ЧЕБЫШЕВСКИЙ СБОРНИК
Том 17 Выпуск 4

УДК 511.321 DOI 10.22405/2226-8383-2016-17-4-79-109

МЕТОДЫ ОЦЕНОК КОРОТКИХ СУММ КЛООСТЕРМАНА[1]

М. А. Королёв (г. Москва)

Аннотация

Настоящий обзор представляет собой развёрнутое содержание мини-курса, прочитанного автором в ноябре 2015 г. во время "Китайско-Российского симпозиума по тригонометрическим суммам и суммам множеств". Это мероприятие, проходившее в Академии математики и системных наук (Пекин), было организовано профессорами Чаохуа Жиа (Институт математики Китайской академии наук) и Ке Гонгом (Университет Хенань), которым автор приносит глубокую благодарность за всяческую поддержку и гостеприимство.

Обзор состоит из Введения, трёх частей и Заключения. Во Введении даются определения и приводятся основные факты, связанные с оценками полных сумм Клоостермана.

В первой части излагается метод оценки неполных сумм Клоостермана по специальному модулю, равному растущей степени фиксированного простого числа. Этот метод основан на идее А. Г. Постникова, которая сводит оценку таких сумм к оценкам тригонометрических сумм с многочленом в показателе экспоненты с помощью теоремы о среднем И. М. Виноградова.

Во второй части излагается метод А. А. Карацубы оценок неполных сумм Клоостермана по произвольному модулю, который основан на весьма точной оценке числа решений симметричного сравнения, содержащего обратные величины по заданному модулю. Эта оценка играет в рассматриваемых здесь вопросах ту же роль, что и теорема о среднем И. М. Виноградова при оценке соответствующих тригонометрических сумм.

В третьей части излагается метод Ж. Бургейна и М. З. Гараева, в основе которого лежит глубокая теорема об "оценке сумм-произведений", а также уточнение оценки А. А. Карацубы числа решений симметричного сравнения.

В Заключении сформулирован ряд новых результатов об оценках коротких сумм Клоостермана, полученных в последние годы, доказательства которых не вошли в настоящий обзор.

Ключевые слова: обратные вычеты, неполные суммы Клоостермана, метод Постникова, метод Карацубы, метод Бургейна-Гараева, теорема Виноградова о среднем, оценка сумм-произведений.

Библиография: 57 названий.

METHODS OF ESTIMATING OF INCOMPLETE KLOOSTERMAN SUMS

M. A. Korolev (Moscow)

Abstract

[1]Исследование выполнено за счет гранта Российского научного фонда (проект 14-11-00433

This survey contains enlarged version of a mini-course which was read by the author in November 2015 during “Chinese - Russian workshop of exponential sums and sumsets”. This workshop was organized by professors Chaohua Jia (Institute of Mathematics, Academia Sinica) and Ke Gong (Henan University) in Academy of Mathematics and System Science, CAS (Beijing). The author is warmly grateful to them for the support and hospitality.

The survey contains the Introduction, three parts and Conclusion. The basic definitions and results concerning the complete Kloosterman sums are given in the Introduction.

The method of estimating of incomplete Kloosterman sums to moduli equal to the raising power of a fixed prime is described in the first part. This method is based on one idea of A. G. Postnikov which reduces the estimate of such sums to the estimate of the exponential sums with polynomial by I. M. Vinogradov's mean value theorem.

A. A. Karatsuba's method of estimating of incomplete sums to an arbitrary moduli is described in the second part. This method is based on a very precise estimate of the number of solutions of one symmetric congruence involving inverse residues to a given modulus. This estimate plays the same role in thie problems under considering as Vinogradov's mean value theorem in the estimating of corresponding exponential sums.

The method of J. Bourgain and M. Z. Garaev is described in the third part. This method is based on very deep “sum-product estimate” and on the improvement of A. A. Karatsuba's bound for the number of solutions of symmetric congruence.

The Conclusion contains a series of recent results concerning the estimates of short Kloosterman sums.

Keywords: inverse residues, incomplete Kloosterman sums, method of Postnikov, method of Karatsuba, method of Bourgain and Garaev, Vinogradov's mean value theorem, sum-product estimate.

Bibliography: 57 titles.

Введение

Пусть $q \geqslant 2$ — целое число, и пусть $(m,q)=1$. Всюду ниже через m^*, $\overline{m}$ и $1/m$ будем обозначать вычет, обратный к m по модулю q: $mm^* \equiv m\overline{m} \equiv 1 (\mathrm{mod}\ q)$. Пусть, далее, $(a,q)=1$. Выражение

$$S(q)=S(q;a,b)=\sum_{\substack{m=1\\(m,q)=1}}^{q} e_q\bigl(am^*+bm\bigr)=\sum_{m=1}^{q}{}' e_q\bigl(am^*+bm\bigr), \quad e_q(v)=e^{2\pi i v/q},$$

называется *полной* суммой Клоостермана по модулю q. Пусть $\mathcal{A}$ — подмножество приведённой системы вычетов $\mathbb{Z}_q^*$ по модулю q с числом элементов $|\mathcal{A}|<\varphi(q)$. Сумму вида

$$S(q;\mathcal{A})=S(q;\mathcal{A};a,b)=\sum_{m\in\mathcal{A}} e_q\bigl(am^*+bm\bigr)$$

будем называть *неполной* суммой Клоостермана. В случае, когда $|\mathcal{A}|<\sqrt{q}$, сумму $S(q;\mathcal{A})$ условимся называть *короткой*. Для решения многих задач теории чисел необходимы нетривиальные оценки коротких сумм $S(q;\mathcal{A})$ вида $|S(q;\mathcal{A})|<|\mathcal{A}|\Delta$, где $\Delta=\Delta(q)\to 0$. Прежде чем перейти к изложению методов оценок таких сумм, упомянем основные результаты, связанные с суммами Клоостермана $S(q;\mathcal{A})$, для которых $\sqrt{q}\ll|\mathcal{A}|\leqslant q$. В свою очередь, их оценка опирается на оценки полных сумм $S(q)$.

Теорема 1. *Полные суммы Клоостермана $S(q)$ мультипликативны по q.*

Доказательство. Действительно, пусть $q=q_1q_2$, где $(q_1,q_2)=1$, и пусть y и z пробегают приведённые системы вычетов по модулям q_1 и q_2 соответственно. Тогда величина

$x = yq_2 + zq_1$ пробегает приведённую систему вычетов $\mathbb{Z}_q^*$ по модулю q. Определим величину w соотношением $w = \overline{y}\,\overline{q}_2^2 q_2 + \overline{z}\,\overline{q}_1^2 q_1$, в котором

$$y\overline{y} \equiv q_2\overline{q}_2 \equiv 1 (\mathrm{mod}\ q_1), \quad z\overline{z} \equiv q_1\overline{q}_1 \equiv 1 (\mathrm{mod}\ q_2).$$

Тогда

$$xw \equiv y\overline{y}(q_2\overline{q}_2)^2 \equiv 1 (\mathrm{mod}\ q_1), \quad xw \equiv z\overline{z}(q_1\overline{q}_1)^2 \equiv 1 (\mathrm{mod}\ q_2),$$

так что $xw \equiv 1 (\mathrm{mod}\ q)$. Следовательно, $w \equiv x^* (\mathrm{mod}\ q)$. Таким образом,

$$S(q;a,b) = \sideset{}{'}\sum_{y=1}^{q_1}\sideset{}{'}\sum_{z=1}^{q_2} e_{q_1q_2}\big(a(\overline{y}\,\overline{q}_2^2 q_2 + \overline{z}\,\overline{q}_1^2 q_1) + b(yq_2 + zq_1)\big) =$$

$$= \sideset{}{'}\sum_{y=1}^{q_1} e_{q_1}\big(a_1\overline{y} + by\big)\sideset{}{'}\sum_{z=1}^{q_2} e_{q_2}\big(a_2\overline{z} + bz\big) = S(q_1;a_1,b)S(q_2;a_2,b),$$

где $a_1 \equiv a\overline{q}_2^2 (\mathrm{mod}\ q_1)$, $a_2 \equiv a\overline{q}_1^2 (\mathrm{mod}\ q_2)$. □

Итак, достаточно получить оценку $|S(q)|$ для случая, когда $q = p^n$, где p — простое, $n \geqslant 1$. Если $n \geqslant 2$, то суммы $S(p^n)$ вычисляются в явном виде (см. [1], а также [2], [3]). В этом можно убедиться, если представить переменную суммирования m в виде $k + pl$, где величины k и l независимо друг от друга пробегают промежутки $1 \leqslant k < p$, $0 \leqslant l < p^{n-1}$, после чего рассмотреть отдельно случаи чётных и нечётных n и p соответственно. При этом оказывается, что $|S(p^n)| \leqslant cp^{n/2}$ для некоторой постоянной c, такой, что $c \leqslant \tau(p^n)$ (здесь и далее через $\tau(q)$ обозначается функция делителей).

Наиболее сложным оказывается случай, когда $q = p$ — простое число. Первая нетривиальная оценка величины $S(p)$ была найдена Г. Д. Клоостерманом [4].

Теорема 2. *Для простого p справедлива оценка $|S(p)| \leqslant 3^{1/4}p^{3/4}$.*

Доказательство. Пусть $(t,p) = 1$. Так как m и tm одновременно пробегают приведённую систему вычетов по модулю p, то

$$|S(p)|^2 = \left|\sum_{m=1}^{p-1} e_p\big(at^*m^* + btm\big)\right|^2.$$

Суммируя обе части по t, получим:

$$(p-1)|S(p)|^2 = \sum_{t=1}^{p-1}\left|\sum_{m=1}^{p-1} e_p(at^*m^* + btm)\right|^2.$$

Далее, применяя неравенство Коши, будем иметь:

$$(p-1)^2|S(p)|^4 \leqslant (p-1)\sum_{t=1}^{p-1}\left|\sum_{m=1}^{p-1} e_p(at^*m^* + btm)\right|^4 \leqslant (p-1)\sum_{t_1,t_2=1}^{p}\left|\sum_{m=1}^{p-1} e_p(at_1m^* + bt_2m)\right|^4 =$$

$$= (p-1)\sum_{t_1,t_2=1}^{p}\ \sum_{m_1,m_2,n_1,n_2=1}^{p-1} e_p(at_1(m_1^* + m_2^* - n_1^* - n_2^*) + bt_2(m_1 + m_2 - n_1 - n_2)) =$$

$$= p^2(p-1)I(p),$$

где $I(p)$ обозначает число решений системы сравнений

$$\begin{cases} m_1^* + m_2^* \equiv n_1^* + n_2^* \ (\mathrm{mod}\ p), \\ m_1 + m_2 \equiv n_1 + n_2 \ (\mathrm{mod}\ p). \end{cases}$$

Зафиксируем пару (m_1, m_2). Тогда

$$\begin{cases} n_1^* + n_2^* \equiv \lambda (\mathrm{mod}\ p), \\ n_1 + n_2 \equiv \mu (\mathrm{mod}\ p) \end{cases} \quad \text{или, что то же,} \quad \begin{cases} \lambda n_1 n_2 \equiv \mu (\mathrm{mod}\ p), \\ n_1 + n_2 \equiv \mu (\mathrm{mod}\ p) \end{cases}$$

для соответствующих λ и μ. Если $\lambda \equiv 0 (\mathrm{mod}\ p)$, то $\mu \equiv 0 (\mathrm{mod}\ p)$, так что $m_2 \equiv -m_1 (\mathrm{mod}\ p)$, $n_2 \equiv -n_1 (\mathrm{mod}\ p)$. Вклад от таких решений в $I(p)$ равен $(p-1)^2$. Если же $\lambda \not\equiv 0 (\mathrm{mod}\ p)$, то $\mu \not\equiv 0 (\mathrm{mod}\ p)$ и $\lambda n_1^2 - \lambda \mu n_1 + \mu \equiv 0 (\mathrm{mod}\ p)$. Последнее сравнение имеет не более двух решений, так что окончательно находим:

$$I(p) \leqslant (p-1)^2 + 2(p-1)(p-2) < 3p(p-1)$$

и, следовательно,

$$(p-1)^2 |S(p)|^4 \leqslant p^2 (p-1) \cdot 3p(p-1), \quad |S(p)|^4 \leqslant 3p^3. \quad \square$$

Замечание. Различные варианты доказательства оценки $S(p) \ll p^{3/4}$ были предложены И. М. Виноградовым [5], [7], Д. Р. Хизбрауном [24], Д. И. Толевым [8].

Впоследствии показатель $3/4$ в теореме 2 был уменьшен Г. Салье [9] и независимо Г. Дэвенпортом [10] до $2/3$. В 1948 г. А. Вейль [11], используя методы алгебраической геометрии, получил наилучшую возможную оценку $|S(p)| \leqslant 2\sqrt{p}$. Элементарное (хотя всё ещё достаточно сложное) доказательство этого факта было найдено С. А. Степановым [12] (также см. [13]).

Из перечисленных выше результатов и теоремы 1 следует неравенство

$$|S(q; a, b)| \leqslant \tau(q) \sqrt{q}. \tag{1}$$

С его помощью можно оценить и неполную сумму Клоостермана в случае, когда переменная суммирования пробегает сплошной интервал. Имеет место

Теорема 3. *Пусть $1 < x < q$. Тогда для суммы*

$$S(x) = S(q; x) = \sum_{\substack{1 \leqslant m \leqslant x \\ (m,q)=1}} e_q(am^* + bm).$$

из (1) *следует оценка*

$$|S(x)| \leqslant \tau(q) \sqrt{q}\, (\log q + 1). \tag{2}$$

Доказательство. Действительно, полагая $N = [x]$, будем иметь:

$$\begin{aligned} S(x) &= \sideset{}{'}\sum_{m=1}^{q} \Bigg(\sum_{\ell=1}^{N} \frac{1}{q} \sum_{|c| \leqslant q/2} e_q(c(m-\ell)) \Bigg) e_q(am^* + bm) = \\ &= \frac{1}{q} \sum_{|c| \leqslant q/2} \Bigg(\sum_{\ell=1}^{N} e_q(-c\ell) \Bigg) \sideset{}{'}\sum_{m=1}^{q} e_q(am^* + (b+c)m) = \\ &= \frac{N}{q} S(q; a, b) + \frac{1}{q} \sum_{1 \leqslant |c| \leqslant q/2} e_q(-c) \frac{e_q(-cN) - 1}{e_q(-c) - 1} S(q; a, b+c). \end{aligned}$$

Переходя к неравенствам, получим:

$$|S(x)| \leqslant \left(\frac{N}{q} + \frac{1}{q}\sum_{1\leqslant|c|\leqslant q/2}\left(\sin\frac{\pi|c|}{q}\right)^{-1}\right)\tau(q)\sqrt{q} \leqslant$$
$$\leqslant \left(1 + \frac{2}{q}\sum_{1\leqslant c\leqslant q/2}\frac{q}{2c}\right)\tau(q)\sqrt{q} \leqslant \tau(q)\sqrt{q}\,(\log q + 1). \quad \square$$

Поскольку $\tau(q) \ll_\varepsilon q^\varepsilon$ для любого фиксированного $\varepsilon > 0$, то оценка (2) нетривиальна при $x \geqslant q^{0.5+\varepsilon}$.

В начале 1990-х гг. А. А. Карацуба [14] – [16] разработал новый метод, с помощью которого ему удалось получить первые нетривиальные оценки коротких сумм Клоостермана с числом слагаемых порядка q^α, где $0 < \alpha < 0.5$ (см. также [17] – [19]). Метод Карацубы излагается далее в §2.

А. А. Карацубе принадлежит и важное замечание, согласно которому в случае специального модуля вида $q = p^n$, где p — фиксированное простое число, а $n \to +\infty$, оценки неполных сумм Клоостермана могут быть получены с помощью метода А. Г. Постникова [20]. Число слагаемых в таких суммах может иметь порядок $e^{c(\log q)^{2/3}}$, где c — достаточно большая положительная постоянная. Этому методу посвящён §1.

Первые оценки сумм $S(x)$, полученные с помощью метода Карацубы, давали нетривиальное понижение при $x \geqslant q^\varepsilon$, где $\varepsilon > 0$ — произвольное фиксированное число (см. [17]). Нижняя граница этого диапазона была впоследствии снижена до такой: $x \geqslant e^{(\log q)^{4/5}(\log\log q)^5}$ (см. [22]). Однако А. А. Карацуба неоднократно высказывал предположение о том, что его метод позволяет получать нетривиальные оценки сумм $S(x)$ по сплошному промежутку вида $1 \leqslant n \leqslant x$ уже при $x \geqslant e^{(\log q)^{2/3+\varepsilon}}$. Первые оценки столь коротких сумм для простого модуля q были найдены Ж. Бургейном и М. З. Гараевым [23] (2012). Они опирались на очень глубокую и сложную теорему Бургейна об оценке полилинейной тригонометрической суммы достаточно общего вида, а также на некоторые факты из геометрии чисел. Набросок метода Бургейна и Гараева излагается в §3.

По ряду причин мы практически не касаемся здесь приложений сумм Клоостермана к задачам теории чисел. Краткий обзор такого рода приложений можно найти в статье Д. Р. Хизбрауна [24] и монографии А. В. Устинова [25]. Также представляется уместным упомянуть серию незаслуженно забытых работ И. М. Виноградова [5] – [7], [26], [27], посвящённых оценкам сумм Клоостермана и некоторых их обобщений. Для простоты изложения в §§2,3 мы рассматриваем лишь случай простого модуля q. Это позволяет избежать ряда технических трудностей.

1. Метод Постникова

1.1. Предварительные замечания

В 1955 г. А. Г. Постников [20] обнаружил, что индекс числа $1 + pu$ по модулю $q = p^n$, где p — нечётное простое, представляется некоторым полиномом степени $(n-1)$ от переменной u:

$$\frac{\operatorname{ind}(1+pu)}{p-1} \equiv f(u) \pmod{p^{n-1}}, \qquad f(u) = a_1u + a_2u^2 + \ldots + a_{n-1}u^{n-1}. \tag{3}$$

Поскольку всякий неглавный характер χ по модулю q имеет вид

$$\chi(a) = \exp\left(\frac{2\pi i c \operatorname{ind}(a)}{\varphi(p^n)}\right) = \exp\left(\frac{2\pi i c \operatorname{ind}(a)}{p^{n-1}(p-1)}\right), \quad 1 \leqslant c < \varphi(p^n),$$

то соотношение (3) сводит многие задачи, связанные с оценками сумм характеров Дирихле к оценкам тригонометрических сумм с многочленом в экспоненте. К последним же можно применить всю мощь метода И. М. Виноградова. Это обстоятельство позволило, в частности, построить примеры сумм вида

$$W = W_q(\chi; N, M) = \sum_{a=M+1}^{M+N} \chi(a),$$

которые допускают нетривиальную оценку уже при очень малом числе N слагаемых. Так, теорема Постникова позволила получать такие оценки в случае, когда $N \geqslant e^{c(\log q)^{3/4}(\log\log q)^{3/4}}$, $q = p^n$, $p \to +\infty$ и показатель n должным образом зависит от p (см. [20], [21] а также работы [28], [29], в которых оценка Постникова распостранялась на случай фиксированного простого $p \geqslant 3$ и $q = p^n$, $n \to +\infty$). Последующие работы А. А. Карацубы [30] и В. Н. Чубарикова [31] позволили заменить нижнюю границу N величиной $e^{c(\log q)^{2/3}(\log\log q)^{1/3}}$. Для сравнения: в случае, когда модуль q — простое число, наилучшей для $W_q(\chi; N, M)$ (в смысле длины промежутка суммирования) остаётся оценка Д. Берджесса вида $|W| \leqslant Nq^{-c\varepsilon^2}$, справедливая при $N \geqslant q^{1/4+\varepsilon}$ (см. [32]- [34]).

Ещё одним примером задачи, в которой специфика модуля позволяет получать очень точные результаты, является задача об оценке суммы значений неглавного характера Дирихле на последовательности "сдвинутых" простых чисел, т.е. суммы

$$V = V_q(\chi; N, a) = \sum_{p \leqslant N} \chi(p + a),$$

где $(a, q) = 1$. В случае простого модуля q наилучшей на сегодняшний день является оценка $V \ll Nq^{-c\varepsilon^2}$, полученная А. А. Карацубой [35] в предположении $N \geqslant q^{1/2+\varepsilon}$. В то же время в случае нечётного простого p и $q = p^n$ та сумма допускает нетривиальную оценку уже при $N \geqslant e^{c(\log q)^{2/3}}$ (см. работы [36], [37], в которых такие оценки получены при $N \geqslant q^{\varepsilon}$).

Формула (3) является "конечным" аналогом разложения

$$\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots, \quad |x| < 1.$$

"Конечный" аналог ряда

$$\frac{1}{1 + x} = 1 - x + x^2 - x^3 + \ldots, \quad |x| < 1,$$

для величины $(1 + pu)^*$ имеет более простой вид (лемма 1). Поэтому, применяя к неполным суммам Клоостермана по модулю $q = p^n$ технику всех перечисленных работ, можно получать их нетривиальные оценки в случаях, когда длина N суммы очень мала по сравнению с модулем.

Отметим, что сумма Клоостермана является простейшим примером тригонометрической суммы с рациональной функцией, т.е. суммы вида

$$\sum_{c < \nu \leqslant c+N} e_q\left(\frac{f(\nu)}{g(\nu)}\right),$$

где f, g – взаимно простые полиномы степеней $k \geqslant 1$, $\ell \geqslant 1$. Для таких сумм С.А. Степанов и И.Е. Шпарлинский в случае $q = p^n$ в работе [38] получили оценки, нетривиальные при $N \geqslant q^{\varepsilon}$ (фактически - уже при $N \geqslant e^{(\log q)^{2/3+\varepsilon}}$).

Ниже мы получим ряд оценок неполных сумм Клоостермана и их аналогов для случая, когда модуль $q = p^n$ является растущей степенью фиксированного нечётного простого числа

p. Отметим, что наряду с аналогом формулы (3) Постникова и теоремы "о среднем" И. М. Виноградова мы пользуемся т.н. "сдвигом" переменной суммирования. Этот приём восходит к И. М. Виноградову, но впервые был применён к задачам с характерами Дирихле по модулю p^n А. А. Карацубой.

1.2. Вспомогательные утверждения

Лемма 1. *Пусть p — простое число, $n \geqslant 2$, $q = p^n$, и пусть $1 \leqslant s \leqslant n$. Тогда*

$$(1+up^s)^* \equiv 1 - up^s + (up^s)^2 - \ldots + (-1)^m (up^s)^m (\mathrm{mod}\ q),$$

где m — наименьшее целое, удовлетворяющее неравенству $(m+1)s \geqslant n$.

Доказательство. Утверждение леммы следует из легко проверяемого соотношения

$$(1+up^s)(1 - up^s + (up^s)^2 - \ldots + (-1)^m (up^s)^m) \equiv 1 (\mathrm{mod}\ q).$$

Лемма 2. *Пусть a_n, b_n, $n = 1, 2, \ldots, N$, — произвольные комплексные числа, $k \geqslant 2$. Тогда*

$$\left(\sum_{n=1}^{N} |a_n|\right)^k \leqslant N^{k-1} \sum_{n=1}^{N} |a_n|^k;$$

$$\left(\sum_{n=1}^{N} |a_n b_n|\right)^k \leqslant \left(\sum_{n=1}^{N} |a_n|\right)^{k-1} \sum_{n=1}^{N} |a_n|\,|b_n|^k;$$

$$\left(\sum_{n=1}^{N} |a_n b_n|\right)^2 \leqslant \left(\sum_{n=1}^{N} |a_n|^2\right)\left(\sum_{n=1}^{N} |b_n|^2\right).$$

Лемма 3. *Пусть $P \geqslant 1, \alpha$ — произвольные вещественные числа. Тогда*

$$\left|\sum_{1 \leqslant n \leqslant P} e(\alpha n)\right| \leqslant \min\left(P, \frac{1}{2\|\alpha\|}\right),$$

где через $\|\alpha\|$ обозначено расстояние от α до ближайшего целого числа.

Лемма 4. *Пусть*

$$\alpha = \frac{a}{q} + \frac{\theta}{q^2}, \quad (a,q) = 1, \quad q \geqslant 1, \quad |\theta| \leqslant 1.$$

Тогда для любых вещественных чисел $\beta, U > 0, P \geqslant 1$ справедливо неравенство

$$\sum_{1 \leqslant n \leqslant P} \min\left(U, \|\alpha n + \beta\|^{-1}\right) \leqslant 6\left(\frac{P}{q} + 1\right)(U + q \log q).$$

Обозначим через $J_{k,n}(P)$ число решений системы уравнений

$$\begin{cases} x_1 + \ldots + x_k = x_{k+1} + \ldots + x_{2k}, \\ \ldots \\ x_1^n + \ldots + x_k^n = x_{k+1}^n + \ldots + x_{2k}^n \end{cases}$$

в целых числах $1 \leqslant x_1, \ldots, x_{2k} \leqslant P$.

Лемма 5 (теорема И.М. Виноградова "о среднем"). *Пусть $\tau \geqslant 1$, $k \geqslant n\tau$, $P \geqslant 1$ — целые числа. Тогда*

$$J_{k,n}(P) \leqslant D(n,\tau) P^{2k - \Delta(n;\tau)},$$

где

$$D(n,\tau) = (n\tau)^{6n\tau} (2n)^{4n(n+1)\tau}, \quad \Delta(n,\tau) = \frac{n(n+1)}{2}\left(1 - \left(1 - \frac{1}{n}\right)^{\tau}\right).$$

Доказательство лемм 2–5, см., например, в книге А. А. Карацубы [39].

1.3. Основная теорема

Теорема 4. *Пусть $p \geqslant 2$ — фиксированное простое число, $(a,p)=1$, $n \geqslant 72$, $q=p^n$, и пусть $N=q^{1/\varrho}$, где $3 \leqslant \varrho \leqslant n/24$. Тогда для суммы*

$$S = \sum_{\mu<\nu\leqslant\mu+N}{}' e_q\big(a\nu^* + b\nu\big)$$

справедлива оценка $|S| \leqslant 6N^{1-c/\varrho^2}$, $c=13^{-4}$, равномерная по параметру μ, $1 \leqslant \mu \leqslant q$.

Доказательство. Не ограничивая общности, можем считать, что $\mu \equiv 0 (\mathrm{mod}\ p)$. Выполнения этого условия можно добиться сдвигом области суммирования на величину, не превосходящую $0.5p$. Далее, будем считать сперва, что $\mu+N<q$. Положим $h=[N^{0.25}]$, $s=[n/(4\varrho)]+1$. Тогда

$$S = \sum_{1\leqslant\nu+p^sxy\leqslant N}{}' e_q\big(a(\nu+\mu+p^sxy)^* + b(\nu+\mu+p^sxy)\big) =$$

$$= e_q(b(\nu+\mu)) \sum_{1\leqslant\nu\leqslant N}{}' e_q(a(\nu+\mu+p^sxy)^* + bp^sxy\big) + 2\theta p^sxy$$

для любых $1 \leqslant x,y \leqslant h$ и некоторого $|\theta| \leqslant 1$. Суммируя по x,y, будем иметь:

$$|S| \leqslant \frac{1}{h^2} \sum_{1\leqslant\nu\leqslant N}{}' \left| \sum_{x,y=1}^{h} e_q\big(a(\nu+\mu+p^sxy)^* + bp^sxy\big)\right| + 2p^sh^2.$$

Далее, выберем и зафиксируем то значение ν, для которого модуль соответствующей суммы по x,y будет наибольшим, и положим $u=(\mu+\nu)^*$. Так как $p|\mu$ и $(\nu,p)=1$ то $(u,p)=1$. Следовательно,

$$|S| \leqslant Nh^{-2}\left| \sum_{x,y=1}^{h} e_q\big(a(\overline{u}+p^sxy)^* + bp^sxy\big)\right| + 2p^sh^2.$$

Возьмём теперь $m=\big[4\varrho\big]+1$. Тогда $(m+1)s \geqslant n$, так что в силу леммы 1 имеем

$$a(\overline{u}+p^sxy)^* \equiv au - au^2p^sxy + au^3p^{2s}(xy)^2 - \ldots + (-1)^m au^{m+1}p^{ms}(xy)^m (\mathrm{mod}\ q).$$

Значит, $|S| \leqslant Nh^{-2}|W| + 2p^sh^2$, где

$$W = \sum_{x,y=1}^{h} e(\alpha_1xy + \alpha_2(xy)^2 + \ldots + \alpha_m(xy)^m),$$

$$\alpha_r = \frac{a_r}{q_r}, \qquad q_r = p^{n-rs}, \quad a_1 \equiv b - au^2 (\mathrm{mod}\ q), \quad a_r \equiv a(-u)^{r+1} (\mathrm{mod}\ q), \ \ r \geqslant 2,$$

причём $(a_r,q_r)=1$ при $r \geqslant 2$. Возьмём некоторое целое $\tau \geqslant 1$ и обозначим $k=m\tau$. Согласно лемме 2,

$$|W|^{2k} \leqslant h^{2k-1}\sum_{x=1}^{h}\left| \sum_{y=1}^{h} e(\alpha_1xy + \alpha_2(xy)^2 + \ldots + \alpha_m(xy)^m)\right|^{2k} =$$

$$= h^{2k-1}\sum_{x=1}^{h}\sum_{\lambda_1,\ldots,\lambda_m} J_{k,m}(\lambda_1,\ldots,\lambda_m) e(\alpha_1\lambda_1x + \alpha_2\lambda_2x^2 + \ldots + \alpha_m\lambda_mx^m),$$

где $J_{k,m}(\lambda_1,\ldots,\lambda_m)$ — число решений системы уравнений

$$\begin{cases} y_1+\ldots+y_k \;=\; y_{k+1}+\ldots+y_{2k}+\lambda_1, \\ \ldots \\ y_1^m+\ldots+y_k^m \;=\; y_{k+1}^m+\ldots+y_{2k}^m+\lambda_m \end{cases} \tag{4}$$

в целых числах $1\leqslant y_1,\ldots,y_{2k}\leqslant h$. Возводя обе части неравенства

$$|W|^{2k} \;\leqslant\; h^{2k-1}\sum_{\lambda_1,\ldots,\lambda_m} J_{k,m}(\lambda_1,\ldots,\lambda_m)\left|\sum_{x=1}^{h} e(\alpha_1\lambda_1 x+\alpha_2\lambda_2 x^2+\ldots+\alpha_m\lambda_m x^m)\right|$$

в степень $2k$ и применяя лемму 2, будем иметь:

$$|W|^{4k^2} \;\leqslant\; h^{2k(2k-1)}\Bigl(\sum_{\lambda_1,\ldots,\lambda_m} J_{k,m}(\lambda_1,\ldots,\lambda_m)\Bigr)^{2k-1}\times$$
$$\times\sum_{\lambda_1,\ldots,\lambda_m} J_{k,m}(\lambda_1,\ldots,\lambda_m)\left|\sum_{x=1}^{h} e(\alpha_1\lambda_1 x+\alpha_2\lambda_2 x^2+\ldots+\alpha_m\lambda_m x^m)\right|^{2k}.$$

Поскольку

$$\sum_{\lambda_1,\ldots,\lambda_m} J_{k,m}(\lambda_1,\ldots,\lambda_m) \;=\; h^{2k},\quad J_{k,m}(\lambda_1,\ldots,\lambda_m)\;\leqslant\; J_{k,m}(h),$$

то

$$|W|^{4k^2} \;\leqslant\; h^{4k(2k-1)}J_{k,m}(h)\sum_{\lambda_1,\ldots,\lambda_m}\left|\sum_{x=1}^{h} e(\alpha_1\lambda_1 x+\alpha_2\lambda_2 x^2+\ldots+\alpha_m\lambda_m x^m)\right|^{2k}.$$

Из (4) следует, что $|\lambda_r|<\Lambda_r=kh^r$, $r=1,\ldots,m$. Суммируя теперь по сплошным интервалам вида $|\lambda_r|<\Lambda_r$ в последнем соотношении и пользуясь леммой 3, получим:

$$|W|^{4k^2} \;\leqslant\; h^{4k(2k-1)}J_{k,m}(h)\sum_{\substack{|\lambda_r|<\Lambda_r\\ r=1,\ldots,m}}\;\sum_{\mu_1,\ldots,\mu_m} J_{k,m}(\mu_1,\ldots,\mu_m)e(\alpha_1\lambda_1\mu_1+\ldots+\alpha_m\lambda_m\mu_m)\;\leqslant$$
$$\leqslant h^{4k(2k-1)}J_{k,m}(h)\sum_{\mu_1,\ldots,\mu_m} J_{k,m}(\mu_1,\ldots,\mu_m)\prod_{r=1}^{m}\left|\sum_{|\lambda_r|<\Lambda_r} e(\alpha_r\lambda_r\mu_r)\right|\;\leqslant$$
$$\leqslant\; h^{4k(2k-1)}J_{k,m}^2(h)\prod_{r=1}^{m}\sum_{|\mu_r|<\Lambda_r}\left|\sum_{|\lambda_r|<\Lambda_r} e(\alpha_r\lambda_r\mu_r)\right|\;\leqslant$$
$$\leqslant\; h^{4k(2k-1)}J_{k,m}^2(h)\prod_{r=1}^{m}\sum_{|\mu_r|<\Lambda_r}\min\left(2\Lambda_r,\frac{1}{\|\alpha_r\mu_r\|}\right).$$

В силу леммы 4, сумма по μ_r не превосходит

$$6\left(\frac{2\Lambda_r}{q_r}+1\right)(2\Lambda_r+q_r\log q_r)\;<\;(2\Lambda_r)^2\delta_r,$$
$$\delta_r=6(\log q)\left(\frac{1}{\Lambda_r}+\frac{1}{q_r}+\frac{q_r}{4\Lambda_r^2}\right)\;=\;6(\log q)\left(\frac{1}{\sqrt{q_r}}\;+\;\frac{\sqrt{q_r}}{2\Lambda_r}\right)^2.$$

Вместе с тем, эта сумма не превосходит, очевидно, $(2\Lambda_r)^2$. Поэтому

$$|W|^{4k^2}\;\leqslant\; h^{4k(2k-1)}J_{k,m}^2(h)\Delta\prod_{r=1}^{m}(2\Lambda_r)^2,\quad \Delta=\prod_{r=1}^{m}\Delta_r,$$

где $\Delta_r = \min(1, \delta_r)$.

Далее, полагая $k = m\tau$ в лемме 5, находим, что

$$J_{k,m}(h) \leqslant k^{6k}(2m)^{4k(m+1)} h^{2k - \frac{m(m+1)}{2}\left(1 - \left(1 - \frac{1}{m}\right)^{\tau}\right)}.$$

Поскольку

$$\prod_{r=1}^{m} (2\Lambda_r)^2 = (2k)^{2m} h^{m(m+1)},$$

то

$$|W|^{4k^2} \leqslant k^{12k}(2k)^{2m}(2m)^{8k(m+1)} h^{8k^2 + m(m+1)\left(1 - \frac{1}{m}\right)^{\tau}} \Delta.$$

Пусть теперь $r_1 = [2\varrho], r_2 = [3\varrho]$, и пусть $r_1 < r \leqslant r_2$. Тогда

$$n \leqslant r\frac{n}{2\varrho} \leqslant r\left(s + \frac{n}{4\varrho}\right), \quad \text{откуда} \quad n - rs \leqslant \frac{rn}{4\varrho}, \quad q_r = p^{n-rs} \leqslant p^{\frac{rn}{4\varrho}} = N^{r/4} \leqslant h^r,$$

так что

$$q_r \leqslant 2\Lambda_r \quad \text{и} \quad \frac{\sqrt{q_r}}{2\Lambda_r} < \frac{1}{\sqrt{q_r}}.$$

Поэтому при любом r, $r_1 < r \leqslant r_2$, выполняется оценка:

$$\delta_r < 6(\log q)\left(\frac{1}{\sqrt{q_r}} + \frac{1}{\sqrt{q_r}}\right)^2 = 24(\log q)q_r^{-1} = 24(\log q)p^{rs-n}.$$

Так находим:

$$\Delta < \prod_{r=r_1+1}^{r_2} 24(\log q)p^{rs-n} = (24\log q)^{r_2-r_1} p^{(r_2-r_1)v},$$

где

$$v = \frac{s}{2}(r_1 + r_2 + 1) - n \leqslant \frac{1}{2}\left(\frac{n}{4\varrho} + 1\right)(5\varrho + 3) - n = -\frac{3n}{8} + \frac{3n}{8\varrho} + \frac{5\varrho}{2} + \frac{3}{2}.$$

По условию теоремы, $3 \leqslant \varrho n/24$. Поэтому

$$\frac{3n}{8\varrho} \leqslant \frac{n}{8}, \quad \frac{5\varrho}{2} + \frac{3}{2} \leqslant \frac{5n}{48} + \frac{3}{2} \leqslant \frac{n}{8}, \quad \text{так что} \quad v \leqslant -\frac{n}{8}.$$

Замечая, что

$$r_2 - r_1 \geqslant \varrho - 1 \geqslant \frac{2\varrho}{3}$$

будем иметь:

$$\Delta < \left(24(\log q)p^{-n/8}\right)^{r_2-r_1} = \left(24(\log q)q^{-1/8}\right)^{r_2-r_1} < q^{-\frac{1}{10}(r_2-r_1)} < q^{-\frac{\varrho}{15}}.$$

Положим теперь $\tau = \kappa m$, $\kappa = 8$. Тогда

$$m(m+1)\left(1 - \frac{1}{m}\right)^{\tau} < e^{-\kappa}m(m+1) < 2e^{-\kappa}m^2,$$

$$h^{m(m+1)\left(1 - \frac{1}{m}\right)^{\tau}} < (2N)^{0.5e^{-\kappa}m^2} \leqslant (2N)^{10e^{-\kappa}\varrho^2} < N^{\frac{\varrho^2}{240}} = q^{\frac{\varrho}{240}},$$

откуда

$$|W|^{4k^2} \leqslant k^{12k}(2k)^{2m}(2m)^{16km} h^{8k^2} q^{-\frac{\varrho}{16}}.$$

Поскольку $k = 8m^2$, $m \geqslant 4\varrho \geqslant 12$, то

$$|W| \,<\, 2.7h^2 q^{-\frac{\varrho}{64k^2}} \,<\, 2.7h^2 q^{-c/\varrho^3} \,=\, 2.7h^2 N^{-c/\varrho^2},$$

где $c = 13^{-4}$. Наконец, замечая, что

$$p^s h^2 \,\leqslant\, p^{\frac{n}{4\varrho}+1}\sqrt{N} \,\leqslant\, N^{\frac{3}{4}+\frac{\varrho}{n}} \,\leqslant\, N^{\frac{3}{4}+\frac{1}{24}},$$

находим:

$$|S| \,\leqslant\, 2.7N^{1-c/\varrho^2} \,+\, 2N^{19/24} \,<\, 3N^{1-c/\varrho^2}.$$

Если μ таково, что $q < \mu + N < 2q$, то исходную сумму можно разбить на две, каждая из которых оценивается подобно тому, как это делалось выше. В этом случае приходим к оценке $|S| < 6N^{1-c/\varrho^2}$. $\square$

2. Метод Карацубы

2.1. Введение

В основе метода Карацубы лежит верхняя оценка $I_k(X)$ — числа решений сравнения

$$x_1^* + \ldots + x_k^* \,\equiv\, x_{k+1}^* + \ldots + x_{2k}^* \pmod p,$$

где $X < x_1, \ldots, x_{2k} \leqslant 2X$ и $k(2X)^{2k-1} < p$ (см. лемму 9). В свою очередь, оценка $I_k(X)$ используется для оценки коротких сумм Клоостермана, в которых множество $\mathcal{A}$, по которому ведётся суммирование, состоит из произведений вида $n = xy$, где $X < x \leqslant 2X$, $Y < y \leqslant 2Y$. При определённых соотношениях между X, Y и q такие суммы оказываются очень маленькими. (см. лемму 10).

Здесь приводится простейший вариант оценки $I_k(X)$, отвечающий случаю, когда переменные x_j являются простыми числами. С одной стороны, это позволяет избежать ряда некоторых технических трудностей, но, с другой стороны, получающиеся при этом результаты вполне достаточны для большинства приложений.

Оценка неполной суммы Клоостермана $S(p; x)$ по сплошному промежутку $1 \leqslant n \leqslant x$ проводится следующим образом. Все целые числа $n \leqslant x$ разбиваются на два множества. К первому относят все n, у которых есть по крайней мере одна пара простых делителей x, y, лежащих в интервалах $X < x \leqslant 2X$, $Y < y \leqslant 2Y$ с некоторыми специально подобранными X и Y. Оценка части исходной суммы по числам n из первого множества может быть сведена к оценке сумм из леммы 10. Числа n, принадлежащие ко второму множеству, простых делителей с указанными свойствами не имеют, но, как оказывается, мощность такого множества очень мала. Для доказательства последнего факта используются леммы 6 – 8.

2.2. Вспомогательные утверждения

Лемма 6. *Пусть* $\log x < y \leqslant \sqrt{x}$ *и пусть* $N(x, y)$ *— количество чисел* $n \leqslant x$*, все простые делители которых* $\leqslant y$*. Тогда*

$$N(x, y) \,\ll\, x \exp\left(-\xi\left(\log\xi + \log\log\xi + 1 - \frac{2}{\log\xi}\right)\right), \quad \xi = \frac{\log x}{\log y}.$$

Доказательство см. в работе А. И. Виноградова [42].

Лемма 7. *Пусть $2 < y \leqslant x$ и пусть $\Phi(x,y)$ — количество чисел $n \leqslant x$, все простые делители которых $> y$. Тогда*

$$\Phi(x,y) \leqslant \frac{x}{\log y} + \frac{13.5x}{(\log y)^2}.$$

Если $2 < y \leqslant 3$, то утверждение очевидно. В случае, когда $\sqrt{x} < y \leqslant x$, утверждение сразу получается из асимптотического закона распределения простых чисел. Если же $3 < y \leqslant \sqrt{x}$, то искомое неравенство получается стандартным применением метода решета А. Сельберга.

Лемма 8. *При $x \to +\infty$ справедливо асимптотическое равенство*

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

в котором $\gamma = 0.57721\ldots$ — постоянная Эйлера.

Доказательство см. в [44, гл.III, §5].

2.3. Симметричное сравнение с обратными величинами

Следующие утверждения принадлежат А. А. Карацубе [15].

Лемма 9. *Пусть $k \geqslant 2$ — целое число и пусть $k < X < X_1 \leqslant 2X$, $k(2X)^{2k-1} < p$. Тогда число $I_k(X)$ решений сравнения*

$$p_1^* + \ldots + p_k^* \equiv p_{k+1}^* + \ldots + p_{2k}^* \pmod p, \tag{5}$$

в простых числах $X < p_1, \ldots, p_{2k} \leqslant X_1$ не превосходит $k!X^k$.

Доказательство. Пусть $p_1, \ldots, p_{2k}$ — произвольное решение (5). Достаточно доказать,что p_1 совпадает с одним из чисел $p_{k+1}, \ldots, p_{2k}$. Не ограничивая общности, будем считать, что $p_1, \ldots, p_s$ – все различные числа набора $p_1, \ldots, p_k$. Обозначим через α_j кратность вхождения в набор числа p_j, $1 \leqslant j \leqslant s$, так что $\alpha_1 + \ldots + \alpha_s = k$.

Положим, далее, $P = p_1 \ldots p_s p_{k+1} \ldots p_{2k} = p_j P_j$ для $j = 1, \ldots, s, k+1, \ldots, 2k$. Тогда, домножая обе части (5) на P, получим

$$\alpha_1 P_1 + \ldots + \alpha_s P_s \equiv P_{k+1} + \ldots + P_{2k} \pmod p. \tag{6}$$

Поскольку $1 < P_j < (2X)^{2k-1}$, обе части (6) не превосходят $k(2X)^{2k-1} < p$. Следовательно, сравнение (6) в действительности оказывается уравнением

$$\alpha_1 P_1 + \ldots + \alpha_s P_s = P_{k+1} + \ldots + P_{2k}.$$

Так как $P_j \equiv 0 \pmod{p_1}$ при $2 \leqslant j \leqslant 2k$, то $\alpha_1 P_1 \equiv 0 \pmod{p_1}$. Из определения следует, что $\alpha_1 \leqslant k < X < p_1$. Таким образом, $P_1 \equiv 0 \pmod{p_1}$. Если $p_1 \neq p_{k+1}, \ldots, p_{2k}$, мы приходим к противоречию. □

Лемма 10. *Пусть $(ab,p) = 1$, $k, s \geqslant 2$, $k < X < X_1 \leqslant 2X$, $s < Y < Y_1 \leqslant 2Y$, $k(2X)^{2k-1} < p$, $s(2Y)^{2s-1} < p$. Тогда для сумм*

$$S_1 = \sideset{}{'}\sum_{X < x \leqslant X_1} \sideset{}{'}\sum_{Y < y \leqslant Y_1} e_p\big(ax^*y^*\big), \quad S_2 = \sideset{}{'}\sum_{X < x \leqslant X_1} \sideset{}{'}\sum_{Y < y \leqslant Y_1} e_p\big(ax^*y^* + bxy\big),$$

в которых штрих означает суммирование по простым числам x, y, удовлетворяют неравенствам $|S_j| \leqslant XY\Delta_j$,

$$\Delta_1 = 2k^{\frac{1}{2s}} s^{\frac{1}{2k}} \big(pX^{-k}Y^{-s}\big)^{\frac{1}{2ks}}, \quad \Delta_2 = 2k^{\frac{1}{2s}} s^{\frac{1}{2k}} \big(pX^{1-k}Y^{-s}\big)^{\frac{1}{2ks}}.$$

Замечание. Утверждение леммы остаётся в силе и для сумм вида

$$S_1 = \sideset{}{'}\sum_{X<x\leqslant X_1}\sideset{}{'}\sum_{Y<y\leqslant Y_1} F(x)G(y)e_p\big(ax^*y^*\big),\ S_2 = \sideset{}{'}\sum_{X<x\leqslant X_1}\sideset{}{'}\sum_{Y<y\leqslant Y_1} F(x)G(y)e_p\big(ax^*y^* + bxy\big),$$

где F, G — произвольные комплекснозначные функции, удовлетворяющие условиям $|F(x)| \leqslant 1$, $|G(y)| \leqslant 1$.

Доказательство. Согласно лемме 2,

$$|S_1|^k \leqslant Y^{k-1}\sideset{}{'}\sum_{Y<y\leqslant Y_1}\Bigg|\sideset{}{'}\sum_{X<x\leqslant X_1} e_p\big(ax^*y^*\big)\Bigg|^k =$$

$$= Y^{k-1}\sideset{}{'}\sum_{Y<y\leqslant Y_1}\Bigg|\sideset{}{'}\sum_{X<x_1,\ldots,x_{2k}\leqslant X_1} e_p\big(ay^*\left(x_1^*+\ldots+x_k^*\right)\big)\Bigg|.$$

Обозначим через $\theta(y)$ аргумент суммы по $x_1,\ldots,x_{2k}$. Тогда

$$|S_1|^k \leqslant Y^{k-1}\sideset{}{'}\sum_{Y<y\leqslant Y_1} e^{-i\theta(y)}\sideset{}{'}\sum_{X<x_1,\ldots,x_k\leqslant X_1} e_p\big(ay^*\left(x_1^*+\ldots+x_k^*\right)\big) =$$

$$= Y^{k-1}\sideset{}{'}\sum_{Y<y\leqslant Y_1} e^{-i\theta(y)}\sum_{\lambda=0}^{p-1} j_k(\lambda)e_p\big(a\lambda y^*\big) \leqslant Y^{k-1}\sum_{\lambda=0}^{p-1} j_k(\lambda)\Bigg|\sideset{}{'}\sum_{Y<y\leqslant Y_1} e^{-i\theta(y)}e_p\big(a\lambda y^*\big)\Bigg|,$$

где $j_k(\lambda)$ — число решений сравнения $x_1^*+\ldots+x_k^*\equiv\lambda(\mathrm{mod}\ p)$ в простых числах

$$X<x_1,\ldots,x_k\leqslant X_1.$$

Далее, из леммы 2 получаем неравенство $|S_1|^{ks} \leqslant Y^{s(k-1)}T_1^{s-1}T_2$, в котором

$$T_1 = \sum_{\lambda=0}^{p-1} j_k(\lambda),\quad T_2 = \sum_{\lambda=0}^{p-1} j_k(\lambda)\Bigg|\sideset{}{'}\sum_{Y<y\leqslant Y_1} e^{-i\theta(y)}e_p\big(a\lambda y^*\big)\Bigg|^s.$$

Сумма T_1 совпадает с числом наборов $(x_1,\ldots,x_k)$, $X<x_j\leqslant X_1$ и, таким образом, $T_1\leqslant X^k$. Следовательно,

$$|S_1|^{2ks} \leqslant X^{2k(s-1)}Y^{2s(k-1)}T_2^2.$$

В силу неравенства Коши, $T_2^2\leqslant T_3T_4$, где

$$T_3 = \sum_{\lambda=0}^{p-1} j_k^2(\lambda),\quad T_4 = \sum_{\lambda=0}^{p-1}\Bigg|\sideset{}{'}\sum_{Y<y\leqslant Y_1} e^{-i\theta(y)}e_p\big(a\lambda y^*\big)\Bigg|^{2s}.$$

Сумма T_3 равна числу решений сравнения

$$x_1^*+\ldots+x_k^* \equiv x_{k+1}^*+\ldots+x_{2k}^*(\mathrm{mod}\ p)$$

в простых числах $X<x_1,\ldots,x_{2k}\leqslant X_1$. По лемме 9, $T_3\leqslant k!X^k$. Поэтому

$$T_4 = \sum_{\lambda=0}^{p-1}\sideset{}{'}\sum_{Y<y_1,\ldots,y_{2s}\leqslant Y_1} e^{-i(\theta(y_1)+\ldots-\theta(y_{2s}))}e_p\Big(a\lambda\left(y_1^*+\ldots-y_{2s}^*\right)\Big) =$$

$$= \sum_{\mu=0}^{p-1}\Bigg(\sideset{}{''}\sum_{Y<y_1,\ldots,y_{2s}\leqslant Y_1} e^{-i(\theta(y_1)+\ldots-\theta(y_{2s}))}\Bigg)\sum_{\lambda=0}^{p-1} e_p\big(a\lambda\mu\big),$$

где двойной штрих в знаке суммы означает суммирование по наборам простых чисел

$$Y < y_1, \ldots, y_{2s} \leqslant Y_1,$$

удовлетворяющих сравнению

$$y_1^* + \ldots + y_s^* \equiv y_{s+1}^* + \ldots + y_{2s}^* + \mu (\mathrm{mod}\ p).$$

Согласно лемме 9, число слагаемых в такой сумме не превышает $s!Y^s$. Таким образом,

$$T_4 \leqslant s!Y^s \sum_{\mu=0}^{p-1} \left| \sum_{\lambda=0}^{p-1} e_p\big(a\lambda\mu\big) \right| = s!Y^s p.$$

Следовательно,

$$T_2^2 \leqslant k!s!X^k Y^s p, \quad |S_1|^{2ks} \leqslant (XY)^{2ks} k!s!X^{-k}Y^{-s}p.$$

Рассуждая подобным образом, для суммы S_2 получаем цепочку соотношений

$$|S_2|^k \leqslant Y^{k-1} \sideset{}{'}\sum_{Y<y\leqslant Y_1} \left| \sum_{\lambda=0}^{p-1} \sum_{kX<\sigma\leqslant kX_1} j_k(\lambda;\sigma) e_p\big(a\lambda y^* + b\sigma y\big) \right| \leqslant$$

$$\leqslant Y^{k-1} \sum_{\lambda=0}^{p-1} \sum_{kX<\sigma\leqslant kX_1} j_k(\lambda;\sigma) \left| \sideset{}{'}\sum_{Y<y\leqslant Y_1} e^{-i\theta(y)} e_p\big(a\lambda y^* + b\sigma y\big) \right|,$$

где $j_k(\lambda;\sigma)$ — число решений системы сравнений

$$\begin{cases} x_1^* + \ldots + x_k^* \equiv \lambda (\mathrm{mod}\ p), \\ x_1 + \ldots + x_k \equiv \sigma (\mathrm{mod}\ p) \end{cases}$$

в простых числах $X < x_1, \ldots, x_k < X_1$. По лемме 2, $|S_2|^{ks} \leqslant Y^{s(k-1)} T_1^{s-1} T_2$, где

$$T_1 = \sum_{\lambda=0}^{p-1} \sum_{kX<\sigma\leqslant kX_1} j_k(\lambda;\sigma), \ T_2 = \sum_{\lambda=0}^{p-1} \sum_{kX<\sigma\leqslant kX_1} j_k(\lambda;\sigma) \left| \sideset{}{'}\sum_{Y<y\leqslant Y_1} e^{-i\theta(y)} e_p\big(a\lambda y^* + b\sigma y\big) \right|.$$

Так как $T_1 \leqslant X^k$, то из леммы 2 находим: $|S_2|^{2ks} \leqslant X^{2k(s-1)} Y^{2s(k-1)} T_3 T_4$, где

$$T_3 = \sum_{\lambda=0}^{p-1} \sum_{kX<\sigma\leqslant kX_1} j_k^2(\lambda;\sigma) \leqslant k!X^k, \quad T_4 = \sum_{\lambda=0}^{p-1} \sum_{kX<\sigma\leqslant kX_1} \left| \sideset{}{'}\sum_{Y<y\leqslant Y_1} e^{-i\theta(y)} e_p\big(a\lambda y^* + b\sigma y\big) \right|^{2s}.$$

Далее,

$$T_4 = \sum_{\mu=0}^{p-1} \sum_{|\tau|\leqslant sY_1} \left(\sideset{}{''}\sum_{Y<y_1,\ldots,y_{2s}\leqslant Y_1} e^{-i(\theta(y_1)+\ldots-\theta(y_{2s}))} \right) \sum_{\lambda=0}^{p-1} \sum_{kX<\sigma\leqslant kX_1} e_p\big(a\lambda\mu + b\sigma\tau\big),$$

где двойной штрих означает суммирование по всем решениям системы

$$\begin{cases} y_1^* + \ldots + y_s^* \equiv y_{s+1}^* + \ldots + y_{2s}^* + \mu (\mathrm{mod}\ p), \\ y_1 + \ldots + y_s \equiv y_{s+1} + \ldots + y_{2s} + \tau (\mathrm{mod}\ p) \end{cases}$$

в простых числах $Y < y_1, \ldots, y_{2s} \leqslant Y_1$. Количество слагаемых в кратной сумме по $|\tau| \leqslant sY_1$ и $y_1, \ldots, y_{2s}$ не превосходит $s!Y^s$. Таким образом,

$$T_4 \leqslant \sum_{\mu=0}^{p-1} s!Y^s \cdot k(X_1 - X) \left| \sum_{\lambda=0}^{p-1} e_p\big(a\lambda\mu\big) \right| \leqslant sk!Y^s pX.$$

Окончательно находим: $|S_2|^{2ks} \leqslant (XY)^{2ks} k!s!spX \cdot Y^{-s}X^{-k}$. $\square$.

2.4. Основная теорема

Теорема 5. *Пусть* $(a,p)=1$, *и пусть* $e^{(\log p)^{2/3}(\log\log p)^{4/3}} \leqslant x \leqslant \sqrt{p}$. *Тогда имеет место следующее неравенство:*

$$\sum_{\nu\leqslant x} e_p\bigl(a\nu^* + b\nu\bigr) \ll x\,\frac{(\log p)^{2/7}}{(\log x)^{3/7}}\,(\log\log p)^{4/7}. \tag{7}$$

Доказательство. Рассмотрим лишь случай $(b,p)=1$, поскольку при b, кратном p, рассуждения оказываются несколько проще и практически дословно повторяют приводимые ниже. Положим

$$Z = \exp\left(\frac{\log x}{\log\log x}\right), \quad Y_k = \frac{1}{4}\,p^{\frac{1}{2k-1}}$$

и определим целое число m из неравенств $Y_m \leqslant Z < Y_{m-1}$. Далее, пусть n, l — целые числа, удовлетворяющие следующим условиям: $2m \leqslant n < \frac{1}{4}\sqrt{\log p}$, $7n < l < \log p$. Положим также

$$\kappa = \frac{1}{4n}, \quad X_k = p^{\frac{1+\kappa}{2k}}, \quad X = X_n, \quad Y = Y_m, \quad U = Y_l, \quad V = Y_{4n}.$$

Тогда $Y_{k+1} < X_k < Y_k$ при любом k, $m \leqslant k \leqslant n$, и, кроме того, $U < V < X < Y \leqslant Z$.

Далее все числа $\nu \leqslant x$ разбиваются на два множества: A и B. Мощность множества A не будет превосходить по порядку правой части (7), так что сумму по $\nu \in A$ достаточно оценить тривиально. Слагаемые суммы по $\nu \in B$ можно распределить по сравнительно небольшому числу двойных сумм, к каждой из которых применима оценка леммы 10.

Итак, поместим сперва во множество A все числа $\nu \leqslant x$, которые не имеют простых делителей из объединения промежутков $(X_k, Y_k]$, $k = m, m+1, \ldots, n$. Все эти числа представимы в виде $\nu = uv$ или $\nu = uvw$, где $u \geqslant 1$ не имеет простых делителей, бóльших X, все простые делители v, напротив, превосходят Y и, наконец, $w = w_m w_{m+1} \ldots w_{n-1}$, где $w_k = 1$ либо все простые делители w_k принадлежат промежутку $(Y_{k+1}, X_k]$. Числа вида $\nu = uw$ не имеют простых делителей, больших Y. Согласно лемме 6, количество таких $\nu \leqslant x$ не превосходит

$$N(x;Y) \leqslant N(x;Z) \leqslant x\exp\bigl(-(\log\log p)\log\log\log p\bigr) < \frac{x}{(\log p)^2}$$

Далее, при фиксированных сомножителях u, w произведения $\nu = uvw$ имеется не более

$$\Phi\left(\frac{x}{uw}; Y\right) \leqslant \frac{2x}{\log Y}\,\frac{1}{uw}$$

возможностей для выбора сомножителя $v = \nu/(uw) \leqslant x/(uw)$. В силу леммы 7, количество таких $\nu \leqslant x$ не превосходит

$$\frac{2x}{\log Y}\sum_u\sum_w \frac{1}{uw} = \frac{2x}{\log Y}\sum_u \frac{1}{u}\sum_{w_m}\frac{1}{w_m}\cdots\sum_{w_{n-1}}\frac{1}{w_{n-1}},$$

где величины u и w_k независимо друг от друга пробегают возрастающие последовательности чисел, чьи простые делители принадлежат соответствующим промежуткам. По лемме 8 имеем:

$$\sum_u \frac{1}{u} \leqslant \prod_{q\leqslant X}\left(1 + \frac{1}{q} + \frac{1}{q^2} + \ldots\right) =$$

$$= \prod_{q\leqslant X}\left(1 - \frac{1}{q}\right)^{-1} = e^{\gamma}(\log X)\left(1 + O\left(e^{-c_1\sqrt{\log X}}\right)\right) < 1.5\log X,$$

$$\sum_{w_k}\frac{1}{w_k} \leqslant \prod_{Y_{k+1}<q\leqslant X_k}\left(1-\frac{1}{q}\right)^{-1} = \frac{\log X_k}{\log Y_{k+1}}\left(1+O\Big(e^{-c_1\sqrt{\log Y_{k+1}}}\Big)\right) <$$
$$< (1+\kappa)\left(1+\frac{1}{2k}\right)\left(1-\frac{(2k+1)\log 4}{\log p}\right)^{-1}\left(1+O\Big(e^{-c_2\sqrt{\log p}}\Big)\right) <$$
$$< (1+4\kappa)\left(1+\frac{1}{2k}\right).$$

Следовательно,

$$\sum_{u,w}\frac{1}{uw} < 1.5(\log X)(1+4\kappa)^n\prod_{k=m}^{n-1}\left(1+\frac{1}{2k}\right) < 1.5e(\log X)\exp\left(\frac{1}{2}\log\frac{n}{m}\right),$$
$$\frac{2x}{\log Y}\sum_{u,w}\frac{1}{uw} < 3ex\frac{\log X}{\log Y}\sqrt{\frac{n}{m}}.$$

Так как $8m < \sqrt{\log p}$, то

$$Y > p^{\frac{1}{2m-0.5}} \quad \text{и} \quad \frac{\log X}{\log Y} < (1+\kappa)\,\frac{2m-0.5}{2n} = \left(1+\frac{1}{4n}\right)\left(\frac{m}{n}-\frac{1}{4n}\right) < \frac{m}{n},$$

откуда следует, что в A помещено не более

$$\frac{x}{(\log p)^2} + 3ex\,\frac{m}{n}\sqrt{\frac{n}{m}} < 9x\sqrt{\frac{m}{n}}$$

чисел.

Далее, отнесём ко множеству A все числа $\nu \leqslant x$, не делящиеся на простые из промежутка $\mathcal{J} = (U, V]$. Такие числа ν представляются в виде $\nu = u$ или $\nu = uv$, где $u \geqslant 1$ не имеет простых делителей $> U$, а v не имеет простых делителей $\leqslant V$. Количество чисел вида $\nu = u$ не превосходит $N(x; Z) < x/(\log p)^2$. Количество же чисел вида $\nu = uv$ ограничено сверху величиной

$$\frac{2x}{\log V}\sum_{u}\frac{1}{u} \leqslant \frac{2x}{\log V}\prod_{q\leqslant U}\left(1-\frac{1}{q}\right)^{-1} < 3x\,\frac{\log U}{\log V} < 12x\,\frac{n}{l}.$$

Так находим:

$$|A| < 9x\sqrt{\frac{m}{n}} + \frac{2x}{(\log p)^2} + 12x\,\frac{n}{l} < 9x\sqrt{\frac{m}{n}} + 13x\,\frac{n}{l}.$$

Множество B разобьём на классы $B_{c,d}$, $c, d = 1, 2, \ldots$, относя к $B_{c,d}$ числа $\nu \leqslant x$, имеющие ровно c простых делителей из $\mathcal{I}$ и ровно d простых делителей из $\mathcal{J}$. Тогда

$$\left|\sum_{\nu\in B} e_p(a\nu^* + b\nu)\right| \leqslant \sum_{c,d\geqslant 1}|S_{c,d}|, \quad \text{где} \quad S_{c,d} = \sum_{\nu\in B_{c,d}} e_p(a\nu^* + b\nu).$$

Сравним сумму $S_{c,d}$ $(c, d \geqslant 1)$ с суммой

$$T_{c,d} = \frac{1}{cd}\sum_{q\in\mathcal{I}}\sum_{r\in\mathcal{J}}\sum_{h\leqslant x/(qr)} e_p(aq^*r^*h^* + bqrh), \tag{8}$$

где q и r независимо друг от друга пробегают множества простых из $\mathcal{I}$ и $\mathcal{J}$ соответственно, а h пробегает монотонно возрастающую последовательность чисел класса $B_{c-1,d-1}$, не зависящую от q и r (смысл обозначения $B_{c-1,d-1}$ при $c = 1$ или $d = 1$ очевиден). Несложно заметить,

что всякое число $\nu \in B_{c,d}$, не делящееся на квадрат простого из $\mathcal{I} \cup \mathcal{J}$, встретится среди произведений hqr в (8) ровно cd раз и потому войдёт в $T_{c,d}$ с коэффициентом 1. Следовательно, $S_{c,d} = T_{c,d} + 2\theta x U^{-1}$, где последнее слагаемое отвечает вкладу чисел ν, делящихся на квадраты простых из $\mathcal{I} \cup \mathcal{J}$.

Далее, разобьём теперь области изменения q, r на промежутки вида $Q < q \leqslant Q_1$, $R < r \leqslant R_1$, где $Q_1 \leqslant 2Q$, $R_1 \leqslant 2R$. Тогда

$$T_{c,d} = \frac{1}{cd} \sum_{Q,R} T_{c,d}(Q,R), \quad \text{где} \quad T_{c,d}(Q,R) = \sum_{Q<q\leqslant Q_1} \sum_{R<r\leqslant R_1} \sum_{h\leqslant x/(qr)} e_p(aq^* r^* h^* + bqrh).$$

Меняя порядок суммирования, будем иметь:

$$T_{c,d}(Q,R) = \sum_{h\leqslant x/(QR)} T_{c,d}(Q,R;h), \quad \text{где}$$

$$T_{c,d}(Q,R;h) = \sum_{Q<q\leqslant Q_2} \sum_{R<r\leqslant R_2} e_p(a_1 q^* r^* + b_1 qr),$$

$$a_1 \equiv ah^* \pmod p, \quad b_1 \equiv bh \pmod p, \quad Q_2 = \min\left(Q_1, \frac{x}{hR}\right), \quad R_2 = \min\left(R_1, \frac{x}{hq}\right).$$

Преобразуем последнюю сумму так, чтобы область изменения r не зависела от q. Получим:

$$T_{c,d}(Q,R;h) = \sum_{Q<q\leqslant Q_1} \sum_{R<r\leqslant R_1} \frac{1}{p} \sum_{|f|<0.5p} \sum_{R<\mu\leqslant R_2} e_p(f(r-\mu)) e_p(a_1 q^* r^* + b_1 qr) =$$

$$= \sum_{|f|<0.5p} \frac{T(f)}{|f|+1}, \quad \text{где} \quad T(f) = \sum_{Q<q\leqslant Q_2} \sum_{R<r\leqslant R_1} F(q) G(r) e_p(a_1 q^* r^* + b_1 qr),$$

$$F(q) = \frac{|f|+1}{p} \sum_{R<\mu\leqslant R_2} e_p(-f\mu), \quad G(r) = e_p(fr).$$

Заметим, что $|F(q)| \leqslant q$ при любых q и f. Кроме того, для всякой пары Q, R найдутся целые k, s такие, что $m \leqslant k \leqslant n$, $4n \leqslant s \leqslant l$ и

$$0.5X_k < Q \leqslant 2Y_k, \quad 0.5Y_{s+1} < R \leqslant 2Y_s. \tag{9}$$

Применяя к оценке $T(f)$ лемму 10, с учётом замечания к ней, будем иметь:

$$|T(f)| \leqslant QR\Delta, \quad \text{где} \quad \Delta = 2k^{\frac{1}{2s}} s^{\frac{1}{2k}} \left(pQ^{-k} R^{1-s}\right)^{\frac{1}{2ks}}.$$

Несложно проверить, что

$$Q^k \geqslant 2^{-k} X_k^k = 2^{-k} p^{\frac{1+\kappa}{2}}, \quad R^{s-1} \geqslant 2^{1-s} Y_{s+1}^{s-1} \geqslant 2^{-s} p^{\frac{1}{2} - \frac{3}{2(2s+1)}}.$$

Так как $s \geqslant 7n > k \geqslant m \geqslant 2$, то

$$\Delta < 5(\log p)^{\frac{1}{2m}} p^{-\frac{1}{56nks}} \leqslant \Delta_0 = (\log p)^{1/2} p^{-\frac{1}{56n^2 l}}.$$

Таким образом,

$$|T_{c,d}(Q,R;h)| \leqslant QR(\log p + 1)\Delta_0 \leqslant \frac{x}{h}(\log p + 1)\Delta_0,$$

$$|T_{c,d}(Q,R)| \leqslant x(\log p + 1)^2 \Delta_0, \quad |T_{c,d}| \leqslant \frac{2x}{cd}(\log p)^4 \Delta_0, \quad |S_{c,d}| \leqslant \frac{3x}{cd}(\log p)^4 \Delta_0.$$

Суммируя по c, d, получим:

$$\sum_{c,d\geqslant 1} |S_{c,d}| \;<\; x(\log p)^5 p^{-\frac{1}{56n^2 l}}, \;\; \Bigl|\sum_{\nu\leqslant x} e_p(a\nu^* + b\nu)\Bigr| \;\leqslant\; 9x\sqrt{\frac{m}{n}} + 13x\frac{n}{l} + x(\log p)^5 p^{-\frac{1}{56n^2 l}}.$$

Положим теперь

$$n \;=\; \left[\frac{1}{22}\,\frac{(\log p)^{3/7}}{(\log x)^{1/7}}\,(\log\log p)^{-1/7}\right], \quad l \;=\; \bigl[(\log p)^{1/7}(\log x)^{2/7}(\log\log p)^{-5/7}\bigr].$$

Тогда $m \leqslant 2n$, $4n < \sqrt{\log p}$, $l > 4n$, $p^{-\frac{1}{56n^2 l}} < (\log p)^{-8}$ и, наконец,

$$\Bigl|\sum_{\nu\leqslant x} e_p\bigl(a\nu^* + b\nu\bigr)\Bigr| \;\leqslant\; 31x\,\frac{(\log p)^{2/7}}{(\log x)^{3/7}}\,(\log\log p)^{4/7}. \quad \square$$

3. Метод Бургейна и Гараева

3.1. Введение

Ещё один метод оценок коротких сумм Клоостермана, в которых переменная суммирования пробегает сплошной промежуток, был предложен в работах Ж. Бургейна и М. З. Гараева [23], [45]. Как и в методе Карацубы, оценка $S(x)$ начинается с разбиения промежутка $1 \leqslant \nu \leqslant x$ на два множества A и B. Мощность A оказывается достаточно малой, так что сумма по $\nu \in A$ оценивается тривиально. Для всякого же числа $\nu \in B$ имеет место представление $\nu = xyzh$, где простые сомножители x, y и z лежат в интервалах специального вида. Поэтому слагаемые, отвечающие $\nu \in B$, можно перераспределить по не очень большому числу "трилинейных" сумм

$$\sum_{x,y,z} e_p\bigl(a_1 x^* y^* z^*\bigr), \quad (a_1, p) = 1,$$

к каждой из которых после ряда преобразований применима фундаментальная лемма Бургейна (лемма 12). Наличие трёх (а не двух, как в методе Карацубы) независимых сомножителей x, y, z даёт больше свободы в обращении с ними. Например, каждый из сомножителей может теперь принимать значения, близкие к числам вида $p^{1/(2k)}$, $k = 1, 2, 3, \ldots$. Напомним, что в методе Карацубы необходимо было тщательно следить за тем, чтобы соответствующие простые делители чисел $\nu \in B$ лежали в интервалах вида $p^{(1+\kappa)/(2k)} < q \leqslant p^{(1-\kappa)/(2k-2)}$, где $\kappa > 0$, и, таким образом, "избегали" малых окрестностей точек $p^{1/(2k)}$.

Вместе с тем, необходимо отметить, что при оценке сумм $S(x)$ по сплошному промежутку главной отличительной особенностью метода Бургейна-Гараева от метода Карацубы является не сколько лемма 12, сколько новая оценка числа решений сравнения (5) (лемма 13 настоящего обзора). Именно, эта оценка свободна от обременительного ограничения $k(2X)^{2k-1} < p$, которое присутствует в лемме 9.

3.2. Вспомогательные утверждения

Лемма 11. *Пусть $m \geqslant 2, (a, m) = 1, r \geqslant 1$, и пусть $A_1, \ldots, A_r$ — произвольные подмножества $\mathbb{Z}_m$. Далее, пусть $k_1, \ldots, k_r \geqslant 2$ — произвольные чётные числа, и пусть*

$$W \;=\; \sum_{x_1\in A_1} \cdots \sum_{x_r\in A_r} e_m\bigl(a\,x_1 \ldots x_r\bigr).$$

Тогда

$$|W|^k \leqslant \left(\prod_{r=1}^{r} |A_j|^{k-k_j}\right) \sum_{h_1,\ldots,h_r=0}^{m-1} \xi_1(h_1)\ldots\xi_r(h_r) e_m\big(a\,h_1\ldots h_r\big),$$

где $k = k_1\ldots k_r$ *и* $\xi_j(h)$ *обозначает число решений сравнения*

$$y_1+\ldots+y_t \equiv y_{t+1}+\ldots+y_{2t}+h(\mathrm{mod}\ m), \quad 2t = k_j,$$

с условиями $y_1,\ldots,y_{2t}\in A_j$.

Замечание. Утверждение леммы 11 остаётся в силе и для "взвешенной" суммы

$$W = \sum_{x_1\in A_1}\cdots\sum_{x_r\in A_r} f_1(x_1)\ldots f_r(x_r) e_m\big(a\,x_1\ldots x_r\big)$$

где $|f_s(x)|\leqslant 1$ при любых $x\in\mathbb{Z}_m$, $s=1,\ldots,r$. Разница состоит лишь в том, что в этом случае через $\xi_j(h)$ будут обозначаться некоторые функции, такие, что их абсолютные величины $|\xi_j(h)|$ не превосходят чисел решений соответствующих сравнений.

Доказательство (индукция по r). В случае $r=1$ утверждение очевидно:

$$|W|^{k_1} = |W|^{2t} = \sum_{x_1^{(1)},\ldots,\,x_{2t}^{(1)}} e_m\big(a\,(x_1^{(1)}+\ldots-x_{2t}^{(1)})\big) = \sum_{h=0}^{m-1}\xi_1(h)e_m\big(ah\big).$$

Предположим теперь, что утверждение леммы доказано для $1\leqslant r\leqslant s-1$ и проверим его справедливость для $r=s$. Обозначим исходную сумму через W_s. Тогда, полагая $k_s=2t$, из леммы 2 получим:

$$|W_s|^{k_s} \leqslant \big(|A_1|\ldots|A_{s-1}|\big)^{k_s-1}\sum_{x_1\in A_1}\ldots\sum_{x_{s-1}\in A_{s-1}}\left|\sum_{x_s\in A_s} e_m\big(a\,x_1\ldots x_s\big)\right|^{k_s} =$$

$$= \big(|A_1|\ldots|A_{s-1}|\big)^{k_s-1}\sum_{h_s=0}^{m-1}\xi_s(h_s)W_{s-1}, \quad (10)$$

где

$$W_{s-1} = \sum_{x_1\in A_1}\ldots\sum_{x_{s-1}\in A_{s-1}} e_m\big(ah_s\,x_1\ldots x_{s-1}\big).$$

В силу предположения индукции,

$$|W_{s-1}|^{\kappa} \leqslant$$

$$\leqslant \left(\prod_{j=1}^{s-1}|A_j|^{\kappa-k_j}\right)\sum_{h_1,\ldots,h_{s-1}=0}^{m-1}\xi_1(h_1)\ldots\xi_{s-1}(h_{s-1})e_m\big(a\,h_1\ldots h_s\big), \quad \kappa = k_1\ldots k_{s-1} = \frac{k}{k_s}.$$

Вновь применяя лемму 2, будем иметь:

$$\left(\sum_{h_s=0}^{m-1}\xi_s(h_s)|W_{s-1}|\right)^{\kappa} \leqslant \left(\sum_{h_s=0}^{m-1}\xi_s(h_s)\right)^{\kappa-1}\sum_{h_s=0}^{m-1}\xi_s(h_s)|W_{s-1}|^{\kappa} \leqslant$$

$$\leqslant |A_s|^{k_s(\kappa-1)}\left(\prod_{j=1}^{s-1}|A_j|^{\kappa-k_j}\right)\sum_{h_1,\ldots,h_s=0}^{m-1}\xi_1(h_1)\ldots\xi_s(h_s)e_m\big(a\,h_1\ldots h_s\big). \quad (11)$$

Возводя обе части (10) в степень κ и пользуясь (11), приходим к искомому утверждению. □

Лемма 12. *Пусть p — простое число, $(a,p)=1$, и пусть $\alpha_j(x), j=1,2,3$ — произвольные комплекснозначные функции, такие,что $\|\alpha_j\|_1<1$ и $\|\alpha_1\|_2\cdot\|\alpha_2\|_2\cdot\|\alpha_3\|_2<p^{-0.5-\varepsilon}$, где $\varepsilon>0$ — постоянное число и*

$$\|\alpha\|_r \;=\; \left(\sum_{x=1}^{p}|\alpha(x)|^r\right)^{1/r}, \quad r=1,2.$$

Тогда для суммы

$$W \;=\; \sum_{x,y,z=1}^{p}\alpha_1(x)\alpha_2(y)\alpha_3(z)e_p\big(a\,xyz\big)$$

справедливо неравенство: $|W|<p^{-\delta}$, где $\delta=(0.1\varepsilon)^{10^4}$.

Доказательство этой леммы, принадлежащее Ж. Бургейну и М.З. Гараеву [23], опирается на утверждения из геометрии чисел и, в частности, на теорему о последовательных минимумах выпуклого компактного множества относительно решётки в $\mathbb{R}^n$.

3.3. Основная теорема

Теорема 6. *Пусть p – простое число, $(a,p)=1$, и пусть*

$$e^{(\log p)^{2/3}(\log\log p)^{4/3}} \;\leqslant\; x \;\leqslant\; \sqrt{p}.$$

Тогда

$$\sum_{\nu\leqslant x} e_p\big(a\nu^*\big) \;\ll\; \frac{x}{D}\log D, \quad \text{где} \quad D=\frac{(\log x)^{3/2}}{(\log p)(\log\log p)^2}.$$

Доказательство. Положим $Q=\exp\left(\dfrac{\log x}{\log\log p}\right)$ и определим m неравенствами

$$p^{1/(2m)}\leqslant Q\leqslant p^{1/(2m-2)}.$$

Далее, зададимся целым числом n с условием $3m\leqslant n\leqslant\sqrt{\log p}$ и обозначим $X=p^{1/(2n)}$, $Y=p^{1/(2m)}$. Все числа $\nu\leqslant x$ разобьём на два множества: A и B.

Прежде всего, отнесём к A все числа $\nu\leqslant x$, не имеющие простых делителей $>Y$. Количество таких ν не превосходит $N(x;Y)\leqslant N(x;Q)<x(\log p)^{-10}$. Далее, отнесём к A все числа, не имеющие простых делителей из промежутка $(X,Y]$. Все такие ν представляются в виде uv, где u не имеет простых делителей $>X$, а v не имеет простых делителей $\leqslant Y$. Следовательно, количество таких чисел ν не превосходит

$$\sum_u \Phi\Big(\frac{x}{u};Y\Big) \;\leqslant\; \frac{2x}{\log Y}\sum_u\frac{1}{u} \;\leqslant\; 3x\,\frac{\log X}{\log Y} \;=\; 3x\,\frac{m}{n}.$$

Наконец, отнесём к A те числа ν, которые имеют в точности один простой делитель $q\in(X,Y]$. Записывая такие ν в виде uvq, где обозначения u и v сохраняют тот же смысл, что и выше, заключаем, что их количество не превышает

$$\sum_{u,q}\Phi\Big(\frac{x}{uq};Y\Big) \;\leqslant\; \frac{2x}{\log Y}\sum_u\frac{1}{u}\sum_q\frac{1}{q} \;<\; 3x\,\frac{m}{n}\log\frac{n}{m}.$$

Таким образом,

$$|A| \;\leqslant\; \frac{x}{(\log p)^{10}} \;+\; 3x\,\frac{m}{n} \;+\; 3x\,\frac{m}{n}\log\frac{n}{m} \;<\; 7x\,\frac{m}{n}\log\frac{n}{m}.$$

Обозначим через $S_{c,d}$ сумму по числам $\nu \in B$, имеющим ровно c простых делителей из промежутка $\mathcal{I} = (X, Y]$ и ровно d простых делителей из промежутка $\mathcal{J} = (Y, x]$ $(c \geqslant 2, d \geqslant 1)$. Тогда

$$\left| \sum_{\nu \in B} e_p\bigl(a\nu^*\bigr) \right| \leqslant \sum_{c \geqslant 2,\, d \geqslant 1} |S_{c,d}|.$$

Применяя те же рассуждения, что и при доказательстве теоремы 5, получим:

$$S_{c,d} \,=\, \frac{1}{c(c-1)d} \sum_{h} \sum_{p_1 p_2 p_3 \leqslant x h^{-1}} e_p\bigl(a h^* p_1^* p_2^* p_3^*\bigr) \,+\, 2\theta x X^{-1}, \tag{12}$$

где h пробегает некоторую возрастающую последовательность, а простые p_1, p_2 и p_3 независимо друг от друга пробегают промежутки $\mathcal{I}, \mathcal{I}$ и $\mathcal{J}$ соответственно. Последнее слагаемое в (12) отвечает вкладу от чисел n, делящихся на q^2 при некотором $q \in \mathcal{I} \cup \mathcal{J}$. Фиксируя h, разобьём области изменения переменных p_j на промежутки вида $P_j < p_j \leqslant Q_j$, где

$$Q_1 \,=\, \min\left(2P_1, \frac{x}{hXY}\right), \quad Q_2 \,=\, \min\left(P_2(1 + (\log p)^{-4}), \frac{x}{hXY}\right),$$
$$Q_3 \,=\, \min\left(2P_3, \frac{x}{hX^2}\right). \tag{13}$$

Так получим

$$S_{c,d} = \frac{1}{cd(c-1)} \sum_{h} \sum_{P_1, P_2, P_3} T \,+\, 2\theta x X^{-1},$$
$$T = T_{c,d}(h; P_1, P_2, P_3) \,=\, \sum_{P_1 < p_1 \leqslant Q_1} \sum_{P_2 < p_2 \leqslant R_2} \sum_{P_3 < p_3 \leqslant R_3} e_p\bigl(a_1 p_1^* p_2^* p_3^*\bigr),$$

где

$$a_1 \equiv a h^* (\mathrm{mod}\ p), \quad R_2 = \min\,(Q_2, y), \quad R_3 = \min\,(Q_3, t), \quad y = \left[\frac{x}{hYp_1}\right], \quad t = \left[\frac{x}{hp_1p_2}\right].$$

Если $t < P_3$, то сумма по p_3 пуста; если $t \geqslant Q_3$, то область изменения p_3 в T имеет вид $P_3 < p_3 \leqslant Q_3$ и, следовательно, не зависит от p_2. В случае, когда $P_3 \leqslant t < Q_3$, заменяя верхнюю границу изменения p_3 величиной $z = \bigl[x(hp_1P_2)^{-1}\bigr]$. Ошибка от такой замены не превзойдет

$$\sum_{P_1 < p_1 \leqslant Q_1} \sum_{P_2 < p_2 \leqslant Q_2} \left(\frac{x}{hp_1P_2} - \frac{x}{hp_1p_2} + 1\right) \leqslant$$
$$\leqslant \frac{x}{h} \sum_{P_1 < p_1 \leqslant Q_1} \frac{1}{p_1} \sum_{P_2 < p_2 \leqslant Q_2} \frac{Q_2 - P_2}{p_1p_2P_2} \,+\, (Q_1 - P_1)(Q_2 - P_2) \,\leqslant$$
$$\leqslant \frac{x}{h}(\log p)^{-4} \sum_{P_1 < p_1 \leqslant Q_1} \frac{1}{p_1} \sum_{P_2 < p_2 \leqslant Q_2} \frac{1}{p_2} \,+\, \frac{x}{hY}\,(\log p)^{-4} \,=\, s(h; P_1, P_2).$$

Так как вклад от величин $s(h; P_1, P_2)$ в $S_{c,d}$ не превосходит

$$\frac{x}{(\log p)^4} \sum_{h \leqslant x} \frac{1}{h} \sum_{X < p_1, p_2 \leqslant Y} \frac{1}{p_1p_2} \,<\, \frac{x}{(\log p)^2},$$

то

$$S_{c,d} \,=\, \frac{1}{cd(c-1)} \sum_{h} \sum_{P_1,P_2,P_3} V \,+\, \theta\Big(\frac{x(\log p)^{-2}}{cd(c-1)} \,+\, 2xX^{-1}\Big),$$

где

$$V \,=\, V_{c,d}(h;P_1,P_2,P_3) \,=\, \sum_{P_1<p_1\leqslant Q_1} \sum_{P_2<p_2\leqslant R_2} \sum_{P_3<p_3\leqslant \min(Q_3,z)} e_p(a_1p_1^*p_2^*p_3^*).$$

Преобразуем V так, чтобы границы области изменения p_2 и p_3 не зависели от p_1. Имеем:

$$V \,=$$

$$=\, \sum_{\substack{P_j<p_j\leqslant Q_j\\ j=1,2,3}} \frac{1}{p}\Big(\sum_{|f|<p/2} \sum_{1\leqslant\lambda\leqslant y} e_p(f(p_2-\lambda))\Big) \frac{1}{p}\Big(\sum_{|g|<p/2} \sum_{1\leqslant\mu\leqslant z} e_p(g(p_3-\mu))\Big) e_p(a_1p_1^*p_2^*p_3^*) \,=$$

$$=\, \sum_{|f|,|g|<p/2} \frac{W}{(|f|+1)(|g|+1)},$$

$$\text{где}\quad W = W(f,g) = \sum_{\substack{P_j<p_j\leqslant Q_j\\ j=1,2,3}} F(p_1)G(p_2)H(p_3)e_p(a_1p_1^*p_2^*p_3^*),$$

$$F(p_1) \,=\, \frac{|f|+1}{p}\Big(\sum_{1\leqslant\lambda\leqslant y} e_p(-f\lambda)\Big) \cdot \frac{|g|+1}{p}\Big(\sum_{1\leqslant\mu\leqslant z} e_p(-g\mu)\Big),$$

$$G(p_2) \,=\, e_p(fp_2), \quad H(p_3) \,=\, e_p(gp_3),$$

причем, как несложно видеть, каждая из величин $F(p_1), G(p_2), H(p_3)$ по модулю не превосходит единицы.

Определим теперь числа k_j из неравенств

$$p^{\frac{1}{2k_j}} \,\leqslant\, P_j \,\leqslant\, p^{\frac{1}{2(k_j-1)}}$$

и положим

$$l_j \,=\, 2n_j \,=\, \begin{cases} k_j, & \text{если } k_j \text{ чётное},\\ k_j+1, & \text{если } k_j \text{ нечётное}. \end{cases}$$

Тогда из леммы 11 и замечания к ней получаем:

$$|W|^k \,\leqslant\, (P_1P_2P_3)^k \sum_{h_1,h_2,h_3=0}^{p-1} \alpha_1(h_1)\alpha_2(h_2)\alpha_3(h_3)e_p\big(a_1\,h_1h_2h_3\big),$$

где $k = l_1l_2l_3$, $\alpha_j(h) = P_j^{-l_j}\xi_j(h)$, а величина $|\xi_j(h)|$ не превосходит числа решений сравнения

$$x_1^* + \ldots + x_{n_j}^* \,\equiv\, x_{n_j+1}^* + \ldots + x_{2n_j}^* + h (\mathrm{mod}\ p)$$

в простых числах x_s, $P_j < x_s \leqslant Q_j$, $s = 1,\ldots,2n_j$. Покажем, что весовые функции $\alpha_j(h)$ удовлетворяют условиям леммы 12. Действительно,

$$\|\alpha_j\|_1 \,=\, \sum_{h=0}^{p-1} |\alpha_j(h)| \,=\, P_j^{-l_j} \sum_{h=0}^{p-1} |\xi_j(h)| \,\leqslant P_j^{-l_j} \cdot P_j^{l_j} \,=\, 1.$$

Далее, предположим сперва, что k_j – чётное число. Тогда $l_j = k_j$, так что сумма величин $|\xi_j(h)|^2$ не превзойдёт числа решений сравнения

$$x_1^* + \ldots + x_{k_j}^* \,\equiv\, x_{k_j+1}^* + \ldots + x_{2k_j}^* (\mathrm{mod}\ p), \quad P_j < x_1,\ldots,x_{2k_j} \leqslant Q_j.$$

В силу леммы 13,

$$\|\alpha_j\|_2^2 \leqslant P_j^{-2l_j}\, k_j! P_j^{k_j}\left(\frac{2k_j(2P_j)^{2k_j-1}}{p} + 1\right) < 2^{2k_j}(k_j+1)!\left(\frac{P_j^{k_j-1}}{p} + P_j^{-k_j}\right) \leqslant$$
$$\leqslant (2k_j)^{k_j} p^{-0.5} \leqslant (2n)^n p^{-0.5} < e^{(\log p)^{1/2}\log\log p} p^{-0.5} < p^{-0.4}.$$

Предположим теперь, что k_j нечётное. Тогда $l_j = k_j+1$, а сумма величин $|\xi_j(h)|^2$ не превзойдёт числа решений сравнения

$$x_1^* + \ldots + x_{k_j+1}^* \equiv x_{k_j+2}^* + \ldots + x_{2k_j+2}^* (\mathrm{mod}\ p), \quad P_j < x_1, \ldots, x_{2k_j+2} \leqslant Q_j.$$

Фиксируя переменные $x_{k_j+1}, x_{2(k_j+1)}$ (не более чем $\leqslant P_j^2$ способами), получим сравнение вида

$$x_1^* + \ldots + x_{k_j}^* \equiv x_{k_j+1}^* + \ldots + x_{2k_j}^* + h (\mathrm{mod}\ p), \quad P_j < x_1, \ldots, x_{2k_j} \leqslant Q_j.$$

Оценивая число его решений с помощью леммы 13, будем иметь:

$$\|\alpha_j\|_2^2 = P_j^{-2l_j} \cdot P_j^2\, k_j! P_j^{k_j}\left(\frac{2k_j(2P_j)^{2k_j-1}}{p} + 1\right) < (2k_j)^{k_j} p^{-0.5} < p^{-0.4}.$$

Таким образом, в каждом из случаев $\|\alpha_j\|_2 < p^{-0.2}$. Следовательно, неравенство $\|\alpha_1\|_2 \cdot \|\alpha_2\|_2 \cdot \|\alpha_3\|_2 < p^{-0.5-c}$ выполняется с $c = 0.1$. Поэтому в силу леммы 12 имеем:

$$|W|^k \leqslant (P_1P_2P_3)^k p^{-c_1}, \quad c_1 = (0.1c)^{10^4} = 10^{-2\cdot 10^4}.$$

Так как $k \leqslant (k_1+1)(k_2+1)(k_3+1) \leqslant 8mn^2$, то

$$|W| \leqslant P_1P_2P_3 p^{-\frac{c_1}{k}} \leqslant \frac{x}{h} p^{-\frac{c_1}{8mn^2}}.$$

Возвращаясь к оценке исходной суммы, находим:

$$|V| \leqslant \frac{x}{h}(\log p + 1)^2 p^{-\frac{c_1}{8mn^2}},$$
$$|S_{c,d}| \leqslant \frac{2x}{cd(c-1)}(\log p + 1)^2 p^{-\frac{c_1}{8mn^2}} \sum_h \frac{1}{h} \sum_{P_1,P_2,P_3} 1 \leqslant \frac{2x}{cd(c-1)}(\log p + 1)^9 p^{-\frac{c_1}{8mn^2}},$$
$$\left|\sum_{\nu\in B} e_p(a\nu^*)\right| \leqslant x(\log p + 1)^{10} p^{-\frac{c_1}{8mn^2}},$$
$$\left|\sum_{\nu\in B} e_p(a\nu^*)\right| \leqslant 7x\frac{m}{n}\log\frac{n}{m} + x(\log p + 1)^{10} p^{-\frac{c_1}{8mn^2}}.$$

Беря теперь

$$n = \left[\frac{10^{-10^4}\sqrt{\log x}}{7\log\log p}\right],$$

приходим к искомому утверждению. □

Заключение

Завершим настоящий обзор рядом замечаний.

1. Из теоремы 4 с помощью тождества И.М. Виноградова в форме Р. Вона (см., например, [47, гл. II, §6]) стандартным образом выводится оценка суммы Клоостермана по простым числам. Именно, справедлива

Теорема 7. *Пусть выполнены условия теоремы* 4. *Тогда для суммы*

$$S_1 = \sum_{\varpi \leqslant N} e_q(a\varpi^* + b\varpi),$$

где ϖ *пробегает простые числа, справедлива оценка:* $|S| < N^{1-c_1/\varrho^2}$, $c_1 = 2^{-11}c$.

2. Теорема 5 в случае $b \equiv 0 \pmod p$ значительно уступает по силе теореме 6. Так, в случае $x = p^\alpha$, где $0 < \alpha \leqslant 0.5$ - фиксированная постоянная эти теоремы приводят, соответственно, к оценкам

$$\sum_{\nu \leqslant x} e_p(a\nu^*) \ll \frac{x(\log\log p)^{4/7}}{(\log p)^{1/7}}, \quad \sum_{\nu \leqslant x} e_p(a\nu^*) \ll \frac{x(\log\log p)^3}{(\log p)^{1/2}}.$$

Однако соединение метода Карацубы с леммой 13 и разбиением промежутка $1 \leqslant \nu \leqslant x$ на множества A и B, которое применялось Ж. Бургейном и М.З. Гараевым в теореме 6, позволяет доказать следующие утверждения, несколько расширяющие диапазон нетривиальности оценок теорем 5 и 6 (см. [43]). Так, справедливы:

Теорема 8. *Пусть* $e^{(\log p)^{2/3}(\log\log p)^{4/3}} < x \leqslant \sqrt{p}$, $(a,p) = 1$. *Тогда*

$$\sum_{\nu \leqslant x} e_p(a\nu^*) \ll xD_1^{-1}, \quad D_1 = \frac{(\log x)^{3/2}}{(\log p)(\log\log p)^2}.$$

Теорема 9. *Пусть* $e^{(\log p)^{2/3}(\log\log p)^{1/3}} < x \leqslant \sqrt{p}$, $(ab,p) = 1$. *Тогда*

$$\sum_{\nu \leqslant x} e_p(a\nu^*) \ll xD_2^{-1}(\log D_2),$$

$$\sum_{\nu \leqslant x} e_p(a\nu^* + b\nu) \ll xD_2^{-3/4}, \quad D_2 = \frac{\log x}{(\log p)^{2/3}(\log\log p)^{1/3}}.$$

Эти утверждения представляются не лишёнными интереса потому, что их доказательство вполне элементарно и не опирается на лемму Бургейна. Отметим, что в доказательстве теоремы 6 оценка трилинейной суммы W из условия леммы 12 используется в случае, когда нормы $\|\alpha_j\|_2$ не превышают $p^{-1/4}\tau$, где величина τ растет не быстрее сколь угодно малой степени p. Очень краткое и изящное доказательство оценки вида $W \ll \tau^{33/18}p^{-1/4} + \max_{j=1,2,3}|\alpha_j(0)|$ (где $\tau \geqslant 1$), отличное от доказательства Ж. Бургейна [46], было найдено И.Д. Шкредовым (частное сообщение от 28 июня 2016 г.). Оно опирается на оценку трилинейной суммы из недавней работы Г. Петридиса и И.Е. Шпарлинского [50].

3. В случае, когда $x \asymp p^\alpha$, где $0 < \alpha < 0.5$ – фиксированное число, отстоящее от значений вида $(2k)^{-1}$, $k = 1, 2, 3, \ldots$, оценки сумм из п. 2 могут быть усилены (см. [51]). Именно, справедлива

Теорема 10. *Пусть* $k \geqslant 2$ *– фиксированное целое число,* c *– абсолютная постоянная с условием* $0 < c \leqslant 0.25$, $\varepsilon = c/(k^2 - k)$. *Тогда при любых* x, *таких, что* $p^{1/(2k)+\varepsilon} \leqslant x \leqslant p^{1/(2k-2)-\varepsilon}$ *имеет место оценка*

$$\sum_{\nu \leqslant x} e_p(a\nu^* + b\nu) \ll_{c,k} x\,\frac{\log\log p}{\log p}.$$

4. Утверждения, подобные теоремам 5, 6, справедливы для сумм вида

$$\sum_{\nu\leqslant x} f(\nu)e_p(a\nu^* + b\nu),$$

где $f(\nu)$ – любая из функций $\tau_k(\nu), 2^{\omega(\nu)}$, $\varphi(\nu)$, $r(\nu)$ (здесь $\tau_k(\nu)$ – многомерная функция делителей, $\omega(\nu)$ – число различных простых делителей ν, $r(\nu)$ - количество представлений ν суммою двух квадратов целых чисел). Более того, все утверждения теорем 5, 6 остаются в силе для случая, когда $f(\nu)$ – произвольная мультипликативная функция с условием $|f(\nu)| \leqslant 1$. Исследованию сумм такого типа в случае произвольного модуля q и $x \geqslant q^{0.5+\varepsilon}$ посвящены работы [52]- [55], в случае простого q - статьи [56], [57].

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Salie H. Über die Kloostermanschen Summen $S(u, v; q)$ // *Math. Z.*, **34** (1931), 91–109.
2. Whiteman A.L. A note on Kloosterman sums // *Bull. Amer. Math. Soc.* **51**:6 (1945), 373–377.
3. Williams K.S. Note on the Kloosterman sum // *Proc. Amer. Math. Soc.* **30**:1 (1971), 61–62.
4. Kloosterman H.D. On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$ // *Acta Math.*, **49** (1926), 407–464.
5. Виноградов И.М. Об одной тригонометрической сумме и ее приложениях в теории чисел // *Доклады АН СССР. Нов. сер.*, **5** (1933), 195–204.
6. Виноградов И.М. О некоторых тригонометрических суммах и их приложениях, *Доклады АН СССР. Нов. сер.*, **6** (1933), 249–255.
7. Виноградов И.М.Тригонометрические суммы, зависящие от составного модуля // *Доклады АН СССР. Нов. сер.*, **5** (1934), 225–229.
8. Tolev D.I. An identity for the Kloosterman sum // `arXiv:1007.2054 [math.NT]` (2010).
9. Salie H. Zur Abschätzung der Fourierkoeffizienten ganzer Modulformen // *Math. Z.*, **36** (1932), 263–278.
10. Davenport H. On certain exponential sums // *J. reine angew. Math.*, **169** (1933), 158–176.
11. Weil A. On some exponential sums // *Proc. Nat. Acad. Sci. USA*, **34** (1948), 204–207.
12. Степанов С.А. Об оценке сумм Клостермана // *Изв. АН СССР. Сер. матем.*, **35**:2 (1971), 308–323.
13. Королёв М.А. О нелинейной сумме Клоостермана // *Чебышевский сб.*, **17**:1 (2016), 140–147.
14. Карацуба А.А. Распределение обратных величин в кольце вычетов по заданному модулю // *Доклады АН*, **333**:2 (1993), 138–139.
15. Карацуба А.А. Дробные доли специального вида функций // *Изв. РАН. Сер. матем.*, **59**:4 (1995), 61–80
16. Карацуба А.А. Аналоги сумм Клоостермана // *Изв. РАН. Сер. матем.*, **59**:5 (1995), 93–102.

17. Карацуба А.А. Суммы дробных долей специального вида функций // *Доклады АН*, **54**:1 (1996), 541.

18. Карацуба А.А. Аналоги неполных сумм Клоостермана и их приложения // *Tatra Mt. Math. Publ.*, **11** (1997), 89–120.

19. Карацуба А.А. Двойные суммы Клоостермана // *Матем. заметки*, **66**:5 (1999), 682–687.

20. Постников А.Г. О сумме характеров по модулю, равному степени простого числа // *Изв. АН СССР. Сер. матем.*, **19**:1 (1955), 11–16.

21. Postnikov A.G. On dirichlet L-series with the character modulus equal to the power of a prime number // *J. Indian Math. Soc. (N.S.)*, **20** (1956), 217–226.

22. Королёв М.А. Неполные суммы Клоостермана и их приложения // *Изв. РАН. Сер. матем.*, **64**:6 (2000), 41–64.

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

24. Heath-Brown D.R. Arithmetic applications of Kloosterman sums // *Nieuw. Arch. Wiskd.*, **5/1**:4 (2000), 380–384.

25. Устинов А.В. Приложения сумм Клоостермана к арифметике и геометрии. Алгоритм Евклида, цепные дроби, решетки и числа Фробениуса. Lambert Academic Publishing, 2011.

26. Виноградов И.М. Новые приложения тригонометрических сумм // *Доклады АН СССР. Нов. сер.*, **1** (1934), 10–14.

27. Виноградов И.М. Новые асимптотические выражения // *Доклады АН СССР. Нов. сер.*, **1** (1934), 49–51.

28. Розин С.М. О нулях L-рядов Дирихле // *Изв. АН СССР. Сер. матем.*, **23**:4 (1959), 503–508.

29. Чудаков Н.Г. О нулях L-функций Дирихле для модулей, равных степеням нечётного простого // *Вестник ЛГУ. Сер. матем., мех. астрон.*, **1** (1966), 93–98.

30. Карацуба А.А. Тригонометрические суммы специального вида и их приложения // *Изв. АН СССР. Сер. матем.*, **28**:1 (1964), 237–248.

31. Чубариков В.Н. Уточнение границы нулей L-рядов Дирихле по модулю, равному степени простого числа // *Вестник МГУ. Сер. матем., мех.*, **2** (1973), 46–52.

32. Burgess D.A. The distribution of quadratic residues and non-residues // *Mathematika*, **4**:1 (1957), 106–112.

33. Burgess D.A. On character sums and primitive roots // *Proc. London Math. Soc.* (3), **12** (1962), 179–192.

34. Burgess D.A. On character sums and L-series // *Proc. London Math. Soc.* (3), **12** (1962), 193–206.

35. Карацуба А.А. Суммы характеров с простыми числами // *Изв. АН СССР. Сер. матем.*, **34**:2 (1970), 299–321.

36. Копанева А.А. Оценка коротких сумм характеров Дирихле по сдвинутым простым числам // *Чебышевский сб.*, **9**:1 (2008), 122–143.

37. Копанева А.А., Бурлакова Е.А. Оценка сумм характеров по сплошному промежутку суммирования // *Чебышевский сб.*, **14**:2 (2013), 118–122.

38. Степанов С.А., Шпарлинский И.Е. Об оценке тригонометрических сумм с рациональными и алгебраическими функциями. // В сб.: *Автоморфные функции и теория чисел.* Владивосток, 1989. С. 5–18.

39. Карацуба А.А. Основы аналитической теории чисел. 2-е изд. М., Наука, 1983.

40. Карацуба А.А. Оценки тригонометричеких сумм особого вида и их приложения // *Докл. АН СССР*, **137** (1961), 513–514.

41. Карацуба А.А. Рациональные тригонометрические суммы специального вида и их приложения. *Автореферат дисс. на соискание уч. ст. к. ф.-м. н.* М., МГПИ им. В.И. Ленина, 1962.

42. Виноградов А.И. О числах с малыми простыми делителями // *Доклады АН СССР*, **109**:4 (1956), 683–686.

43. Королёв М.А. О методе Карацубы оценок сумм Клоостермана // *Мат. сборник*, **207**:8 (2016), 117–134.

44. Прахар К. Распределение простых чисел. М., Мир, 1967.

45. Bourgain J., Garaev M.Z. Kloosterman sums in residue rings // *Acta Arith.*, **164**:1 (2014), 43–64.

46. Bourgain J. Multilinear exponential sums in prime fields under optimal entropy condition on the sources // *Geom. Funct. Anal.*, **18**:5 (2009), 1477–1502.

47. Воронин С.М., Карацуба А.А. Дзета-функция Римана. М., Физматлит, 1994.

48. Iwaniec H. On zeros of Dirichlet L-series // *Invent. Math.* **23** (1974), 97–104.

49. Королев М.А. Короткие суммы Клоостермана по мощному модулю // *Доклады РАН*, **470**:5 (2016), 505–507

50. Petridis G., Shparlinski I.E. Bounds of trilinear and quadrilinear exponential sums // `arXiv:1604.08469v2 [math.NT]`.

51. Королёв М.А. О коротких суммах Клоостермана по простому модулю // *Матем. заметки*, **100**:6 (2016), 843–851.

52. Hajela D., Pollington A., Smith B. On Kloosterman sums with oscillating coefficients // *Canad. Math. Bull.* **31**:1 (1988), 32–36.

53. Wang G., Zheng Z. Kloosterman sums with oscillating coefficients // *Chinese Ann. Math.*, **19** (1998), 237–242 (Chinese); English transl.: *Chinese J. Contemp. Math.* **19** (1998), 185–191.

54. Deng P. On Kloosterman sums with oscillating coefficients // *Canad. Math. Bull.* **42**:3 (1999), 285–290.

55. Gong K., Jia C. Kloosterman sums with multiplicative coefficients // *Sci. China Math.* **59**:4 (2016), 653–660.

56. Королёв М.А. Короткие суммы Клоостермана с весами // *Матем. заметки*, **88**:3 (2010), 415–427.

57. Korolev M.A., On Kloosterman sums with multiplicative coefficients // `arXiv: 1610.09171 [math.NT]`.

REFERENCES

1. Salie H. 1931, "Über die Kloostermanschen Summen $S(u, v; q)$", Math. Z., vol. 34, pp. 91–109.

2. Whiteman A.L. 1945, "A note on Kloosterman sums", Bull. Amer. Math. Soc., vol. 51, no. 6, pp. 373–377.

3. Williams K.S. 1971, "Note on the Kloosterman sum", Proc. Amer. Math. Soc., vol. 30, no. 1, pp. 61–62.

4. Kloosterman H.D. 1926, "On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$", Acta Math., vol. 49, pp. 407–464.

5. Vinogradow I.M. 1933, "On a certain trigonometrical expressions and its applications in the theory of numbers", Compt. Rend. Acad. Sci. URSS. N.S., vol. 5, pp. 195–204 (Russian; English summary).

6. Vinogradow I.M. 1933, "Some trigonometrical polynomes and their applications", Compt. Rend. Acad. Sci. URSS. N.S., vol. 6, pp. 249–255 (Russian; English summary).

7. Vinogradow I.M. 1934, "Trigonometrical polynomials for complicated moduli", Compt. Rend. Acad. Sci. URSS. N.S., vol. 5, pp. 225–229 (Russian; English summary).

8. Tolev D.I. 2010, "An identity for the Kloosterman sum", `arXiv:1007.2054 [math.NT]`.

9. Salie H. 1932, "Zur Abschätzung der Fourierkoeffizienten ganzer Modulformen", Math. Z., vol. 36, pp. 263–278.

10. Davenport H. 1933, "On certain exponential sums", J. reine angew. Math., vol. 169, pp. 158–176.

11. Weil A. 1948, "On some exponential sums", Proc. Nat. Acad. Sci. USA, vol. 34, pp. 204–207.

12. Stepanov S.A. 1971, "An estimation of Kloosterman sums", Izv. Akad. Nauk SSSR Ser. Mat., vol. 35, no. 2, pp. 308–323.

13. Korolev M.A. 2016, "On non-linear Kloosterman sum", Chebyshevsk. sb., vol. 17, no. 1, pp. 140–147.

14. A.A. Karatsuba. 1993, "Distribution of inverse values in a residue ring modulo a given number", Russian Acad. Sci. Dokl. Math., vol. 48, no. 3, pp. 452–454.

15. A.A. Karatsuba. 1995, "Fractional parts of functions of a special form", Izv. Math., vol. 59, no. 4, pp. 721–740.

16. A.A. Karatsuba. 1995, "Analogues of Kloosterman sums", Izv. Math., vol. 59, no. 5, pp. 971–981.

17. A.A. Karatsuba. 1996, "Sums of fractional parts of functions of a special form", Russian Acad. Sci. Dokl. Math., vol. 54, no. 1, p. 541.

18. A.A. Karatsuba. 1997, “Analogues of incomplete Kloosterman sums and their applications”, Tatra Mt. Math. Publ., vol. 11, pp. 89–120.

19. A.A. Karatsuba. 1999, “Double Kloosterman sums”, Math. Notes, vol. 66, no. 5, pp. 565–569.

20. A.G. Postnikov. 1955, “On the sum of characters with respect to a modulus equal to a power of a prime number”, Izv. Akad. Nauk SSSR Ser. Mat., vol. 19, no. 1, pp. 11–16.

21. A.G. Postnikov. 1956, “On dirichlet L-series with the character modulus equal to the power of a prime number”, J. Indian Math. Soc. (N.S.), vol. 20, pp. 217–226.

22. M.A. Korolev. 2000, “Incomplete Kloosterman sums and their applications”, Izv. Math., vol. 64, no. 6, pp. 1129–1152.

23. J. Bourgain, M.Z. Garaev. 2014, “Sumsets of reciprocals in prime fields and multilinear Kloosterman sums”, Izv. RAN. Ser. Mat., vol. 78, no. 4, pp. 19–72.

24. Heath-Brown D.R. 2000, “Arithmetic applications of Kloosterman sums”, Nieuw. Arch. Wiskd., vol. 5/1, no. 4, pp. 380–384.

25. A.V. Ustinov. 2011. Applications of Kloosterman Sums in Arithmetic and Geometry, Lambert Academic Publishing. (Russian).

26. I.M. Vinogradow. 1934, “New applications of trigonometrical polynomes”, Compt. Rend. Acad. Sci. URSS. N.S., vol. 1, pp. 10–14 (Russian; English summary).

27. I.M. Vinogradow. 1934, “New asymptotic expressions”, Compt. Rend. Acad. Sci. URSS. N.S., vol. 2, pp. 49–51 (Russian; English summary).

28. S.M. Rozin. 1959, “On null Dirichlet L-series”, Izv. Akad. Nauk SSSR Ser. Mat., vol. 23, no. 4, pp. 503–508.

29. N.G. Chudakov. 1966, “On the zeros of Dirichlet L-functions for moduli equal to the powers of an odd prime”, Vestn. Leningr. State Univ. Ser. Mathem., mech. and astron., vol. 1, pp. 93–98 (Russian).

30. A.A. Karatsuba. 1964, “Trigonometric sums of a special type and their applications”, Izv. Akad. Nauk SSSR. Ser. Mat., vol. 28, no. 1, pp. 237–248.

31. V.N. Chubarikov. 1973, “More precise band for zeroes of Dirichlet L-series in modul equal to power of a prime number”, Vestn. Moscow State Univ. Ser. Math. Mech., vol. 2, pp. 46–52 (Russian).

32. D.A. Burgess. 1957, “The distribution of quadratic residues and non-residues”, Mathematika, vol. 4, no. 1, pp. 106–112.

33. D.A. Burgess. 1962, “On character sums and primitive roots”, Proc. London Math. Soc. (3), vol. 12, pp. 179–192.

34. D.A. Burgess. 1962, “On character sums and L-series”, Proc. London Math. Soc. (3), vol. 12, pp. 193–206.

35. A.A. Karatsuba. 1970, “Sums of characters over prime numbers”, Math. USSR-Izv., vol. 4, no. 2, pp. 303–326.

36. A.A. Kopaneva. 2008, “An estimate for short sums of Dirichlet characters over shifted primes”, Chebyshevsk. sb., vol. 9, no. 1, pp. 122–143.

37. A.A. Kopaneva, E.A. Burlakova. 2013, “Evaluation of character sums over the continuous interval of summation”, Chebyshevsk. sb., vol. 14, no. 2, pp. 118–122.

38. Stepanov S.A., Shparlinski I.E. 1989, “On the estimate of exponential sums with rational and algebraic functions”, Authomorphic functions and number theory. pp. 5–18 (Russian).

39. A.A. Karatsuba. 1993, Basics analytic number theory. Springer-Verlag, Berlin Heidelberg.

40. A.A. Karatsuba. 1961, “Estimates of trigonometric sums of a special form, and their applications”, Dokl. Akad. Nauk SSSR, vol. 137, pp. 513–514.

41. A.A. Karatsuba. 1962, Rational trigonometric sums of a special form, and their applications. *PhD Thesis*, Moscow, Moscow State Pedegogical Institute in the name of V.I. Lenin (Russian).

42. A.I. Vinogradov. 1956, “On the numbers with small prime factors”, Dokl. Akad. Nauk SSSR (N.S.), vol. 109, no. 4, pp. 683–686.

43. M.A. Korolev. 2016, “On Karatsuba’s method of estimating of Kloosterman sums”, Math. Sb., vol. 207, no. 8, pp. 1142–1158.

44. K. Prachar. 1957, Primzahlverteilung. Springer-Verlag.

45. J. Bourgain, M.Z. Garaev. 2014, “Kloosterman sums in residue rings”, Acta Arith., vol. 164, no. 1, pp. 43–64.

46. J. Bourgain. 2009, “Multilinear exponential sums in prime fields under optimal entropy condition on the sources”, Geom. Funct. Anal., vol. 18, no. 5, pp. 1477–1502.

47. A.A. Karatsuba, S.M. Voronin. 1992, The Riemann zeta function, W. de Gruyter, Berlin New York.

48. H. Iwaniec. 1974, “On zeros of Dirichlet L-series”, Invent. Math., vol. 23, pp. 97–104.

49. M.A. Korolev. 2016, “Short Kloosterman sums to powerful modulus”, Doklady Mathematics, vol. 94, no. 2, pp. 561–562.

50. Petridis G., Shparlinski I.E. Bounds of trilinear and quadrilinear exponential sums // `arXiv:1604.08469v2 [math.NT]`.

51. M.A. Korolev. 2016, “Short Kloosterman sums of modulo prime”, Mat. Zametki, vol. 100, no. 6, pp. 843–851.

52. D. Hajela, A. Pollington, B. Smith. 1988, “On Kloosterman sums with oscillating coefficients”, Canad. Math. Bull., vol. 31, no. 1, pp. 32–36.

53. G. Wang, Z. Zheng. 1998, “Kloosterman sums with oscillating coefficients”, Chinese Ann. Math., vol. 19, pp. 237–242 (Chinese); English transl.: Chinese J. Contemp. Math., vol. 19, pp. 185–191.

54. P. Deng. 1999, “On Kloosterman sums with oscillating coefficients”, Canad. Math. Bull., vol. 42, no. 3, pp. 285–290.

55. K. Gong, C. Jia. 2016, “Kloosterman sums with multiplicative coefficients”, Sci. China Math., vol. 59, no. 4, pp. 653–660.

56. M.A. Korolev. 2010, “Short Kloosterman Sums with Weights”, Math. Notes, vol. 88, no. 3, pp. 374–385.

57. Korolev M.A., On Kloosterman sums with multiplicative coefficients // `arXiv: 1610.09171 [math.NT]`.

Математический институт им. В. А. Стеклова.

Поступило 22.04.2016 г.
Принято в печать 12.12.2016 г.