Д. А. Митькин, О величине сумм характеров от многочленов,
Матем. заметки, 1982, том 31, выпуск 6, 827–835

МАТЕМАТИЧЕСКИЕ ЗАМЕТКИ
т. 31, № 6 (1982)

О ВЕЛИЧИНЕ СУММ ХАРАКТЕРОВ ОТ МНОГОЧЛЕНОВ

Д. А. Митькин

Пусть $n > 2$ — целое, $p > n$ — простое, $f(x)$ — многочлен степени n с коэффициентами из поля Z_p вычетов $\bmod p$, χ — неглавный характер мультипликативной или аддитивной группы поля Z_p. Наилучшие оценки сверху для полных сумм характеров от многочленов были получены Г. Хассе [1] и А. Вейлем [2, 3]:

$$\left|\sum_{x=1}^{p} \chi(f(x))\right| \leqslant (n-1)\sqrt{p}, \qquad n < \sqrt{p}.$$

Для сумм символов Лежандра нетривиальные оценки получены в несколько большем интервале $n < c\sqrt{p}$, $c > 1$ (см. [4 — 6]), а в случае сумм характеров от многочленов специального вида А. А. Карацубе [7] удалось получить нетривиальные оценки сверху при всех $n < p$. В указанной работе А. А. Карацубы поставлена задача о неулучшаемых оценках сверху и доказано, что при n порядка $p/\ln p$ тривиальная оценка сверху не может быть улучшена для сумм с аддитивным характером. В дальнейшем результаты в этой задаче при растущем n были получены для сумм символов Лежандра (см. [8, 9]), но понизить границу для n, при которых тривиальная верхняя оценка неулучшаема, не удалось. При фиксированном n задача тесно связана с распределением простых идеальных чисел алгебраических числовых полей. Неулучшаемость оценки Г. Хассе для сумм символов Лежандра от многочленов третьей степени следует из результатов Гекке (см. [10, 11]) о распределении простых идеальных чисел мнимого квадратичного поля в секторах. Неулучшаемость оценки

А. Вейля для сумм аддитивных характеров от многочленов четвертой степени была установлена автором [12] при помощи результатов о распределении простых идеальных чисел мнимого квадратичного поля в секторах и арифметических прогрессиях. Следствием работы [12] явилась следующая схема подхода к доказательству неулучшаемости оценок А. Вейля при произвольном фиксированном n: основываясь на таких суммах характеров от многочленов, которые представляются в виде суммы гауссовых сумм (гауссовы суммы являются делителями p в круговом расширении кольца целых чисел), применить результаты о распределении простых идеальных чисел круговых полей. Воспользовавшись результатами И. П. Кубилюса [13] о распределении простых идеальных чисел алгебраического числового поля и их сопряженных в секторах и прогрессиях, являющимися обобщением результатов Гекке, Л. А. Книжнерман и В. З. Соколинский [14] провели в соответствии с предложенной схемой доказательство неулучшаемости оценок А. Вейля для сумм символов Лежандра при произвольном n и для сумм аддитивных характеров при бесквадратном n.

В настоящей работе доказательство неулучшаемости оценок А. Вейля дано в общем случае, т. е. для сумм аддитивных и мультипликативных (фиксированного показателя) характеров от многочленов произвольной фиксированной степени $n > 2$.

Далее всюду будем полагать, что $m \geqslant 3$ — целое, K — поле, полученное присоединением примитивного корня степени m из 1 к полю рациональных чисел $\mathbf{Q}$, p — простое число с условием $p \equiv 1 \pmod{2m}$. Известно, что $[K\colon \mathbf{Q}] = \varphi(m)$, где $\varphi(m)$ — функция Эйлера (см. [15]).

ЛЕММА 1. *Пусть* $\delta > 0$. *Существует бесконечное множество попарно не ассоциированных простых элементов* ρ *поля* K *с простой нормой таких, что* $\rho \equiv 1 \pmod{2m}$ *и для всех сопряженных к* ρ *выполняется неравенство*

$$|\arg \rho^{(j)}| \leqslant \delta \quad (j = 1, \ldots, \varphi(m)).$$

Лемма является очевидным следствием теорем И. П. Кубилюса [13].

ЛЕММА 2. *Пусть* q — *простое*, ξ — *корень из* 1, ζ_q — *примитивный корень степени* q *из* 1, F — *некоторое конечное расширение поля* $\mathbf{Q}$, *содержащее* ξ *и* ζ_q. *Пусть*

в поле F имеет место сравнение

$$1 - \xi \equiv 0 \pmod{(1 - \zeta_q)\,\lambda}, \tag{1}$$

где λ — целое число поля F, не являющееся единицей. Тогда $\xi = 1$.

Доказательство. Пусть ξ является примитивным корнем из 1 степени $l > 1$. Вычислим норму $1 - \xi$ из $\mathbf{Q}(\xi)$ в $\mathbf{Q}$.

Имеем

$$N_{\mathbf{Q}(\xi)/\mathbf{Q}}(1 - \xi) = f_l(1),$$

где $f_l(x)$ — l-й круговой многочлен (см. [15]). Воспользовавшись формулой

$$f_l(x) = \frac{x^l - 1}{\prod_{d \mid l,\, d < l} f_d(x)}$$

найдем, что

$$f_l(1) = \begin{cases} q_1, \text{ если } l = q_1^k, \text{ где } k \geqslant 1,\ q_1 \text{ — простое;} \\ 1 \text{ в противном случае.} \end{cases}$$

Из сравнения (1) теперь следует, что $l = q_1^k$, $k \geqslant 1$, где q_1 — простое. Возьмем норму из F в $\mathbf{Q}$ от обеих частей сравнения (1). Тогда получим

$$q_1^{[F:\mathbf{Q}(\xi)]} = \mu q^{[F:\mathbf{Q}(\zeta_q)]}\, N_{F/\mathbf{Q}}(\lambda), \tag{2}$$

где μ — целое. Отсюда следует, что $q_1 = q$. Так как теперь

$$[F\colon \mathbf{Q}(\xi)] \leqslant [F\colon \mathbf{Q}(\zeta_q)]$$

и

$$|\, N_{F/\mathbf{Q}}(\lambda)\,| > 1,$$

то равенство (2) невозможно. Следовательно, $\xi = 1$. Лемма доказана.

ЛЕММА 3. *Пусть χ и ψ — характеры* mod p, *величина $\pi(\chi, \psi)$ определена равенством*

$$\pi(\chi, \psi) = \sum_{x=1}^{p} \chi(x)\,\psi(1 - x).$$

Допустим, что для любых характеров χ, ψ показателя m выполнено сравнение

$$\pi(\chi, \psi) \equiv \varepsilon(\chi, \psi) \pmod{2m},$$

где $\varepsilon(\chi, \psi)$ — корень из 1. Тогда $\varepsilon(\chi, \psi) = -1$ для характеров показателя m.

Доказательство. Заметим, что из сравнения $\pi(\chi, \psi) \equiv -1 \pmod{2m}$ следует, что $\varepsilon(\chi, \psi) = -1$. Действительно, в этом случае $\varepsilon(\chi, \psi) \equiv -1 \pmod{2m}$ и так как примитивный корень из 1 степени 2 равен -1, то из леммы 2 при $q = 2$ получим, что $\varepsilon(\chi, \psi) = -1$. Каждый характер показателя m представляется единственным образом в виде произведения характеров, показатели которых взаимно просты и являются степенями простых чисел из канонического разложения m на простые множители. Доказательство леммы будем вести индукцией по суммарному числу ν таких компонент в χ и ψ. Пусть $\nu = 0$. Это соответствует случаю, когда χ и ψ — главные характеры. В этом случае

$$\pi(\chi, \psi) = p - 2 \equiv -1 \pmod{2m}$$

и, следовательно, $\varepsilon(\chi, \psi) = -1$. При $\nu = 1$ или когда только один из характеров χ или ψ главный, имеет равенство $\pi(\chi, \psi) = -1$ и, значит, $\varepsilon(\chi, \psi) = -1$.

Допустим, что равенство $\varepsilon(\chi, \psi) = -1$ доказано для всех χ, ψ показателя m с числом компонент ν. Докажем его для характеров χ', ψ', у которых на одну компоненту больше. Мы можем считать, что χ' и ψ' — не главные характеры. Выделим из ψ' компоненту ψ_1, соответствующую показателю $q_1^{k_1}$, $k_1 \geqslant 1$. Пусть одна из компонент χ' соответствует показателю q^k, $k \geqslant 1$, ζ_q — примитивный корень степени q из 1, ξ — примитивный корень степени $q_1^{k_1}$ из 1. Число $1 - \xi$ не является единицей. Обозначим его λ. При $x = 1, \ldots, p$ имеем

$$\psi'(1 - x) - \psi'\psi_1^{-1}(1 - x) \equiv 0 \pmod{\lambda}. \qquad (3)$$

В силу предположения индукции выполняется сравнение

$$\pi(\chi'\chi'', \psi'\psi_1^{-1}) = -1 \pmod{2m}, \qquad (4)$$

где χ'' — произвольный характер показателя q^k. Пусть χ_k — первообразный характер показателя q^k,

$$\chi_j = \chi_k^{q^{k-j}}; \quad j = 1, \ldots, k - 1.$$

Так как (см. [16])

$$q \equiv 0 \pmod{(1 - \zeta_q)^{q-1}},$$

и

$$q_1 \equiv 0 \pmod{\lambda^{\varphi(q_1^{k_1})}},$$

то выполняется сравнение

$$2m \equiv 0 \pmod{q^{k-1}(1-\zeta_q)\lambda}. \tag{5}$$

Из (3), (4) и (5) выводим

$$\varepsilon(\chi'\chi'', \psi') - \varepsilon(\chi'\chi''\chi_1, \psi') \equiv \pi(\chi'\chi'', \psi') - \pi(\chi'\chi''\chi_1, \psi') \equiv$$
$$\equiv \sum_{x=1}^{p} \chi'\chi''(x)(1-\chi_1(x))(\psi'(1-x) - \psi'\psi_1^{-1}(1-x)) \equiv$$
$$\equiv 0 \pmod{(1-\zeta_q)\lambda}.$$

Воспользовавшись леммой 2, получим, что

$$\varepsilon(\chi'\chi'', \psi') = \varepsilon(\chi'\chi''\chi_1, \psi').$$

Так как χ'' — произвольный характер показателя q^k, то мы получаем серию равенств

$$\varepsilon(\chi'\chi'', \psi') = \varepsilon(\chi'\chi''\chi_1^i, \psi'); \quad i = 1, \ldots, q. \tag{6}$$

Введем при $k > 1$ следующие функции

$$\gamma_j(x) = \begin{cases} q^j, & \text{если } x \equiv x_1^{q^j} \pmod{p},\ x \not\equiv 0 \pmod{p}, \\ 0 & \text{в остальных случаях} \end{cases}$$
$$(j = 1, \ldots, k-1).$$

Их легко выразить через характеры показателя q^k:

$$\gamma_j(x) = \sum_{i=1}^{q^j} \chi_j^i(x); \quad j = 1, \ldots, k-1. \tag{7}$$

Допустим теперь, что мы доказали серию равенств

$$\varepsilon(\chi'\chi'', \psi') = \varepsilon(\chi'\chi''\chi_j^i, \psi'); \quad i = 1, \ldots, q^j, \tag{8}$$

где χ'' — произвольный характер показателя q^k. Выведем аналогичное равенство для $j+1$, если $j < k$. Из соотношений (3), (4), (5), (7) и (8) получаем

$$q^j(\varepsilon(\chi'\chi'', \psi') - \varepsilon(\chi'\chi''\chi_{j+1}, \psi')) \equiv$$
$$\equiv \sum_{i=1}^{q^j} (\pi(\chi'\chi''\chi_j^i, \psi') - \pi(\chi'\chi''\chi_{j+1}\chi_j^i, \psi')) \equiv$$
$$\equiv \sum_{x=1}^{p} \chi'\chi''(x)(1-\chi_{j+1}(x))\gamma_j(x)(\psi'(1-x) - \psi'\psi_1^{-1}(1-x)) \equiv$$
$$\equiv q^j \sum_{x_1} \chi'\chi''(x_1^{q^j})(1-\chi_1(x_1))(\psi'(1-x_1^{q^j}) - \psi'\psi_1^{-1}(1-x_1^{q^j})) \equiv$$
$$\equiv 0 \pmod{q^j(1-\zeta_q)\lambda}.$$

Следовательно,

$$\varepsilon(\chi'\chi'', \psi') - \varepsilon(\chi'\chi''\chi_{j+1}, \psi') \equiv 0 \pmod{(1-\zeta_q)\lambda},$$

и в силу леммы 2

$$\varepsilon(\chi'\chi'', \psi') = \varepsilon(\chi'\chi''\chi_{j+1}, \psi').$$

Так как χ'' — произвольный характер показателя q^k, то выполняется серия равенств

$$\varepsilon(\chi'\chi'', \psi') = \varepsilon(\chi'\chi''\chi_{j+1}^i, \psi'); \quad i = 1, \ldots, q^{j+1}.$$

Тем самым по индукции мы доказали, что справедливо равенство

$$\varepsilon(\chi'\chi'', \psi') = \varepsilon(\chi'\chi''\chi_k^i, \psi'); \quad i = 1, \ldots, q^k,$$

и, в частности,

$$\varepsilon(\chi', \psi') = \varepsilon(\chi'\chi_k^i, \psi'); \quad i = 1, \ldots, q^k.$$

Так как χ_k^i пробегает все характеры показателя q^k, то среди характеров $\chi'\chi_k^i$ найдется характер, содержащий на одну компоненту меньше, чем χ' и, следовательно, в силу предположения индукции мы получаем равенство $\varepsilon(\chi', \psi') = -1$. Из соображений симметрии, $\pi(\chi', \psi') = \pi(\psi', \chi')$, нам достаточно ограничиться при доказательстве шага индукции увеличением числа компонент по первому характеру. Лемма доказана.

ТЕОРЕМА. Пусть $\eta > 0$. *Существует бесконечное множество простых чисел* p, $p \equiv 1 \pmod{2m}$ *таких, что при любом* $n \backslash m$, $n > 2$ *справедливы неравенства*:

1° *Для любого неглавного характера* ψ *показателя* m

$$\left|\sum_{x=1}^{p} \psi(x^n - 1)\right| \geqslant \begin{cases} (n-2-\eta)\sqrt{p}, & \text{если } \psi^n \text{ — главный характер;} \\ (n-1-\eta)\sqrt{p} & \text{в противном случае.} \end{cases}$$

2° *При некотором* $\lambda_n \not\equiv 0 \pmod{p}$

$$\left|\sum_{x=1}^{p} \exp(2\pi i \lambda_n x^n / p)\right| \geqslant (n-1-\eta)\sqrt{p}.$$

Доказательство. Пусть $p \equiv 1 \pmod{2m}$, χ — первообразный характер $\bmod p$ показателя n. Так как $n \backslash m$, то χ является характером $\bmod p$ показателя m. Суммы, указанные в формулировке теоремы, выразим через величины $\pi(\chi, \psi)$, определенные в лемме 3. Учи-

тывая, что

$$\chi(-1) = 1, \quad \psi(-1) = 1,$$

имеем следующие соотношения (см. [11]):

$$\sum_{x=1}^{p} \psi(x^n - 1) = \sum_{i=1}^{n-1} \pi(\chi^i, \psi), \tag{9}$$

$$\sum_{x=1}^{p} \exp(2\pi i \lambda_n x^n/p) = \sum_{i=1}^{n-1} S_i(\lambda_n), \tag{10}$$

где

$$S_i(\lambda_n) = \sum_{x=1}^{p} \chi^i(x) \exp(2\pi i \lambda_n x/p),$$

$$S_1(\lambda_n) = \chi^{-1}(\lambda_n) S_1(1), \tag{11}$$

$$S_1^n(\lambda_n) = p\pi(\chi, \chi) \ldots \pi(\chi, \chi^{n-2}), \tag{12}$$

$$S_i(\lambda_n) = \frac{S_1^i(\lambda_n)}{\pi(\chi, \chi) \ldots \pi(\chi, \chi^{i-1})}, \quad i = 1, \ldots, n-1; \tag{13}$$

$$\begin{cases} |\pi(\chi, \psi)| = \sqrt{p}, \text{ если } \psi \neq \chi^{-1}, \\ \pi(\chi, \chi^{-1}) = -1. \end{cases} \tag{14}$$

Положим $\delta_1 = \eta/2m^2$. Допустим, что для любых характеров χ_1, ψ_1 показателя m, $\psi_1 = \chi_1^{-1}$, выполняется неравенство

$$|\arg(-\pi(\chi_1, \psi_1))| \leqslant \delta_1. \tag{15}$$

Тогда из (9) и (14) следует первый пункт теоремы. Из (12) выводим, что при некотором целом k

$$|\arg(-S_1(1)) - 2\pi k/n| \leqslant \delta_1.$$

Выбрав λ_n так, чтобы $\arg \chi(\lambda_n) = 2\pi k/n$, из (11), (13) и (14) получим, что $|S_i(\lambda_n)| = \sqrt{p}$ и

$$|\arg(-S_i(\lambda_n))| < 2m\delta_1; \quad i = 1, \ldots, n-1.$$

С помощью равенства (10) теперь получаем 2°. Для доказательства теоремы нам осталось показать, что неравенство (15) имеет место для бесконечного множества простых p, $p \equiv 1 \pmod{2m}$.

В силу леммы 1 существует бесконечное множество попарно не ассоциированных простых элементов ρ поля K с простой нормой таких, что $\rho \equiv 1 \pmod{2m}$ и для всех сопряженных к ρ выполняется неравенство

$$|\arg \rho^{(j)}| < \delta; \quad j = 1, \ldots, \varphi(m) \tag{16}$$

с $\delta = \delta_1/m$. Пусть p — норма ρ из K в $\mathbf{Q}$. Тогда, очевидно, таких p различных бесконечное множество. Из условия $\rho \equiv 1 \pmod{2m}$ вытекает аналогичное сравнение для сопряженных к ρ, а так как

$$p = \rho^{(1)} \ldots \rho^{(\varphi(m))},$$

то $p \equiv 1 \pmod{2m}$. Из равенства $\pi(\chi_1, \psi_1)\,\overline{\pi(\chi_1, \psi_1)} = p$ где $\psi_1 \neq \chi_1^{-1}$, в силу однозначности, с точностью до единиц поля K, разложения на простые идеальные множители получим, что

$$\pi(\chi_1, \psi_1) = \varepsilon(\chi_1, \psi_1) \cdot \rho^{(i_1)} \ldots \rho^{(i_{\varphi(m)/2})}, \qquad (17)$$

где $\varepsilon(\chi_1, \psi_1)$ — единица, причем $|\varepsilon(\chi_1, \psi_1)| = 1$. Аналогичные равенства имеют место для сопряженных к $\pi(\chi_1, \psi_1)$. Следовательно,

$$|\varepsilon^{(j)}(\chi_1, \psi_1)| = 1; \quad j = 1, \ldots, \varphi(m).$$

Из известной теоремы (см. [17]) следует теперь, что $\varepsilon(\chi_1, \psi_1)$ — корень из 1. Перейдя к сравнениям по модулю $2m$ в равенстве (17), получим, что $\pi(\chi_1, \psi_1) \equiv \varepsilon(\chi_1, \psi_1) \pmod{2m}$ для всех характеров χ_1, ψ_1 показателя m. Согласно лемме 3 $\varepsilon(\chi_1, \psi_1)$ должно равняться -1. Подставив это значение в (17) и применив неравенство (16), получим неравенство (15). Теорема доказана.

Московское научно-производственное объединение по механизации и автоматизации производства

Поступило 8.VIII.1980

ЦИТИРОВАННАЯ ЛИТЕРАТУРА

[1] Hasse H., Abstrakte Begründung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern, Abh. Math. Sem. Hamburg, 10 (1934), 325—348.
[2] Weil A., Sur les courbes algebriques et les variétés qui s'en deduisent, Publ. Inst. Math. Strasbourg, 1041 (1948), 1—85.
[3] Weil A., On some exponential sums, Proc. Nat. Acad. Sci. USA, 34, № 5 (1948), 204—207.
[4] Коробов Н. М., Оценка суммы символов Лежандра, Докл. АН СССР, 196, № 4 (1971), 764—767.
[5] Митькин Д. А., Оценка суммы символов Лежандра от многочленов четной степени, Матем. заметки, 14, вып. 1 (1973), 73—81.
[6] Stark H. M., On the Riemann hypothesis in hyperelliptic function fields, Proc. of symposia in pure mathematics, 24 (1973), 285—302.

[7] Карацуба А. А., Об оценках полных тригонометрических сумм, Матем. заметки, 1, вып. 2 (1967), 199—208.
[8] Карацуба А. А., Об оценках снизу сумм характеров от многочленов, Матем. заметки, 14, вып. 1 (1973), 67—72.
[9] Митькин Д. А., Об оценках снизу сумм символов Лежандра и рациональных тригонометрических сумм, Успехи матем. наук, 30 (1975), 214.
[10] Hecke E., Eine neue Art von Zetafunktion und ihre Beziechungen zur Verteilung der Primzahlen, Math. Z., 6 (1920), 11—51.
[11] Хассе Г., Лекции по теории чисел, М., ИЛ, 1953.
[12] Митькин Д. А., Об оценках снизу рациональных тригонометрических сумм 4-й степени, Тезисы докладов и сообщений Всесоюзной школы по теории чисел, Душанбе, 1977, 89—90.
[13] Кубилюс Й. П., О некоторых задачах геометрии простых чисел, Матем. сб., 31 (73), № 3 (1952), 507—542.
[14] Книжнерман Л. А., Соколинский В. З., О неулучшаемости оценок А. Вейля для рациональных тригонометрических сумм и сумм символов Лежандра, М., Деп. ВИНИТИ, № 2152 от 29.V.1979.
[15] Ленг С., Алгебра, М., «Мир», 1968.
[16] Ленг С., Алгебраические числа, М., «Мир», 1966.
[17] Гекке Э., Лекции по теории алгебраических чисел, М.— Л., ГИТТЛ, 1940.