Math-Net.Ru

Общероссийский математический портал

М. З. Гараев, О тригонометрической сумме Гаусса, *Матем. заметки*, 2000, том 68, выпуск 2, 173–178

DOI: <https://doi.org/10.4213/mzm935>

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: 35.173.137.237

26 апреля 2023 г., 12:28:13

УДК 511.3

О ТРИГОНОМЕТРИЧЕСКОЙ СУММЕ ГАУССА

М. З. Гараев

В работе доказывается, что аргументы суммы Гаусса для шестых степеней не являются в совокупности всюду плотным множеством. Получена также нижняя оценка для соответствующих тригонометрических сумм.

Библиография: 3 названия.

1. Введение. Пусть p – простое число, a, k – натуральные числа, $k \geq 3$, $m = [(k-1)/2]$, $a \not\equiv 0 \pmod{p}$, $p \equiv 1 \pmod{k}$. Пусть, далее g – фиксированный первообразный корень по модулю p ,

$$S(p, a, k) = \sum_{x=0}^{p-1} e^{2\pi i a x^k / p}.$$

При $r = 1, 2, \dots, m$ определим χ_r , характер по модулю p , следующим образом: для каждого неотрицательного целого числа t полагаем

$$\chi_r(g^t) = e^{2\pi i r t / k}.$$

Тогда найдутся вещественные числа $\theta_r \in [0, 1)$, $1 \leq r \leq m$, такие, что

$$\tau(\chi_r) = \sqrt{p} e^{2\pi i \theta_r},$$

где

$$\tau(\chi_r) = \sum_{x=0}^{p-1} \chi_r(x) e^{2\pi i x / p}.$$

Между числами θ_r и суммой $S(p, a, k)$ известна (см. [1]) следующая связь:

а) при $p \equiv 1 \pmod{2k}$ выполняется соотношение

$$\frac{S(p, g^t, k)}{\sqrt{p}} = \omega(-1)^t + 2 \sum_{1 \leq r \leq m} \cos\left(2\pi\left(\theta_r - \frac{rt}{k}\right)\right), \quad (1)$$

где

$$\omega = \begin{cases} 0, & \text{если } k - \text{нечетное число,} \\ 1, & \text{если } k - \text{четное число;} \end{cases}$$

б) при $p \equiv k + 1 \pmod{2k}$ выполняется соотношение

$$\frac{S(p, g^t, k)}{\sqrt{p}} = \omega(-1)^{t+2} \sum_{\substack{1 \leq r \leq m \\ r \equiv 0 \pmod{2}}} \cos\left(2\pi\left(\theta_r - \frac{rt}{k}\right)\right) + 2i \sum_{\substack{1 \leq s \leq m \\ s \equiv 1 \pmod{2}}} \sin\left(2\pi\left(\theta_s - \frac{st}{k}\right)\right), \quad (2)$$

где

$$\omega = \begin{cases} 1, & \text{если } p \equiv 1 \pmod{4}, \\ i, & \text{если } p \equiv 3 \pmod{4}. \end{cases}$$

В частности, если $k = 3$, то выполнено равенство

$$\frac{S(p, g^t, 3)}{\sqrt{p}} = 2 \cos\left(2\pi\left(\theta_1 - \frac{t}{3}\right)\right).$$

Хиз-Браун и Паттерсон [2] показали, что когда p пробегает простые числа вида $p \equiv 1 \pmod{3}$, то θ_1 будет равномерно распределена по модулю 1. Значит, $S(p, g^t, 3)/\sqrt{p}$ может сколь угодно близко приближаться к любому числу из промежутка $[-2, 2]$.

Если $k = 4$, то выполнено равенство

$$\frac{S(p, g^t, 4)}{\sqrt{p}} = \begin{cases} (-1)^t + 2 \cos\left(2\pi\left(\theta_1 - \frac{t}{4}\right)\right), & \text{если } p \equiv 1 \pmod{8}, \\ (-1)^t + 2i \sin\left(2\pi\left(\theta_1 - \frac{t}{4}\right)\right), & \text{если } p \equiv 5 \pmod{8}. \end{cases}$$

Паттерсон [3] показал, что и в этом случае θ_1 равномерно распределена по модулю 1, когда p пробегает простые числа вида $p \equiv 1 \pmod{4}$. В работе [1] отмечается, что по-видимому метод Паттерсона мог бы быть модифицирован для получения равномерного распределения θ_1 как в случае, когда p пробегает простые числа вида $p \equiv 1 \pmod{8}$, так и в случае, когда p пробегает простые числа вида $p \equiv 5 \pmod{8}$. Это дало бы ответ на вопрос о распределении значений $S(p, a, 4)/\sqrt{p}$.

Что же касается произвольного k , то Паттерсон [3] показал, что при каждом r , $1 \leq r \leq m$, θ_r равномерно распределена по модулю 1, когда p пробегает простые числа вида $p \equiv 1 \pmod{k}$.

В работе [1] было высказано предположение, что если зафиксировать k и заставить p пробегать простые числа вида $p \equiv 1 \pmod{k}$, то $\theta_1, \dots, \theta_m$ по модулю 1 будут сколь угодно близко приближаться к любой заданной конфигурации бесконечно много раз.

Но уже при $k = 6$ это оказалось не так.

Итак, пусть $k = 6$, как и выше, p – простое число, $p \equiv 1 \pmod{6}$, a – натуральное число, $a \not\equiv 0 \pmod{p}$.

Обозначим

$$S(p, a) = S(p, a, 6) = \sum_{x=0}^{p-1} e^{2\pi i a x^6/p}.$$

Перепишем соотношения (1), (2) для наших рассмотрений при $t = 0$:

$$\frac{S(p, 1)}{\sqrt{p}} = 1 + 2 \cos(2\pi\theta_1) + 2 \cos(2\pi\theta_2), \quad \text{если } p \equiv 1 \pmod{12}, \quad (3)$$

$$\frac{S(p, 1)}{\sqrt{p}} = i + 2i \sin(2\pi\theta_1) + 2 \cos(2\pi\theta_2), \quad \text{если } p \equiv 7 \pmod{12}. \quad (4)$$

ТЕОРЕМА 1. *Существует абсолютная положительная постоянная c такая, что для чисел θ_1 и θ_2 выполнена оценка*

$$\left| \theta_1 - \frac{1}{2} \right| + \left| \theta_2 - \frac{1}{2} \right| > c.$$

Мы докажем более точное соотношение:

$$\cos(2\pi\theta_1) + \cos(2\pi\theta_2) > -\frac{143}{72}.$$

ТЕОРЕМА 2. *Если $p \equiv 7 \pmod{12}$, то имеет место равенство*

$$|S(p, a)| > \frac{\sqrt{3}}{2} \sqrt{p}.$$

Из результатов работы [1], в частности, следует, что для простых p из теоремы 2 выполнено неравенство

$$|S(p, a)| \leq \sqrt{13p}.$$

Последнее неравенство можно сделать строгим. Поэтому

$$\frac{\sqrt{3}}{2} < \left| \frac{S(p, a)}{\sqrt{p}} \right| < \sqrt{13}$$

для всех простых чисел $p, p \equiv 7 \pmod{12}$.

В дальнейшем будем также пользоваться обозначением

$$S_1(p, a) = \sum_{x=0}^{p-1} e^{2\pi i a x^3/p}.$$

2. Вспомогательная лемма.

ЛЕММА. *Для всех простых p справедливо равенство*

$$S(p, a) = S_1(p, a) + \frac{(S_1(p, 4a))^2 - p \left(\frac{a}{p} \right)}{\sqrt{p}} i^{((p-1)/2)^2}, \quad (5)$$

где $\left(\frac{a}{p} \right)$ – символ Лежандра.

ДОКАЗАТЕЛЬСТВО. Заметим, что $S_1(p, a), S_1(p, 4a)$ являются действительными числами. Имеем

$$\begin{aligned} (S_1(p, 4a))^2 &= \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} e^{2\pi i 4a(x^3 - y^3)/p} = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} e^{2\pi i 4a((x+y)^3 - y^3)/p} \\ &= p + \sum_{x=1}^{p-1} \sum_{y=0}^{p-1} e^{2\pi i 4a(x^3 + 3x^2y + 3xy^2)/p} = p + \sum_{x=1}^{p-1} \sum_{y=0}^{p-1} e^{2\pi i 4ax^3(3y^2 + 3y + 1)/p} \\ &= p + \sum_{x=1}^{p-1} e^{2\pi i ax^3/p} \sum_{y=0}^{p-1} e^{2\pi i 3ax^3y^2/p}. \end{aligned}$$

Поскольку $(3a, p) = 1$, $(x, p) = 1$, то

$$\sum_{y=0}^{p-1} e^{2\pi i 3ax^3 y^2/p} = \left(\frac{3ax^3}{p}\right) \sqrt{p} \cdot i^{((p-1)/2)^2} = \left(\frac{3a}{p}\right) \left(\frac{x}{p}\right) \sqrt{p} \cdot i^{((p-1)/2)^2}.$$

Поэтому

$$\begin{aligned} (S_1(p, 4a))^2 &= p + \left(\frac{3a}{p}\right) \sqrt{p} \cdot i^{((p-1)/2)^2} \sum_{x=1}^{p-1} \left(\frac{x}{p}\right) e^{2\pi i ax^3/p} \\ &= p + \left(\frac{3a}{p}\right) \sqrt{p} \cdot i^{((p-1)/2)^2} \left(\sum_{x=0}^{p-1} \left(1 + \left(\frac{x}{p}\right)\right) e^{2\pi i ax^3/p} - \sum_{x=0}^{p-1} e^{2\pi i ax^3/p} \right) \\ &= p + \left(\frac{3a}{p}\right) \sqrt{p} \cdot i^{((p-1)/2)^2} \left(\sum_{x=0}^{p-1} e^{2\pi i ax^6/p} - \sum_{x=0}^{p-1} e^{2\pi i ax^3/p} \right). \end{aligned}$$

Учитывая, что $p \equiv 1 \pmod{6}$, $\left(\frac{3}{p}\right) = (-1)^{(p-1)/2} = (-1)^{((p-1)/2)^2}$, получим утверждение леммы.

3. Доказательство теоремы 1. Прежде всего заметим, что суммы $S_1(p, a)$ и $S_1(p, 4a)$ между собой жестко связаны. Действительно, при каждом a , $a \not\equiv 0 \pmod{p}$, сумма $S_1(p, a)$ совпадает с одной из трех сумм: $S_1(p, 1)$, $S_1(p, g)$, $S_1(p, g^2)$. Для последних же имеет место система уравнений

$$\begin{cases} S_1(p, 1) + S_1(p, g) + S_1(p, g^2) = 0, \\ (S_1(p, 1))^2 + (S_1(p, g))^2 + (S_1(p, g^2))^2 = 6p. \end{cases}$$

Отсюда получаем, что либо $S_1(p, a) = S_1(p, 4a)$, либо $(S_1(p, a))^2 + S_1(p, a) \cdot S_1(p, 4a) + (S_1(p, 4a))^2 = 3p$, в зависимости от того, является ли число 2 кубическим вычетом по модулю p или нет.

Докажем, что

$$\cos(2\pi\theta_1) + \cos(2\pi\theta_2) > -\frac{143}{72}.$$

Пусть это не так, т.е. для некоторого простого числа p выполнено неравенство

$$\cos(2\pi\theta_1) + \cos(2\pi\theta_2) \leq -\frac{143}{72}.$$

Обозначим

$$\alpha = \frac{S_1(p, 1)}{\sqrt{p}}, \quad \beta = \frac{S_1(p, 4)}{\sqrt{p}}.$$

Тогда из (5) следует, что

$$\frac{S(p, 1)}{\sqrt{p}} = \alpha + (\beta^2 - 1)i^{((p-1)/2)^2}. \quad (6)$$

В силу известных неравенств имеем $|\alpha| \leq 2$, $|\beta| \leq 2$. Кроме того, либо $\alpha = \beta$, либо $\alpha^2 + \alpha\beta + \beta^2 = 3$.

Рассмотрим две возможности:

- 1) $p \equiv 1 \pmod{12}$;
- 2) $p \equiv 7 \pmod{12}$.

В случае 1) из (3), (6) следует, что

$$\alpha + \beta^2 - 1 = 1 + 2(\cos(2\pi\theta_1) + \cos(2\pi\theta_2)).$$

С учетом предположения имеем $\alpha + \beta^2 \leq -71/36$, откуда

$$|\beta| \leq \frac{1}{6}, \quad \alpha \leq -\frac{71}{36}, \quad \alpha \neq \beta.$$

Следовательно,

$$3 = \alpha^2 + \alpha\beta + \beta^2 \geq \left(\frac{71}{36}\right)^2 - 2|\beta| > 3.$$

Противоречие.

Пусть теперь имеет место случай 2), т.е. $p \equiv 7 \pmod{12}$. Из (4), (6) имеем

$$2 \cos(2\pi\theta_2) = \alpha, \quad 1 + 2 \sin(2\pi\theta_1) = \beta^2 - 1.$$

По предположению $\cos(2\pi\theta_1) + \cos(2\pi\theta_2) \leq -143/72$, откуда следует, что

$$\cos(2\pi\theta_2) \leq -\frac{71}{72}, \quad |\sin(2\pi\theta_1)| < \frac{1}{6}, \quad \alpha \leq -\frac{71}{36}, \quad \frac{5}{3} < \beta^2 < \frac{7}{3}.$$

Поэтому $\alpha \neq \beta$. Это означает, что $\alpha^2 + \alpha\beta + \beta^2 = 3$. Следовательно, $\beta > 0$, т.е. $\sqrt{5/3} < \beta < \sqrt{7/3}$. Ввиду того, что $\beta + \alpha/2 > \sqrt{5/3} - 1 > 0$, имеем

$$3 = \alpha^2 + \alpha\beta + \beta^2 = \left(\beta + \frac{\alpha}{2}\right)^2 + \frac{3\alpha^2}{4} > \left(\sqrt{\frac{5}{3}} - 1\right)^2 + \frac{3 \cdot 71^2}{72^2} > 3.$$

Противоречие. Теорема 1 доказана.

4. Доказательство теоремы 2. По условию $p \equiv 7 \pmod{12}$. Обозначим

$$\alpha = \frac{S_1(p, a)}{\sqrt{p}}, \quad \beta = \frac{S_1(p, 4a)}{\sqrt{p}}.$$

Из (5) следует, что

$$\frac{S(p, a)}{\sqrt{p}} = \alpha + (\beta^2 - 1)i.$$

В силу того, что α, β – действительные числа, имеем

$$\left| \frac{S(p, a)}{\sqrt{p}} \right| = \sqrt{\alpha^2 + (\beta^2 - 1)^2}.$$

Если $\alpha = \beta$, то

$$\alpha^2 + (\beta^2 - 1)^2 = \left(\alpha^2 - \frac{1}{2}\right)^2 + \frac{3}{4} \geq \frac{3}{4}.$$

При этом $\alpha^2 \neq 1/2$. Действительно, пусть

$$\gamma = \frac{S(p, ag)}{\sqrt{p}}, \quad \theta = \frac{S(p, ag^2)}{\sqrt{p}},$$

а N – число решений сравнения $u^3 + v^3 + w^3 \equiv 0 \pmod{p}$. Тогда

$$\alpha + \gamma + \theta = 0, \quad \alpha^2 + \gamma^2 + \theta^2 = 6,$$

$$pN = \sum_{b=0}^{p-1} \left(\sum_{x=0}^{p-1} e^{2\pi i b x^3/p} \right)^3 = p^3 + \frac{p-1}{3}(\alpha^3 + \gamma^3 + \theta^3)p^{3/2}.$$

Отсюда следует, что величина $3\alpha(3 - \alpha^2)\sqrt{p} = 3\alpha\gamma(\alpha + \gamma)\sqrt{p}$ является рациональным числом. Следовательно, $\alpha^2 \neq 1/2$.

Если же $\alpha \neq \beta$, то

$$3 = \alpha^2 + \alpha\beta + \beta^2 < \frac{3}{2}(\alpha^2 + \beta^2),$$

откуда

$$\alpha^2 + (\beta^2 - 1)^2 > 2 - \beta^2 + (\beta^2 - 1)^2 = \left(\beta^2 - \frac{3}{2}\right)^2 + \frac{3}{4} \geq \frac{3}{4}.$$

Теорема 2 доказана.

В заключение выражаю глубокую благодарность профессору В. Н. Чубарикову за полезные советы.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Montgomery H. L., Vaughan R. C., Wooley T. D. Some remarks on Gauss sums associated with k th powers // Math. Proc. Camb. Soc. 1995. V. 118. № 21. P. 21–33.
- [2] Heath-Brown D. R., Patterson S. J. The distribution of Kummer sums at prime arguments // J. Reine Angew. Math. 1979. V. 310. P. 111–130.
- [3] Patterson S. J. The distribution of general Gauss sums and similar arithmetic functions at prime arguments // Proc. London Math. Soc. (3). 1987. V. 54. P. 193–215.

Московский государственный университет им. М. В. Ломоносова

Поступило
09.12.1999