Math-Net.Ru

Общероссийский математический портал

Е. А. Гречников, Оценка суммы символов Лежандра,
Матем. заметки, 2010, том 88, выпуск 6, 859–866

DOI: <https://doi.org/10.4213/mzm8562>

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: 54.197.130.99

26 апреля 2023 г., 14:06:03

Оценка суммы символов Лежандра

Е. А. Гречников

Для суммы символов Лежандра S от многочлена нечетной степени $n \geq 3$ по простому модулю $p \geq 3$ известны оценка Вейля $|S| \leq (n-1)\sqrt{p}$ и оценка Коробова

$$|S| \leq (n-1)\sqrt{p - \frac{(n-3)(n-4)}{4}} \quad \text{при } p \geq \frac{n^2+9}{2}.$$

В этой работе доказывается несколько более сильная оценка, а именно

$$|S| < (n-1)\sqrt{p - \frac{(n-3)(n+1)}{4}}.$$

Библиография: 4 названия.

Пусть $n \geq 3$ – нечетное, p – нечетное простое, $f(x) \in \mathbb{F}_p[x]$ – многочлен степени n . Определим сумму символов Лежандра от многочлена f формулой

$$S(f) = \sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right).$$

Согласно [1], [2] выполнена оценка Вейля

$$|S(f)| \leq (n-1)\sqrt{p}.$$

Элементарное доказательство этой оценки получил Коробов, доказав в работе [3] даже несколько более сильное утверждение: при $p \geq (n^2+9)/2$

$$|S(f)| \leq (n-1)\sqrt{p - \frac{(n-3)(n-4)}{4}}.$$

В этой работе доказывается еще несколько более сильная оценка, сходная с оценкой Коробова.

ТЕОРЕМА. При нечетном $n \geq 3$, простом $p \geq (n^2-1)/2$ и многочлене $f \in \mathbb{F}_p[x]$ степени n выполнено неравенство

$$|S(f)| < (n-1)\sqrt{p - \frac{(n-3)(n+1)}{4}}.$$

ДОКАЗАТЕЛЬСТВО. Введем следующие обозначения:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0, \quad a_i \in \mathbb{F}_p, \quad a_n \neq 0, \\ r = \frac{n(p+1)}{2}, \quad F(x) = f(x)^{(p+1)/2}, \quad H(x) = x^p - x.$$

Нам понадобится информация о производных многочлена F . Применим формулу для производной степени

$$(f^\tau)^{(\nu)} = \nu! \sum_{\substack{n_1 + \dots + n_\tau = \nu, \\ n_j \geq 0}} \frac{f^{(n_1)} \dots f^{(n_\tau)}}{n_1! \dots n_\tau!}$$

к $\tau = (p+1)/2$, $\nu \leq (p+1)/2$ (так что $\nu < p$): в каждом слагаемом числитель делится на $f^{(p+1)/2-\nu}$, следовательно,

$$\frac{1}{\nu!} F^{(\nu)} = f^{(p+1)/2-\nu} B_\nu, \quad (1)$$

где $B_\nu = B_\nu(x)$ – некоторые многочлены над $\mathbb{F}_p$. Здесь и далее при выписывании многочлена многоточием будем обозначать члены младших степеней по сравнению с уже выписанными. Поскольку

$$f(x) = a_n x^n + \dots,$$

то

$$F(x) = (a_n x^n)^{(p+1)/2} + \dots, \quad \frac{1}{\nu!} F^{(\nu)}(x) = a_n^{(p+1)/2} C_r^\nu x^{n(p+1)/2-\nu} + \dots,$$

так что

$$B_\nu(x) = C_r^\nu a_n^\nu x^{(n-1)\nu} + \dots. \quad (2)$$

Пусть $s \geq 0$ и $0 \leq k \leq (p-2s+1)/4$ – некоторые параметры, значения которых будут определены позднее. Положим

$$\Delta = \begin{vmatrix} B_{s+1} & \dots & B_{s+k} \\ \vdots & \ddots & \vdots \\ B_{s+k} & \dots & B_{s+2k-1} \end{vmatrix}$$

(получающийся при $k=0$ определитель размера 0 полагаем равным 1 – это согласуется с формулой разложения определителя по строке или столбцу) и при $1 \leq j \leq k$

$$\Delta_j = \begin{vmatrix} B_{s+1} & \dots & B_{s+j-1} & B_{s+k+1} & B_{s+j+1} & \dots & B_{s+k} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ B_{s+k} & \dots & B_{s+k+j-2} & B_{s+2k} & B_{s+k+j} & \dots & B_{s+2k-1} \end{vmatrix},$$

что после перестановки столбцов можно записать как

$$\Delta_j = (-1)^{k-j} \begin{vmatrix} B_{s+1} & \dots & B_{s+j-1} & B_{s+j+1} & \dots & B_{s+k} & B_{s+k+1} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots & \vdots \\ B_{s+k} & \dots & B_{s+k+j-2} & B_{s+k+j} & \dots & B_{s+2k-1} & B_{s+2k} \end{vmatrix}.$$

Положим $\Delta_{k+1} = -\Delta$. Введем при $0 \leq j \leq k$ многочлены

$$\varphi_j = f^j \Delta_{j+1}.$$

Тогда при $s+1 \leq \nu \leq s+k$ согласно (1) и тому, что определитель с двумя совпадающими строками равен нулю, получаем

$$\begin{aligned} \sum_{j=0}^k \frac{F^{(\nu+j)}}{(\nu+j)!} \varphi_j &= f^{(p+1)/2-\nu} \sum_{j=0}^k B_{\nu+j} \Delta_{j+1} \\ &= f^{(p+1)/2-\nu} (-1)^{k-1} \begin{vmatrix} B_\nu & B_{\nu+1} & \dots & B_{\nu+k} \\ B_{s+1} & B_{s+2} & \dots & B_{s+k+1} \\ \vdots & \vdots & \ddots & \vdots \\ B_{s+k} & B_{s+k+1} & \dots & B_{s+2k} \end{vmatrix} = 0. \end{aligned} \quad (3)$$

Для дальнейшего нам понадобятся две леммы.

ЛЕММА 1. Пусть $s \geq 0$, $0 \leq k \leq (p-2s+1)/4$, $k < (p-n)/2$. Тогда

$$D_k(s) = \begin{vmatrix} C_r^s & C_r^{s+1} & \dots & C_r^{s+k} \\ C_r^{s+1} & C_r^{s+2} & \dots & C_r^{s+k+1} \\ \vdots & \vdots & \ddots & \vdots \\ C_r^{s+k} & C_r^{s+k+1} & \dots & C_r^{s+2k} \end{vmatrix} \not\equiv 0 \pmod{p}.$$

ДОКАЗАТЕЛЬСТВО. Прибавим в $D_k(s)$ каждый последующий столбец к предыдущему:

$$D_k(s) = \begin{vmatrix} C_{r+1}^{s+1} & C_{r+1}^{s+2} & \dots & C_{r+1}^{s+k} & C_r^{s+k} \\ C_{r+1}^{s+2} & C_{r+1}^{s+3} & \dots & C_{r+1}^{s+k+1} & C_r^{s+k+1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ C_{r+1}^{s+k+1} & C_{r+1}^{s+k+2} & \dots & C_{r+1}^{s+2k} & C_r^{s+2k} \end{vmatrix}.$$

Теперь повторим это действие со всеми столбцами, кроме последнего, затем еще раз со всеми столбцами, кроме двух последних, и так далее. В результате находим

$$D_k(s) = \begin{vmatrix} C_{r+k}^{s+k} & \dots & C_r^{s+k} \\ \vdots & \ddots & \vdots \\ C_{r+k}^{s+2k} & \dots & C_r^{s+2k} \end{vmatrix}. \quad (4)$$

Поскольку $r-2k \geq s$ и

$$C_{r+k-j}^{s+k+i} = \frac{(r+k-j)!}{(s+k+i)!(r-s-i-j)!} = C_{r-s-i}^j \frac{(r+k-j)!j!}{(s+k+i)!(r-s-i)!}, \quad 0 \leq i, j \leq k,$$

то из всех элементов $(i+1)$ -й строки правой части (4) можно вынести множитель $(s+k+i)!(r-s-i)!$, а из всех элементов $(j+1)$ -го столбца – множитель $(r+k-j)!j!$, в результате чего останется

$$D_k(s) = \begin{vmatrix} C_{r-s}^0 & \dots & C_{r-s}^k \\ \vdots & \ddots & \vdots \\ C_{r-s-k}^0 & \dots & C_{r-s-k}^k \end{vmatrix} \prod_{\nu=0}^k \frac{(r+k-\nu)! \nu!}{(s+k+\nu)!(r-s-\nu)!}.$$

Для подсчета получившегося определителя вычтем каждую последующую строку из предыдущей и повторим эти действия со всеми строками кроме последней, затем кроме двух последних и т.д. После k шагов находим, что

$$\begin{vmatrix}
 C_{r-s}^0 & C_{r-s}^1 & \cdots & C_{r-s}^{k-1} & C_{r-s}^k \\
 C_{r-s-1}^0 & C_{r-s-1}^1 & \cdots & C_{r-s-1}^{k-1} & C_{r-s-1}^k \\
 \vdots & \vdots & \ddots & \vdots & \vdots \\
 C_{r-s-k+1}^0 & C_{r-s-k+1}^1 & \cdots & C_{r-s-k+1}^{k-1} & C_{r-s-k+1}^k \\
 C_{r-s-k}^0 & C_{r-s-k}^1 & \cdots & C_{r-s-k}^{k-1} & C_{r-s-k}^k
 \end{vmatrix}
 =
 \begin{vmatrix}
 0 & 0 & \cdots & 0 & 1 \\
 0 & 0 & \cdots & 1 & C_{r-s-k}^1 \\
 \vdots & \vdots & \ddots & \vdots & \vdots \\
 0 & 1 & \cdots & C_{r-s-k}^{k-2} & C_{r-s-k}^{k-1} \\
 1 & C_{r-s-k}^1 & \cdots & C_{r-s-k}^{k-1} & C_{r-s-k}^k
 \end{vmatrix}
 = (-1)^{k(k+1)/2}.$$

Следовательно,

$$D_k(s) = (-1)^{k(k+1)/2} \prod_{\nu=0}^k \frac{(r-s-\nu+1) \cdots (r+k-\nu)}{(\nu+1) \cdots (s+k+\nu)}.$$

Осталось заметить, что при указанных в условии ограничениях и при $0 \leq \nu \leq k$

$$\frac{(n-1)p}{2} < \frac{(n-1)(p+1)}{2} < r-s-\nu+1, \quad r+k-\nu < \frac{n(p+1)}{2} + \frac{p-n}{2} = \frac{(n+1)p}{2}.$$

Лемма доказана.

ЛЕММА 2. Пусть $s > n/2$ и выполняются условия леммы 1. Тогда многочлен над $\mathbb{F}_p$

$$Q = \sum_{j=0}^k \varphi_j H^{k-j} \left(f^{(p-1)/2+k+s} - \sum_{i=0}^{j+s} f^{k+s-i} B_i H^i \right)$$

ненулевой и имеет степень

$$m = kp + (n-1)k(k+s+1) + n(k+s) + (p-1)s. \quad (5)$$

ДОКАЗАТЕЛЬСТВО. Старшие члены многочленов f и H суть $a_n x^n$ и x^p соответственно по определению. Старший член многочлена B_i есть $C_r^i a_n^i x^{(n-1)i}$ из (2). Таким образом, во внутренней сумме слагаемые имеют вид

$$a_n^{k+s-i} x^{n(k+s-i)} C_r^i a_n^i x^{(n-1)i} x^{pi} + \cdots = a_n^{k+s} C_r^i x^{(p-1)i+n(k+s)} + \cdots$$

и степень внутренней суммы определяется слагаемым с наибольшим i , т.е. при $i = j+s$, и равна $(p-1)(j+s) + n(k+s)$. Степень первого слагаемого в скобках есть $n(p-1)/2 + n(k+s)$ и строго меньше.

Найдем старший член многочлена $\varphi_j = f^j \Delta_{j+1}$. Имеем

$$\Delta = \begin{vmatrix} B_{s+1} & \cdots & B_{s+k} \\ \vdots & \ddots & \vdots \\ B_{s+k} & \cdots & B_{s+2k-1} \end{vmatrix} = \begin{vmatrix} C_r^{s+1} a_n^{s+1} x^{(n-1)(s+1)} & \cdots & C_r^{s+k} a_n^{s+k} x^{(n-1)(s+k)} \\ \vdots & \ddots & \vdots \\ C_r^{s+k} a_n^{s+k} x^{(n-1)(s+k)} & \cdots & C_r^{s+2k-1} a_n^{s+2k-1} x^{(n-1)(s+2k-1)} \end{vmatrix} + \cdots$$

Для подсчета определителя вынесем из i -й строки множитель a_n^{s+i} для $1 \leq i \leq k$, после чего из j -го столбца вынесем множитель a_n^{j-1} . В результате a_n в матрице не останется, а общая степень будет $(s+1) + \cdots + (s+k) + 0 + \cdots + (k-1) = sk + k^2$. Аналогичную процедуру проделаем для x^{n-1} . Получим

$$\Delta = \begin{vmatrix} C_r^{s+1} & \cdots & C_r^{s+k} \\ \vdots & \ddots & \vdots \\ C_r^{s+k} & \cdots & C_r^{s+2k-1} \end{vmatrix} a_n^{sk+k^2} x^{(n-1)(sk+k^2)} + \cdots$$

Обозначим определитель, состоящий из биномиальных коэффициентов, через δ , а $\delta_{k+1} = -\delta$.

При $0 \leq j < k$ согласно определению Δ_{j+1} получается заменой $(j+1)$ -го столбца в Δ на столбец, составленный из $B_{s+k+1}, \dots, B_{s+2k}$. Это означает, что степень множителя $a_n x^{n-1}$ повышается на $k-j$, а коэффициент (соответствующий определитель из биномиальных коэффициентов, обозначим его δ_j) может быть получен заменой j -го столбца в δ на столбец, составленный из $C_r^{s+k+1}, \dots, C_r^{s+2k}$.

Собирая предыдущие рассуждения воедино, находим

$$\begin{aligned} Q(x) &= - \sum_{j=0}^k a_n^j x^{nj} \delta_j a_n^{sk+k^2+k-j} x^{(n-1)(sk+k^2+k-j)} x^{p(k-j)} a_n^{k+s} C_r^{j+s} x^{(p-1)(j+s)+n(k+s)} + \cdots \\ &= -a_n^{sk+k^2+2k+s} x^{(n-1)(sk+k^2+k)+kp+n(k+s)+(p-1)s} \sum_{j=0}^k \delta_j C_r^{j+s} + \cdots \\ &= (-1)^k a_n^{sk+k^2+2k+s} x^m \begin{vmatrix} C_r^s & C_r^{s+1} & \cdots & C_r^{s+k} \\ C_r^{s+1} & C_r^{s+2} & \cdots & C_r^{s+k+1} \\ \vdots & \vdots & \ddots & \vdots \\ C_r^{s+k} & C_r^{s+k+1} & \cdots & C_r^{s+2k} \end{vmatrix} + \cdots \end{aligned}$$

В силу леммы 1 член, содержащий x^m , ненулевой в $\mathbb{F}_p$.

Переходим к доказательству теоремы. Достаточно рассматривать многочлены f такие, что $S = S(f) \geq 0$. Действительно, пусть $S(f_1) < 0$ и теорема верна при любом многочлене f , для которого $S(f) \geq 0$. Тогда, выбирая $f = \beta f_1$, где β – какой-нибудь квадратичный невычет, получим

$$S(f_1) = \sum_{x=0}^{p-1} \left(\frac{f(x)/\beta}{p} \right) = -S(f),$$

так что $S(f) > 0$ и, следовательно, теорема верна для f и f_1 .

Выберем

$$s = \frac{n+1}{2} \quad \text{и} \quad k = \left\lceil \frac{\sqrt{p-s^2+2s}-s}{2} \right\rceil.$$

Проверим, что при $p \geq (n^2-1)/2$ выполнены условия леммы 2. Неравенства для s очевидны. Для k нужно проверить неравенства $0 \leq k \leq (p-n)/4$ и $k < (p-n)/2$; поскольку $n \geq 3$, то $p > n$ и последнее неравенство является следствием первого. Имеем

$$(p-s^2+2s)-s^2 = p-2s(s-1) = p - \frac{2(n+1)}{2} \frac{n-1}{2} = p - \frac{n^2-1}{2} \geq 0,$$

откуда $k \geq 0$.

$$k \leq \frac{\sqrt{p-s^2+2s}-s}{2} \leq \frac{\sqrt{p}}{2} - \frac{s}{2} < \frac{p}{4} - \frac{s}{2} < \frac{p-2s+1}{4} = \frac{p-n}{4}.$$

Обозначим соответственно через n_0 и N_0 степени многочленов f_0 и Φ , определенных над $\mathbb{F}_p$ равенствами

$$f_0 = \gcd(f, H), \quad \Phi = \gcd(1 - f^{(p-1)/2}, H). \quad (6)$$

Поскольку

$$H(x) = \prod_{a=0}^{p-1} (x-a),$$

то n_0 – число корней f (без учета кратностей), а N_0 – число x , для которых $f(x)$ – ненулевой квадратичный вычет. Следовательно,

$$2N_0 + n_0 = \sum_{x=0}^{p-1} \left(1 + \left(\frac{f(x)}{p} \right) \right) = p + S(f). \quad (7)$$

Так как

$$F(x^p) = F(x+H) = \sum_{i=0}^r \frac{F^{(i)}}{i!} H^i,$$

то

$$(f(1 - f^{(p-1)/2}))^p = (f - F)^p = f^p - \sum_{i=0}^r \frac{F^{(i)}}{i!} H^i$$

и, замечая, что $2k+s+1 \leq p$, получим из (6)

$$\begin{aligned} & \Phi^{2k+s+1} \Big| \gcd((f-F)^p, H^{2k+s+1}), \\ & \Phi^{2k+s+1} \Big| \gcd\left(f^p - \sum_{i=0}^{2k+s} \frac{F^{(i)}}{i!} H^i, H^{2k+s+1}\right). \end{aligned} \quad (8)$$

Пусть Q – многочлен, определенный в лемме 2. Пользуясь равенствами (1) и (3), находим

$$\begin{aligned} & \left(f^p - \sum_{i=0}^{2k+s} \frac{F(i)}{i!} H^i \right) \sum_{j=0}^k \varphi_j H^{k-j} - f^{(p+1)/2-k-s} Q \\ &= - \sum_{j=0}^k \varphi_j H^{k-j} \sum_{i=0}^{2k+s} \frac{F(i)}{i!} H^i + \sum_{j=0}^k \varphi_j H^{k-j} \sum_{i=0}^{j+s} f^{(p+1)/2-i} B_i H^i \\ &= -H^k \sum_{j=0}^k \varphi_j \left(\sum_{\nu=s+1}^{s+k} \frac{F(\nu+j)}{(\nu+j)!} H^\nu + \sum_{\nu=s+k+1}^{s+2k-j} \frac{F(\nu+j)}{(\nu+j)!} H^\nu \right) = Q_3 H^{2k+s+1}, \end{aligned}$$

где Q_3 – некоторый многочлен над $\mathbb{F}_p$. Теперь из (8) следует, что

$$\Phi^{2k+s+1} \Big| \gcd(f^{(p+1)/2-k-s} Q, H^{2k+s+1}). \quad (9)$$

Так как $f^j | \varphi_j$ и $f_0 = \gcd(f, H)$, то $f^k f_0^{k+s} | Q$ и, следовательно,

$$Q = f^k f_0^{k+s} Q_0, \quad (10)$$

где Q_0 – некоторый многочлен над $\mathbb{F}_p$. В силу леммы 2 многочлен Q_0 ненулевой и имеет степень $m - kn - (k+s)n_0$. Замечая, что многочлены f и Φ взаимно просты, получим из (9) и (10)

$$\Phi^{2k+s+1} \Big| \gcd(Q_0, H^{2k+s+1}).$$

Сравнение степеней дает

$$N_0 \leq \frac{m - kn - (k+s)n_0}{2k+s+1}.$$

Но тогда в силу (5) и (7)

$$S(f) \leq \frac{2m - 2kn - (s-1)n_0}{2k+s+1} - p \leq \frac{2(n-1)k(k+s+1) + 2ns + 2(p-1)s - sp - p}{2k+s+1}. \quad (11)$$

С учетом того, что $s-1 = (n-1)/2$, получаем

$$S(f) \leq \frac{n-1}{2} \left(\frac{p-s^2+2s-1}{2k+s+1} + 2k+s+1 \right).$$

В соответствии с выбором k имеем

$$\sqrt{p-s^2+2s}-1 \leq 2k+s+1 \leq \sqrt{p-s^2+2s}+1.$$

Поскольку при $a > 0$, $x > 0$ функция $a/x + x$ не имеет локальных максимумов, то на любом отрезке максимум достигается в одном из концов и значение в любой точке отрезка не превосходит значения на одном из концов. В данном случае значения на обоих концах одинаковы и дают неравенство

$$S(f) \leq (n-1) \sqrt{p-s^2+2s}. \quad (12)$$

Пусть равенство в (12) достигается. Поскольку $S(f)$ – целое число, то под корнем стоит квадрат натурального числа. Но тогда правая часть оказывается четной. Из (7) получаем, что n_0 нечетно, в частности, больше нуля. Тогда второе из неравенств (11) строгое и неравенство (12) также строгое – противоречие.

Подстановка в (12) $s = (n + 1)/2$ завершает доказательство.

Приведенное доказательство следует оригинальному доказательству Коробова со следующим важным отличием: в [3] параметры выбирались так, чтобы было $s < n/2$, и тогда в сумме, определяющей многочлен Q из леммы 2, другие соотношения степеней между слагаемыми и общую степень считать несколько проще (главный член Q равен главному члену одного слагаемого). Как выяснилось, при подборе параметров в области $s > n/2$ несколько усложняется доказательство леммы 2 (главный член Q получается суммированием главных членов нескольких слагаемых), но получается лучшая итоговая оценка. В работе [4] была приведена оценка, по существу совпадающая с доказанной здесь теоремой, с доказательством, также следующим оригинальному доказательству Коробова, но, к сожалению, ссылающаяся напрямую на лемму 2 из [3]. Но оригинальное доказательство использует значение параметра $s = (n - 1)/2$, и соответствующая лемма там доказана только для $s < n/2$, следовательно, она неприменима напрямую к рассматриваемому случаю.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., **1041**, Hermann et Cie., Paris, 1948.
- [2] A. Weil, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind., **1064**, Hermann & Cie., Paris, 1948.
- [3] П. М. Коробов, “Оценка сумм символов Лежандра”, *Докл. АН СССР*, **196**:4 (1971), 764–767.
- [4] Д. А. Митькин, “Уточнение оценки для суммы символов Лежандра от многочленов нечетной степени”, *Чебышевский сб.*, **6**:3 (2005), 123–126.

Е. А. Гречников

Московский государственный университет

им. М. В. Ломоносова

E-mail: grechnik@mccme.ru

Поступило

15.07.2009