Math-Net.Ru

Общероссийский математический портал

М. З. Гараев, Оценка сумм Kloostermana с простыми числами и применение, *Матем. заметки*, 2010, том 88, выпуск 3, 365–373

DOI: <https://doi.org/10.4213/mzm7829>

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: 3.93.64.190

26 апреля 2023 г., 10:14:57

УДК 511.33

Оценка сумм Клоостермана с простыми числами и применение

М. З. Гараев

Пусть p – большое простое число. В работе доказывается, что для любого натурального числа $N < p$ имеет место оценка

$$\max_{(a,p)=1} \left| \sum_{q \leq N} e^{2\pi i a q^* / p} \right| \leq (N^{15/16} + N^{2/3} p^{1/4}) p^{o(1)},$$

где q обозначает простое число, а q^* обозначает наименьшее натуральное число такое, что $qq^* \equiv 1 \pmod{p}$. Следствием этой оценки является следующее утверждение: если $p > N > p^{16/17+\varepsilon}$, где $\varepsilon > 0$, и если $\lambda \not\equiv 0 \pmod{p}$, то число J решений сравнения

$$q_1(q_2 + q_3) \equiv \lambda \pmod{p}$$

в простых числах $q_1, q_2, q_3 \leq N$ может быть представлено в виде

$$J = \frac{\pi(N)^3}{p} (1 + O(p^{-\delta})), \quad \delta = \delta(\varepsilon) > 0.$$

Оно улучшает недавний результат Фридландера, Курлберга и Шпарлинского, в котором требовалось условие $p > N > p^{38/39+\varepsilon}$.

Библиография: 11 названий.

*Посвящается доброй памяти
Анатолия Алексеевича Карацубы*

1. Введение. Всюду в статье p – достаточно большое простое число, ε – сколь угодно малое фиксированное положительное число. Выражение вида $A \lesssim B$ будет означать, что $|A| \leq Bp^{o(1)}$, или, что то же самое, $|A| \ll Bp^\varepsilon$, где постоянная в символе Виноградова может зависеть только от ε . При $(a, p) = 1$ и $N < p$ рассматриваем сумму

$$S(a; p, N) = \sum_{q \leq N} e^{2\pi i a q^* / p},$$

где суммирование ведется по простым числам q , а q^* обозначает наименьшее натуральное число такое, что $qq^* \equiv 1 \pmod{p}$. Эта сумма является аналогом неполных сумм Клоостермана. Сумма вида

$$\sum_{q \leq N} e^{2\pi i (aq^* + bq) / m}$$

по-видимому еще была рассмотрена Карацубой в начале 90-х гг. Об этом свидетельствует работа [1], в которой содержатся утверждения (без доказательств) о распределении дробных долей

$$\left\{ \frac{aq^* + bq}{m} \right\}, \quad q \leq N,$$

при этом N может быть величиной порядка m^ε .

Суммы более общего вида, чем $S(a; p, N)$, были оценены в работах Бургейна [2], Фуври и Мишель [3]. Из результатов работы [3], в частности, следует, что

$$S(a; p, N) \lesssim N^{25/32} p^{3/16}.$$

Эта оценка была использована Фридландером, Курлбергом и Шпарлинским [4] в задаче представления классов вычетов в виде произведения простого числа на сумму двух простых чисел. Они показали, что если $p > N > p^{38/39+\varepsilon}$ и $\lambda \not\equiv 0 \pmod{p}$, то имеется $(1+o(1))\pi(N)^3/p$ троек простых чисел $q_1, q_2, q_3 \leq N$ таких, что $q_1(q_2 + q_3) \equiv \lambda \pmod{p}$. Задача была мотивирована условным (при некоторых предположениях о границах нулей L -функций Дирихле) результатом Эрдёша, Оддыжко и Саркози [5] о представлении классов вычетов в виде произведения трех простых чисел.

В настоящей работе доказываем следующую оценку для $S(a; p, N)$.

ТЕОРЕМА 1.1. *При $(a, p) = 1$ имеет место оценка*

$$S(a; p, N) \lesssim N^{15/16} + N^{2/3} p^{1/4}.$$

Из теоремы 1.1 получаем следующее улучшение результата Фридландера, Курлберга и Шпарлинского [4].

СЛЕДСТВИЕ 1. *Пусть $p > N > p^{16/17+\varepsilon}$, $\lambda \not\equiv 0 \pmod{p}$. Тогда число J решений сравнения*

$$q_1(q_2 + q_3) \equiv \lambda \pmod{p}$$

в простых числах $q_1, q_2, q_3 \leq N$ можно представить в виде

$$J = \frac{\pi(N)^3}{p} (1 + O(p^{-\delta})), \quad \delta = \delta(\varepsilon) > 0.$$

Доказательство теоремы 1.1 основано на оценках специальных двойных сумм Клоостермана (см. лемму 2.4). Оценки таких сумм в очень коротких промежутках известны по работам Карацубы [6], [7] и Королёва [8]. Доказательство леммы 2.4, в свою очередь, опирается на один из результатов Хиз-Брауна (см. лемму 2.3).

Далее в статье будем пользоваться сокращением

$$e_p(z) = e^{2\pi iz/p}.$$

2. Леммы. Напомним следующую простую оценку двойных тригонометрических сумм.

ЛЕММА 2.1. *Пусть $(a, p) = 1$. Тогда*

$$\left| \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \nu(x) \varrho(y) e_p(axy) \right| \leq \sqrt{pXY},$$

где $\nu(x)$, $\varrho(y)$ – комплексные числа и

$$\sum_{x=0}^{p-1} |\nu(x)|^2 = X, \quad \sum_{y=0}^{p-1} |\varrho(y)|^2 = Y.$$

Лемма 2.1 содержится в учебнике Виноградова [9; гл. 6] в качестве упражнения. Доказательство следует из применения неравенства Коши–Буняковского и основных тригонометрических тождеств.

Нам также понадобится следующая хорошо известная оценка Вейля неполных сумм Клоостермана.

ЛЕММА 2.2. Пусть $1 \leq K_1 \leq K_2 < p$. Тогда

$$\max_{(a,p)=1} \left| \sum_{x=K_1}^{K_2} e_p(ax^*) \right| \ll p^{1/2} \log p.$$

Следующая лемма следует из работы Хиз-Брауна [10; с. 368].

ЛЕММА 2.3. Пусть $1 \leq K < p$. Для числа J_K решений сравнения

$$x_1^* + x_2^* \equiv x_3^* + x_4^* \pmod{p}, \quad 1 \leq x_1, x_2, x_3, x_4 \leq K,$$

имеет место оценка

$$J_K \lesssim \frac{K^{7/2}}{p^{1/2}} + K^2.$$

В частности, если $K \gg p^{1/3}$, то имеет место оценка $J_K \lesssim K^{7/2} p^{-1/2}$. Кроме того, если $K \ll p^{1/3}$, то $J_K \lesssim K^2$.

Для удобства читателя приведем доказательство леммы 2.3, выбирая только необходимые для нас части [10].

ДОКАЗАТЕЛЬСТВО ЛЕММЫ 2.3. Для данного целого числа λ через $I_K(\lambda)$ обозначим число решений сравнения

$$x_1 + x_2 \equiv \lambda x_1 x_2 \pmod{p}, \quad 1 \leq x_1, x_2 \leq K. \quad (1)$$

Ясно, что

$$J_K = \sum_{\lambda=0}^{p-1} I(\lambda)^2 \leq K^2 + \sum_{\lambda=1}^{p-1} I_K(\lambda)^2.$$

Из принципа Дирихле следует, что для любого фиксированного $\lambda \not\equiv 0 \pmod{p}$ существуют две пары целых чисел $(u_1, v_1) \neq (u_2, v_2)$ с условиями

$$0 \leq u_1, u_2 \leq \left\lfloor \sqrt{\frac{p}{K}} \right\rfloor, \quad 0 \leq v_1, v_2 \leq \lfloor \sqrt{pK} \rfloor$$

такие, что

$$u_1 + \lambda v_1 \equiv u_2 + \lambda v_2 \pmod{p}.$$

В частности, $u_1 \not\equiv u_2 \pmod{p}$, $v_1 \not\equiv v_2 \pmod{p}$. Поэтому существуют целые числа u_0 , v_0 такие, что

$$\lambda \equiv u_0 v_0^* \pmod{p}, \quad 1 \leq u_0 \leq \left\lfloor \sqrt{\frac{p}{K}} \right\rfloor, \quad |v_0| \leq \lfloor \sqrt{pK} \rfloor.$$

Итак, для данного $\lambda \not\equiv 0 \pmod{p}$ уравнение (1) может быть переписано в виде

$$v_0(x_1 + x_2) \equiv u_0x_1x_2 \pmod{p}.$$

Следовательно, для некоторого целого числа z имеет место равенство

$$v_0x_1 + v_0x_2 = u_0x_1x_2 + pz.$$

Из условий на u_0, v_0 имеем $|z| \leq 3K^{3/2}p^{-1/2}$. Так как

$$(u_0x_1 - v_0)(u_0x_2 - v_0) = -u_0pz + v_0^2,$$

легко получаем, что если z зафиксировать, то для переменных x_1 и x_2 будет не более, чем $p^{o(1)}$ возможностей.

Итак, для любого $\lambda \not\equiv 0 \pmod{p}$ имеет место оценка

$$I_K(\lambda) \lesssim K^{3/2}p^{-1/2} + 1.$$

Поэтому

$$J_K \lesssim K^2 + (K^{3/2}p^{-1/2} + 1) \sum_{\lambda=0}^{p-1} I_K(\lambda) \lesssim \frac{K^{7/2}}{p^{1/2}} + K^2.$$

Лемма доказана.

Доказательство теоремы 1.1 существенно опирается на следующую лемму.

ЛЕММА 2.4. Пусть $L, M, M_1, \dots, M_L$ – положительные целые числа, удовлетворяющие условиям $L < p, M < p$ и $M_n \leq M$ для всех n . Пусть $\beta_1, \dots, \beta_M$ – любые комплексные числа такие, что $|\beta_m| = p^{o(1)}$ для всех m . Тогда выполняются следующие три утверждения:

- если $L \gg p^{1/3}, M \gg p^{1/3}$, то

$$\max_{(a,p)=1} \sum_{n=1}^L \left| \sum_{m=1}^{M_n} \beta_m e_p(an^*m^*) \right| \lesssim (LM)^{15/16};$$

- если $M \ll p^{1/3}$, то

$$\max_{(a,p)=1} \sum_{n=1}^L \left| \sum_{m=1}^{M_n} \beta_m e_p(an^*m^*) \right| \lesssim L^{3/4} M^{1/2} p^{1/4};$$

- если $L \ll p^{1/3}$, то

$$\max_{(a,p)=1} \sum_{n=1}^L \left| \sum_{m=1}^{M_n} \beta_m e_p(an^*m^*) \right| \lesssim M^{3/4} L^{1/2} p^{1/4}.$$

ДОКАЗАТЕЛЬСТВО. Сначала с помощью стандартных приемов уберем зависимость верхнего предела во внутреннем суммировании от n . Имеем

$$\sum_{m=1}^{M_n} \beta_m e_p(an^*m^*) = \sum_{m=1}^M \beta_m e_p(an^*m^*) \left(\frac{1}{p} \sum_{|b| \leq (p-1)/2} \sum_{k=1}^{M_n} e_p(b(m-k)) \right).$$

Следовательно,

$$\left| \sum_{m=1}^{M_n} \beta_m e_p(an^* m^*) \right| \leq \frac{1}{p} \sum_{|b| \leq (p-1)/2} \left| \sum_{m=1}^M \beta_m e_p(an^* m^*) \right| \left| \sum_{k=1}^{M_n} e_p(-bk) \right|.$$

Выделяя член, соответствующий $b = 0$, а при $1 \leq |b| \leq (p-1)/2$ используя неравенство

$$\left| \sum_{k=1}^{M_n} e_p(-bk) \right| \leq \frac{p}{|b|},$$

получим

$$\left| \sum_{m=1}^{M_n} \beta_m e_p(an^* m^*) \right| \leq \left| \sum_{m=1}^M \beta_m e_p(an^* m^*) \right| + \sum_{1 \leq |b| \leq (p-1)/2} \frac{1}{|b|} \left| \sum_{m=1}^M \beta_m e_p(bm) e_p(an^* m^*) \right|.$$

Произведя суммирование по n , выводим следующую оценку:

$$\begin{aligned} & \sum_{n=1}^L \left| \sum_{m=1}^{M_n} \beta_m e_p(an^* m^*) \right| \\ & \leq \sum_{n=1}^L \left| \sum_{m=1}^M \beta_m e_p(an^* m^*) \right| + \sum_{1 \leq |b| \leq (p-1)/2} \frac{1}{|b|} \sum_{n=1}^L \left| \sum_{m=1}^M \beta_m e_p(bm) e_p(an^* m^*) \right|. \end{aligned}$$

Заметим, что для каждого b имеем

$$|\beta_m e_p(bm)| = |\beta_m| = p^{o(1)}.$$

Из этого замечания и последней оценки заключаем, что лемму действительно достаточно доказать только в случае, когда $M_n = M$ для всех n .

Далее будем пользоваться методом работ Карацубы [6], [7]. Обозначим

$$W = \sum_{n=1}^L \left| \sum_{m=1}^M \beta_m e_p(an^* m^*) \right|.$$

Для данного целого числа λ через $I_L(\lambda)$ обозначим число решений сравнения

$$n_1^* - n_2^* \equiv \lambda \pmod{p}, \quad 1 \leq n_1, n_2 \leq L. \quad (2)$$

Аналогично определяется $I_M(\lambda)$. Применяя неравенство Коши–Буняковского к сумме по переменной n , затем поменяв знаки суммирования, получим

$$W^2 \lesssim L \sum_{m_1=1}^M \sum_{m_2=1}^M \left| \sum_{n=1}^L e_p(an^*(m_1^* - m_2^*)) \right|.$$

Применяя неравенство Коши–Буняковского к суммам по m_1 и m_2 , получим

$$\begin{aligned} W^4 & \lesssim (LM)^2 \sum_{m_1=1}^M \sum_{m_2=1}^M \sum_{n_1=1}^L \sum_{n_2=1}^L e_p(a(n_1^* - n_2^*)(m_1^* - m_2^*)) \\ & = (LM)^2 \sum_{\lambda=0}^{p-1} \sum_{\nu=0}^{p-1} I_L(\lambda) I_M(\nu) e_p(a\lambda\nu). \end{aligned}$$

Следовательно, по лемме 2.1

$$W^8 \lesssim (LM)^4 p \left(\sum_{\lambda=0}^{p-1} I_L(\lambda)^2 \right) \left(\sum_{\lambda=0}^{p-1} I_M(\lambda)^2 \right).$$

Далее, из леммы 2.3 следует, что если $L \gg p^{1/3}$ и $M \gg p^{1/3}$, то

$$\sum_{\lambda=0}^{p-1} I_L(\lambda)^2 \lesssim L^{7/2} p^{-1/2}, \quad \sum_{\lambda=0}^{p-1} I_M(\lambda)^2 \lesssim M^{7/2} p^{-1/2}.$$

Таким образом, при условии $L \gg p^{1/3}$, $M \gg p^{1/3}$ имеем

$$W^8 \lesssim (LM)^{15/2}.$$

Это доказывает первое утверждение леммы.

Для доказательства второго утверждения леммы заметим, что

$$W^4 \leq L^3 \sum_{n=0}^{p-1} \left| \sum_{m=1}^M \beta_m e_p(anm^*) \right|^4 \lesssim pL^3 J_M,$$

где J_M обозначает количество решений сравнения

$$m_1^* + m_2^* \equiv m_3^* + m_4^* \pmod{p}, \quad 1 \leq m_1, m_2, m_3, m_4 \leq M.$$

Так как предполагается, что $M \ll p^{1/3}$, по лемме 2.3 имеем $J_M \lesssim M^2$. Таким образом,

$$W^4 \lesssim pL^3 M^2,$$

откуда следует второе утверждение леммы.

Третье утверждение леммы фактически содержится во втором (напомним, что мы свели лемму к случаю $M_n = M$). Действительно, существуют такие комплексные числа α_n , что $|\alpha_n| = 1$ и

$$W = \sum_{n=1}^L \alpha_n \left(\sum_{m=1}^M \beta_m e_p(an^* m^*) \right) \lesssim \sum_{m=1}^M \left| \sum_{n=1}^L \alpha_n e_p(an^* m^*) \right|.$$

Применяя второе утверждение леммы, завершаем доказательство.

3. Доказательство теоремы 1.1. Достаточно доказать, что

$$\left| \sum_{n \leq N} \Lambda(n) e_p(an^*) \right| \lesssim N^{15/16} + N^{2/3} p^{1/4},$$

так как утверждение теоремы будет следовать из формулы частного суммирования ($\Lambda(n)$ обозначает функцию Мангольда).

Можем предположить, что $N > p^{3/4}$. Из решета Виноградова в форме Вона (см. [11; гл. 24]) имеем

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

где

$$W_1 = \left| \sum_{n \leq U} \Lambda(n) e_p(an^*) \right|, \quad W_2 = \sum_{n \leq UV} \left| \sum_{m \leq N/n} e_p(an^* m^*) \right|,$$

$$W_3 = \sum_{n \leq V} \left| \sum_{m \leq N/n} (\log m) e_p(an^* m^*) \right|, \quad W_4 = \sum_{U < n \leq N/V} \Lambda(n) \left| \sum_{V < m \leq N/n} \beta_m e_p(an^* m^*) \right|.$$

Здесь $U \geq 2$, $V \geq 2$ являются параметрами с условием $UV \leq N$,

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

Мы берем $U = V = p^{1/3}$. Сумма в W_1 оценивается тривиально:

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

Чтобы оценить W_4 , разобьем интервал суммирования по переменной n на двоичные интервалы вида $(X, 2X]$ и получим, что для некоторого $p^{1/3} < L \leq N/p^{1/3}$

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

Применение первого утверждения леммы 2.4 дает

$$W_4 \lesssim N^{15/16}.$$

Для оценки W_3 мы снова разобьем интервал суммирования по переменной n на двоичные интервалы и получим, что для некоторого $L < p^{1/3}$

$$W_3 \lesssim \sum_{L \leq n < 2L} \left| \sum_{m \leq N/n} (\log m) e_p(an^* m^*) \right|.$$

Применяя к внутренней сумме формулу частного суммирования и лемму 2.2, получим

$$W_3 \lesssim \sum_{L \leq n < 2L} p^{1/2} \lesssim L p^{1/2}.$$

С другой стороны, так как $L < p^{1/3}$, третье утверждение леммы 2.3 влечет

$$W_3 \lesssim \left(\frac{N}{L} \right)^{3/4} L^{1/2} p^{1/4} = \frac{N^{3/4} p^{1/4}}{L^{1/4}}.$$

Последние два неравенства вместе с условием $N > p^{3/4}$ дают

$$W_3 \lesssim N^{3/5} p^{3/10} \lesssim N^{2/3} p^{1/4}.$$

Таким образом,

$$\sum_{n \leq N} \Lambda(n) e_p(an^*) \lesssim N^{2/3} p^{1/4} + N^{15/16} + W_2. \quad (3)$$

Остается доказать, что

$$W_2 := \sum_{n \leq p^{2/3}} \left| \sum_{m \leq N/n} e_p(an^*m^*) \right| \lesssim N^{15/16} + N^{2/3}p^{1/4}.$$

Для этого разобьем интервал суммирования по переменной n на двоичные интервалы и получим, что для некоторого $L \leq p^{2/3}$

$$W_2 \lesssim \sum_{L \leq n < 2L} \left| \sum_{m \leq N/n} e_p(an^*m^*) \right|.$$

Если $L < p^{1/3}$, то точно так же, как и в случае с W_3 , получим

$$W_2 \lesssim N^{3/5}p^{3/10} \lesssim N^{2/3}p^{1/4}.$$

В случае $p^{1/3} < L < Np^{-1/3}$ применим первое утверждение леммы 2.4 и получим, что

$$W_2 \lesssim N^{15/16}.$$

В случае $Np^{-1/3} < L < N^{2/3}$ применим второе утверждение леммы 2.4 и получим, что

$$W_2 \lesssim L^{3/4} \left(\frac{N}{L} \right)^{1/2} p^{1/4} = L^{1/4} N^{1/2} p^{1/4} \leq N^{2/3} p^{1/4}.$$

Наконец, если $N^{2/3} < L < p^{2/3}$, то, применяя неравенство Коши–Буняковского, получим

$$W_2^2 \lesssim L \sum_{L \leq n \leq 2L} \sum_{m_1 \leq N/n} \sum_{m_2 \leq N/n} e_p(an^*(m_1^* - m_2^*)).$$

Поменяв порядки суммирований, получим

$$W_2^2 \lesssim L \sum_{m_1 \leq N/L} \sum_{m_2 \leq N/L} \left| \sum_{L \leq n \leq \min\{2L, N/m_1, N/m_2\}} e_p(an^*(m_1^* - m_2^*)) \right|.$$

Диагональный случай $m_1 = m_2$ вносит в W_2^2 величину порядка $\lesssim LN$. Если $m_1 \neq m_2$, то к внутренней сумме применяем лемму 2.2. Следовательно,

$$W_2^2 \lesssim LN + L \left(\frac{N}{L} \right)^2 p^{1/2} = LN + \frac{N^2 p^{1/2}}{L}.$$

Так как $N^{2/3} < L < p^{2/3}$, то

$$W_2 \lesssim p^{1/3} N^{1/2} + N^{2/3} p^{1/4} \lesssim N^{2/3} p^{1/4}.$$

Таким образом, окончательно имеем

$$W_2 \lesssim N^{15/16} + N^{2/3} p^{1/4}.$$

Учитывая это неравенство в (3), завершаем доказательство теоремы.

4. Доказательство следствия 1. Так же, как и в [4], сравнение переписывается в виде

$$q_2 + q_3 - \lambda q_1^* \equiv 0 \pmod{p}.$$

Результат без труда выводится из метода решений аддитивных тернарных сравнений и теоремы 1.1.

Автор благодарит М. А. Королёва за внимательное прочтение настоящей заметки и за сообщение о работе [1].

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] А. А. Карацуба, “Суммы дробных долей специального вида функций”, *Докл. РАН*, **349**:3 (1996), 302.
- [2] J. Bourgain, “More on the sum-product phenomenon in prime fields and its applications”, *Int. J. Number Theory*, **1**:1 (2005), 1–32.
- [3] E. Fouvry, P. Michel, “Sur certaines sommes d’exponentielles sur les nombres premiers”, *Ann. Sci. École Norm. Sup. (4)*, **31**:1 (1998), 93–130.
- [4] J. B. Friedlander, P. Kurlberg, I. E. Shparlinski, “Products in residue classes”, *Math. Res. Lett.*, **15**:6 (2008), 1133–1147.
- [5] P. Erdős, A. M. Odlyzko, A. Sárközy, “On the residues of products of prime numbers”, *Period. Math. Hungar.*, **18**:3 (1987), 229–239.
- [6] А. А. Карацуба, “Дробные доли специального вида функций”, *Изв. РАН. Сер. матем.*, **59**:4 (1995), 61–80.
- [7] А. А. Карацуба, “Аналоги сумм Клоостермана”, *Изв. РАН. Сер. матем.*, **59**:5 (1995), 93–102.
- [8] М. А. Королёв, “Неполные суммы Клоостермана и их приложения”, *Изв. РАН. Сер. матем.*, **64**:6 (2000), 41–64.
- [9] И. М. Виноградов, *Основы теории чисел*, Наука, М., 1965.
- [10] D. R. Heath-Brown, “Almost-primes in arithmetic progressions and short intervals”, *Math. Proc. Cambridge Philos. Soc.*, **83**:3 (1978), 357–375.
- [11] H. Davenport, *Multiplicative Number Theory*, Grad. Texts in Math., **74**, Springer-Verlag, New York, NY, 2000.

М. З. Гараев

National Autonomous University of Mexico, Мексика
E-mail: garaev@matmor.unam.mx

Поступило
20.04.2009