
4. М. А. Королёв, “Неполные суммы Kloostermana и их приложения”, *Изв. РАН. Сер. матем.*, **64**:6 (2000), 41–64; англ. пер.: M. A. Korolev, “Incomplete Kloosterman sums and their applications”, *Izv. Math.*, **64**:6 (2000), 1129–1152.
5. А. А. Карацуба, “Дробные доли специального вида функций”, *Изв. РАН. Сер. матем.*, **59**:4 (1995), 61–80; англ. пер.: A. A. Karatsuba, “Fractional parts of functions of a special form”, *Izv. Math.*, **59**:4 (1995), 721–740.
6. А. А. Карацуба, “Аналоги сумм Kloostermana”, *Изв. РАН. Сер. матем.*, **59**:5 (1995), 93–102; англ. пер.: A. A. Karatsuba, “Analogues of Kloosterman sums”, *Izv. Math.*, **59**:5 (1995), 971–981.
7. R. C. Baker, “Kloosterman sums with prime variable”, *Acta Arith.*, **156**:4 (2012), 351–372.
8. Wenzhi Luo, “Bounds for incomplete hyper-Kloosterman sums”, *J. Number Theory*, **75**:1 (1999), 41–46.

9. I. E. Shparlinski, “Bounds of incomplete multiple Kloosterman sums”, *J. Number Theory*, **126**:1 (2007), 68–73.
10. D. A. Burgess, “Partial Gaussian sums”, *Bull. London Math. Soc.*, **20**:6 (1988), 589–592.
11. E. Fouvry, I. E. Shparlinski, “On a ternary quadratic form over primes”, *Acta Arith.*, **150**:3 (2011), 285–314.
12. М. З. Гараев, “Оценка сумм Клоостермана с простыми числами и применение”, *Матем. заметки*, **88**:3 (2010), 365–373; англ. пер.: M. Z. Garaev, “Estimation of Kloosterman sums with primes and its application”, *Math. Notes*, **88**:3 (2010), 330–337.
13. J. Bourgain, M. Z. Garaev, S. V. Konyagin, I. E. Shparlinski, “On congruences with products of variables from short intervals and applications”, *Ортогональные ряды, теория приближений и смежные вопросы*, Сб. статей. К 60-летию со дня рождения академика Бориса Сергеевича Кашина, Тр. МИАН, **280**, МАИК, М., 2013, 67–96; *Proc. Steklov Inst. Math.*, **280**:1 (2013), 61–90.
14. J. Friedlander, H. Iwaniec, *Opera de cribro*, Amer. Math. Soc. Colloq. Publ., **57**, Amer. Math. Soc., Providence, RI, 2010, xx+527 pp.
15. М. А. Королёв, “Короткие суммы Клоостермана с весами”, *Матем. заметки*, **88**:3 (2010), 415–427; англ. пер.: M. A. Korolev, “Short Kloosterman sums with weights”, *Math. Notes*, **88**:3 (2010), 374–385.
16. А. А. Карацуба, “Новые оценки коротких сумм Клоостермана”, *Матем. заметки*, **88**:3 (2010), 384–398; англ. пер.: A. A. Karatsuba, “New estimates of short Kloosterman sums”, *Math. Notes*, **88**:3 (2010), 347–359.
17. М. З. Гараев, “Суммы и произведения множеств и оценки рациональных тригонометрических сумм в полях простого порядка”, *УМН*, **65**:4(394) (2010), 5–66; англ. пер.: M. Z. Garaev, “Sums and products of sets and estimates of rational trigonometric sums in fields of prime order”, *Russian Math. Surveys*, **65**:4 (2010), 599–658.
18. J. Friedlander, H. Iwaniec, “The Brun–Titchmarsh theorem”, *Analytic number theory* (Kyoto, 1996), London Math. Soc. Lecture Note Ser., **247**, Cambridge Univ. Press, Cambridge, 1997, 85–93.
19. J. Maynard, “On the Brun–Titchmarsh theorem”, *Acta Arith.*, **157**:3 (2013), 249–296.
20. Y. Motohashi, “An extension of the Linnik phenomenon”, *Математика и информатика*, 1, К 75-летию со дня рождения Анатолия Алексеевича Карацубы, Совр. пробл. матем., **16**, МИАН, М., 2012, 66–75; *Proc. Steklov Inst. Math.*, **280**:suppl. 2 (2013), S56–S64.
21. U. Betke, M. Henk, J. M. Wills, “Successive-minima-type inequalities”, *Discrete Comput. Geom.*, **9**:1 (1993), 165–175.
22. T. Tao, Van H. Vu, *Additive combinatorics*, Cambridge Stud. Adv. Math., **105**, Cambridge Univ. Press, Cambridge, 2006, xviii+512 pp.
23. Ю. В. Линник, “Элементарное решение проблемы Варинга по методу Шнирельмана”, *Матем. сб.*, **12**(54):2 (1943), 225–230.
24. З. И. Борович, И. Р. Шафаревич, *Теория чисел*, Наука, М., 1964, 566 с.; англ. пер.: Z. I. Borevich, I. R. Shafarevich, *Number theory*, Pure and Applied Mathematics, **20**, Academic Press, New York–London, 1966, x+435 pp.
25. K. Ireland, M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Grad. Texts in Math., **84**, Springer-Verlag, New York, 1990, xiv+389 pp.
26. В. В. Прасолов, *Многочлены*, 2-е изд., МЦНМО, М., 2001, 335 с.; англ. пер.: V. V. Prasolov, *Polynomials*, Algorithms Comput. Math., **11**, Springer-Verlag, Berlin, 2004, xiv+301 pp.
27. D. R. Heath-Brown, “Almost-primes in arithmetic progressions and short intervals”, *Math. Proc. Cambridge Philos. Soc.*, **83**:3 (1978), 357–375.

28. J. Bourgain, M. Z. Garaev, S. V. Konyagin, I. E. Shparlinski, “On the hidden shifted power problem”, *SIAM J. Comput.*, **41**:6 (2012), 1524–1557.
29. A. Ayyad, T. Cochrane, Z. Zheng, “The congruence $x_1x_2 \equiv x_3x_4 \pmod{p}$, the equation $x_1x_2 = x_3x_4$ and mean value of character sums”, *J. Number Theory*, **59**:2 (1996), 398–413.
30. J. Friedlander, H. Iwaniec, “Estimates for character sums”, *Proc. Amer. Math. Soc.*, **119**:2 (1993), 365–372.
31. J. Bourgain, “The discretized sum-product and projection theorems”, *J. Anal. Math.*, **112**:1 (2010), 193–236.
32. M. N. Huxley, “On the difference between consecutive primes”, *Invent. Math.*, **15**:2 (1972), 164–170.
33. N. G. de Bruijn, “On the number of positive integers $\leq x$ and free of prime factors $> y$. II”, *Nederl. Akad. Wetensch. Proc. Ser. A 69=Indag. Math.*, **28** (1966), 239–247.
34. R. C. Vaughan, “Sommes trigonométriques sur les nombres premiers”, *C. R. Acad. Sci. Paris Sér. A*, **285**:16 (1977), 981–983.
35. E. Fouvry, Ph. Michel, “Sur certaines sommes d’exponentielles sur les nombres premiers”, *Ann. Sci. École Norm. Sup. (4)*, **31**:1 (1998), 93–130.
36. H. Davenport, *Multiplicative number theory*, 3rd ed., Grad. Texts in Math., **74**, Springer-Verlag, New York, 2000, xiv+177 pp.

ЖАН БУРГЕЙН

(JEAN BOURGAIN)

Institute for Advanced Study, School of Mathematics,
Princeton, NJ, USA

E-mail: bourgain@ias.edu

Поступило в редакцию

20.11.2012

22.07.2013

МУБАРИЗ ЗАФАР ОГЛЫ ГАРАЕВ

(MUBARIZ Z. GARAEV)

National Autonomous University of Mexico,
campus Morelia, Center of Mathematical Sciences,
Mexico

E-mail: garaev@matmor.unam.mx