Доклады Академии наук СССР
1971. Том 196, № 4

УДК 511.33

МАТЕМАТИКА

Н. М. КОРОБОВ

ОЦЕНКА СУММЫ СИМВОЛОВ ЛЕЖАНДРА

(Представлено академиком А. Н. Колмогоровым 3 VII 1970)

Пусть $n \geqslant 3$ — нечетное, p — простое, $f(x) = a_0 + a_1 x + \ldots + a_n x^n$ — целочисленный полином $(a_n, p) = 1$ и S — сумма символов Лежандра $\left(\frac{f(x)}{p}\right)$. Для случая $n = 3$ из работы Хассе [1] и для общего случая из работы А. Вейля [2] следует, что

$$|S| = \left|\sum_{x=1}^{p} \left(\frac{f(x)}{p}\right)\right| \leqslant (n-1)\sqrt{p}. \tag{1}$$

Элементарное доказательство этой оценки при $n = 3$ было получено Ю. И. Маниным [3]. При $n \geqslant 3$ подход к элементарному выводу близкой по порядку, но менее сильной оценки был опубликован С. А. Степановым [4].

В общем случае оценку (1) нельзя существенно усилить, так как согласно работе Гекке [5] при $n = 3$ существует полином $f(x)$ такой, что при любом $\varepsilon > 0$ для бесконечной последовательности простых p будет $|S| > (1-\varepsilon)(n-1)\sqrt{p}$.

В настоящей работе при $p \geqslant (n^2+9)/2$ получена оценка

$$|S| \leqslant (n-1)\sqrt{p - (n-3)(n-4)/4}, \tag{2}$$

которая совпадает с оценкой (1) при $n = 3$ и несколько усиливает ее при $n \geqslant 5$. В отличие от (1) эта оценка может быть нетривиальной при $n > 1 + \sqrt{p}$. Так, например, при $p \geqslant 197$ для любого n из интервала $1 + \sqrt{p} < n < 1 + 1{,}1\sqrt{p}$ из (2) получаем $|S| < 0{,}9(n-1)\sqrt{p} < 0{,}99p$. Отсюда, в частности, следует, что оценку Гекке нельзя распространить на случай полиномов произвольной степени $n = n(p)$.

Пусть $r = n(p+1)/2$ и полиномы $F(x)$ и $H(x)$ определены равенствами

$$F(x) = [f(x)]^{(p+1)/2}, \quad H(x) = x^p - x.$$

В дальнейшем часто вместо $f(x)$, $F(x)$ и $H(x)$ будем писать соответственно f, F и H. Пользуясь выражением для производной произведения

$$(f_1 \ldots f_\tau)^{(\nu)} = \nu! \sum_{n_1+\ldots+n_\tau=\nu} \frac{f_1^{(n_1)} \ldots f_\tau^{(n_\tau)}}{n_1! \ldots n_\tau!} \quad (n_j \geqslant 0),$$

при $\tau = (p+1)/2$ и $f_1 = \ldots = f_\tau = f$ легко показать, что

$$\frac{1}{\nu!} F^{(\nu)} = f^{(p+1)/2-\nu} B_\nu \quad (\nu = 0, 1, \ldots, (p+1)/2),$$

где $B_\nu = B_\nu(x)$ — целочисленные полиномы степени $(n-1)\nu$:

$$B_\nu = C_r^\nu a_n^\nu x^{(n-1)\nu} + \ldots \tag{3}$$

Пусть $0 \leqslant s \leqslant (n+1)/2$, $1 \leqslant k \leqslant (p-n)/4$,

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

и при $j = 1, 2, \ldots, k$ определители Δ_j получаются из Δ с помощью замены j-го столбца столбцом, составленным из величин $B_{s+k+1}, \ldots, B_{s+2k}$. Определим целочисленные полиномы $\varphi_j = \varphi_j(x)$ с помощью равенств

$$\varphi_k = -f^k\Delta, \quad \varphi_j = f^j\Delta_{j+1} \quad (0 \leqslant j \leqslant k-1).$$

Легко видеть, что тогда

$$\sum_{j=0}^{k} \frac{f^{(\nu+j)}}{(\nu+j)!}\varphi_j = 0 \quad (\nu = s+1, \ldots, s+k). \tag{4}$$

Действительно, обозначая эту сумму через σ и полагая $\Delta_{k+1} = -\Delta$, при $s+1 \leqslant \nu \leqslant s+k$ получим

$$\sigma = f^{(p+1)/2-\nu}\sum_{j=0}^{k} B_{\nu+j}\Delta_{j+1} = (-1)^{k-1}f^{(p+1)/2-\nu}\begin{vmatrix} B_\nu & B_{\nu+1} & \ldots B_{\nu+k} \\ B_{s+1} & B_{s+2} & \ldots B_{s+k+1} \\ \ldots & \ldots & \ldots \\ B_{s+k} & B_{s+k+1} & \ldots B_{s+2k} \end{vmatrix} = 0.$$

Лемма 1. *Пусть* $n \geqslant 3$ — *нечетное*, $p > n$ — *простое*, $0 \leqslant s \leqslant (n+1)/2$ *и* $r = n(p+1)/2$. *Тогда при любом* $k \leqslant (p-n)/4$

$$\Delta_k(s) = \begin{vmatrix} C_r^{s+1} & \ldots & C_r^{s+k} \\ \ldots & \ldots & \ldots \\ C_r^{s+k} & \ldots & C_r^{s+2k-1} \end{vmatrix} \not\equiv 0 \pmod p.$$

Доказательство. Прибавим в $\Delta_k(s)$ каждый последующий столбец к предыдущему и повторим эти действия со всеми столбцами кроме последнего, затем кроме двух последних и т. д. Тогда после $k-1$ шага

$$\Delta_k(s) = \begin{vmatrix} C_{r+k-1}^{s+k} & \ldots & C_r^{s+k} \\ \ldots & \ldots & \ldots \\ C_{r+k-1}^{s+2k-1} & \ldots & C_r^{s+2k-1} \end{vmatrix}.$$

Но, очевидно,

$$C_{r+k-j}^{s+k+i-1} = C_{r-s-i}^{j-1}\frac{(r+k-j)!\,(j-1)!}{(s+k+i-1)!\,(r-s-i)!} \quad (1 \leqslant i, j \leqslant k)$$

и, следовательно,

$$\Delta_k(s) = \begin{vmatrix} C_{r-s-1}^{0} & \ldots & C_{r-s-1}^{k-1} \\ \ldots & \ldots & \ldots \\ C_{r-s-k}^{0} & \ldots & C_{r-s-k}^{k-1} \end{vmatrix} \prod_{\nu=1}^{k} \frac{(r+k-\nu)!\,(\nu-1)!}{(s+k+\nu-1)!\,(r-s-\nu)!} =$$

$$= (-1)^{k(k-1)/2}\prod_{\nu=0}^{k-1} \frac{(r-\nu-s)\ldots(r-\nu+k-1)}{(\nu+1)\ldots(\nu+k+s)}. \tag{5}$$

Так как, по условию, $s \leqslant (n+1)/2$, $k \leqslant (p-n)/4$ и $r = n(p+1)/2$, то при $\nu = 0, 1, \ldots, k-1$ будет

$$\frac{n-1}{2}p + \frac{n+1}{2} \leqslant r-\nu-s, \quad r-\nu+k-1 \leqslant \frac{n-1}{2}p + p - 1,$$

и в силу (5) лемма доказана.

Лемма 2. *Пусть* $A_m x^m$ — *старший член полинома*

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

Тогда при $s = (n-1)/2$ *будет* $A_m \not\equiv 0 \pmod p$ *и*

$$m = kp + k(k+s+1)(n-1) + n(k+s) + n(p-1)/2. \tag{6}$$

Доказательство. Заметим прежде всего, что при $s = (n-1)/2$ в силу леммы 1

$$\Delta_k(s+1) = \Delta_k((n+1)/2) \not\equiv 0 \pmod p. \tag{7}$$

Запишем полином Q в виде $Q = Q_1 - Q_2$, где

$$Q_1 = f^{(p-1)/2+k+s}\sum_{j=0}^{k}\varphi_j H^{k-j} \text{ и } Q_2 = \sum_{j=0}^{k}\sum_{i=0}^{j+s}\varphi_j f^{k+s-i}B_i H^{k+i-j}.$$

Так как по определению

$$\varphi_0 = \Delta_1 = (-1)^{k-1}\begin{vmatrix} B_{s+2} & \dots & B_{s+k+1} \\ \dots & \dots & \dots \\ B_{s+k+1} & \dots & B_{s+2k} \end{vmatrix},$$

то, пользуясь равенством (3), получим

$$\varphi_0 = (-1)^{k-1}\begin{vmatrix} C_r^{s+2}(a_n x^{n-1})^{s+2} & \dots & C_r^{s+k+1}(a_n x^{n-1})^{s+k+1} \\ \dots & \dots & \dots \\ C_r^{s+k+1}(a_n x^{n-1})^{s+k+1} & \dots & C_r^{s+2k}(a_n x^{n-1})^{s+2k} \end{vmatrix} + \varphi =$$

$$= (-1)^{k-1}\Delta_k (s+1)\, a_n^{k(k+s+1)} x^{k(k+s+1)(n-1)} + \varphi, \qquad (8)$$

где φ — полином, степень которого меньше, чем $k(k+s+1)(n-1)$.

Из сравнения определителей Δ_{j+1} и Δ_1 видно, что при $j > 0$ степень Δ_{j+1} не превосходит $k(k+s+1)(n-1) - j(n-1)$ и, следовательно, степень φ_j не превосходит величины

$$k(k+s+1)(n-1) - j(n-1) + nj = k(k+s+1)(n-1) + j.$$

Отсюда в силу (8) следует, что старший член полинома Q_1 равен

$$(-1)^{k-1}\Delta_k (s+1)\, a_n^{\lambda} x^{kp+k(k+s+1)(n-1)+n(k+s)+n(p-1)/2},$$

где $\lambda > 0$ — некоторое целое. Так как степень полинома Q_2 не больше

$$\max_{0\leqslant i\leqslant j+s}\,[k(k+s+1)(n-1) + j + n(k+s-i) + (n-1)i +$$

$$+ (k+i-j)p] = kp + k(k+s+1)(n-1) + n(k+s) + s(p-1),$$

то при $s = (n-1)/2$ старшие члены полиномов Q_1 и Q совпадают, и в силу (7) лемма 2 доказана.

Теорема 1. *При всяком нечетном* $n \geqslant 3$ и простом $p \geqslant (n^2+9)/2$ *справедлива оценка*

$$|S| \leqslant (n-1)\sqrt{p - (n-3)(n-4)/4}.$$

Доказательство. Легко видеть, что достаточно рассмотреть случай $S = S(f) \geqslant 0$. Действительно, пусть $S(f_1) < 0$ и теорема верна при любом полиноме f, для которого $S(f) \geqslant 0$. Тогда, выбирая $f = \beta f_1$, где β — какой-нибудь квадратичный невычет, получим

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

и, следовательно,

$$|S(f_1)| = S(f) \leqslant (n-1)\sqrt{p - (n-3)(n-4)/4}.$$

Выберем $s = (n-1)/2$ и $k = [{}^1/_2\sqrt{p - (s^2 - 2s + 1/s)} - s/2]$. Так как $p \geqslant (n^2+9)/2$, то, очевидно, $1 \leqslant k \leqslant (p-n)/4$. Обозначим соответственно через n_0 и N_0 степени полиномов f_0 и Φ, определенных сравнениями

$$f_0 \equiv НОД(f, H) \pmod p, \qquad \Phi \equiv НОД(1 - f^{(p-1)/2}, H) \pmod p. \qquad (9)$$

Легко видеть, что тогда число решений сравнения $y^2 \equiv f(x) \pmod p$ будет равно $2N_0 + n_0$ и, следовательно,

$$2N_0 + n_0 = \sum_{x=1}^{p}\left[1 + \left(\frac{f(x)}{p}\right)\right] = p + S(f). \qquad (10)$$

Так как

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