ОЦЕНКА ПОЛНОЙ РАЦИОНАЛЬНОЙ ТРИГОНОМЕТРИЧЕСКОЙ СУММЫ*)

В работе используются следующий обозначения: $\mathbb{N}$ — множество всех натуральных чисел; $\mathbb{P}$ — множество всех простых чисел; $\mathbb{R}$ — поле всех действительных чисел; $\mathbb{Z}$ — кольцо всех целых чисел; $\mathbb{Z}_+$ — множество всех целых неотрицательных чисел; $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ $(p \in \mathbb{P})$ — поле вычетов по модулю p; $\mathbb{Z}[x]$ — кольцо многочленов с коэффициентами из $\mathbb{Z}$; $\mathbb{F}_p[x]$ — кольцо многочленов с коэффициентами из $\mathbb{F}_p$; кроме того, как обычно,

$$\exp(y) = e^y, \qquad e(y) = e^{2\pi i y} \qquad (y \in \mathbb{R}).$$

На протяжении всей работы

$$n, q, s \in \mathbb{N}, \qquad p \in \mathbb{P},$$

$C_1, C_2, \ldots, C_{29}$ — абсолютные положительные константы.

Пусть $f \in \mathbb{Z}[x]$, $\deg f = n \geqslant 1$. *Полными рациональными тригонометрическими суммами* называются суммы вида

$$S(f,q) = \sum_{k=1}^{q} e\left(\frac{f(k)}{q}\right). \tag{0.1}$$

Суммы $S(f,q)$ имеют важные приложения в теории чисел (см. [1–4]) и изучались многими авторами. Если

$$f(x) = \sum_{\nu=0}^{n} a_\nu x^\nu, \qquad h = (a_1, \ldots, a_n, q) > 1,$$

то

$$S(f,q) = h\, e\left(\frac{a_0}{q}\right) S\left(\frac{(f-a_0)}{h},\, \frac{q}{h}\right). \tag{0.2}$$

Поэтому достаточно исследовать суммы $S(f,q)$ для случая

$$a_0 = 0, \qquad (a_1, \ldots, a_n, q) = 1. \tag{0.3}$$

Если $f \in \mathbb{Z}[x]$, $\deg f = n \geqslant 1$ и выполняются условия (0.3), то будем писать $f \in K_n(q)$.

Случай $n = 1$ тривиален: $S(f,q) = 0$ $(f \in K_1(q),\ q > 1)$. Суммы $S(f,q)$ при $n = 2$ полностью исследованы Гауссом [5]. В частности, из результатов Гаусса вытекает, что

$$|S(f,q)| \leqslant \sqrt{2q} \qquad \bigl(f \in K_2(q)\bigr). \tag{0.4}$$

Поэтому в дальнейшем, если не оговорено противное, предполагается, что $n \geqslant 3$.

Суммы $S(f,q)$ при произвольных $n \in \mathbb{N}$ изучались Харди и Литтлвудом в работах, посвященных проблеме Варинга (см. [6]). Используя метод Вейля [7] оценки тригонометрических сумм, Харди и Литтлвуд показали, что если $(a_n, q) = 1$, то для любого $\varepsilon > 0$

$$|S(f,q)| \leqslant A_1(n,\varepsilon)\, q^{1-2^{1-n}+\varepsilon} \tag{0.5}$$

*) Труды МИАН СССР. 1977. Т. 143. С. 188–207.

(см. также [8, теорема 265]). Кроме того, Харди и Литтлвуд установили, что для сумм Гаусса

$$S_n(a,q) = \sum_{k=1}^{q} e\left(\frac{ak^n}{q}\right), \qquad (a,q) = 1 \tag{0.6}$$

(которые уже встречались ранее в теории деления круга) справедливы следующие оценки:

$$|S_n(a,p)| \leqslant (d-1)\sqrt{p}, \qquad d = (n, p-1), \tag{0.7}$$

$$|S_n(a,q)| \leqslant A_2(n)\, q^{1-1/n}. \tag{0.8}$$

Эти оценки являются достижимыми в смысле порядка соответственно по p и по q. Точнее (см. [1, с. 6, 7]),

$$\overline{\lim_{p\to\infty}} \sup_{a:\,(a,p)=1} \frac{|S_n(a,p)|}{\sqrt{p}} \geqslant \sqrt{n-1} \tag{0.9}$$

и (см. [1, с. 7, 8])

$$S_n(a,p^n) = p^{n-1} = p^{n(1-1/n)}, \qquad (n,p) = 1, \tag{0.10}$$

откуда

$$\overline{\lim_{q\to\infty}} \sup_{a:\,(a,q)=1} \frac{|S_n(a,q)|}{q^{1-1/n}} \geqslant 1. \tag{0.11}$$

Наиболее важной является задача оценки сумм $S(f,q)$ в зависимости от q и n *равномерно относительно коэффициентов многочлена* $f \in K_n(q)$, т.е. задача оценки величины

$$H_n(q) = \sup_{f\in K_n(q)} |S(f,q)|. \tag{0.12}$$

Впервые эта задача рассматривалась в 1924 г. Э. Камке [9] в связи с задачей о распределении дробных долей многочленов и проблемой Варинга для многочленов. Камке доказал, что если $f \in K_n(q)$, то справедлива оценка (0.5).

Поведение $H_n(q)$ существенно зависит от арифметических свойств числа q. Наиболее трудной является задача оценки $H_n(q)$ для случая, когда $q = p$ простое. В 1932 г. Г. Морделл [10] доказал, что

$$H_n(p) \leqslant A_3(n)\, p^{1-1/n}, \tag{0.13}$$

а Г. Давенпорт [11] несколько дополнил этот результат (см. также [3, с. 61, 62]). Хуа Ло-кен исследовал задачу оценки $H_n(q)$ в связи с теоремой о среднем для тригонометрических сумм и проблемой Тэрри. Используя оценку (0.13), Хуа [12] (см. также [1, гл. 3]) установил в 1940 г., что для любого $\varepsilon > 0$

$$H_n(q) \leqslant A_4(n,\varepsilon)\, q^{1-1/n+\varepsilon}. \tag{0.14}$$

В 1948 г. А. Вейль [13, 14] получил оценку

$$H_n(q) \leqslant (n-1)\sqrt{p} \qquad (p > n \geqslant 2), \tag{0.15}$$

которая в силу (0.9) достижима в смысле порядка по p [1)]. Основываясь на (0.15), В.И. Нечаев [16] доказал оценку

$$H_n(q) \leqslant A_5(n)\, q^{1-1/n}, \tag{0.16}$$

[1)] В последнее время С.А. Степанов [15] дал новое, и притом элементарное, доказательство для (0.15).

которая в силу (0.11) достижима по q.

А.А. Карацуба [17] рассмотрел задачу об оценке $H_n(q)$ снизу.

Положим

$$B_n = \sup_{q \in \mathbb{N}} H_n(q)/q^{1-1/n}. \tag{0.17}$$

Настоящая работа посвящена исследованию поведения B_n. В силу (0.11) имеем $B_n \geqslant 1$. В 1953 г. В.И. Нечаев [16] доказал, что $B_n \leqslant \exp(2^n)$ $(n \geqslant 12)$, а в 1975 г. он [18] показал, что

$$B_n \leqslant \exp\{5n^2/\ln n\} \qquad (n \geqslant 3). \tag{0.18}$$

Здесь устанавливается оценка

$$B_n \leqslant \exp\bigl\{n + O(n/\ln n)\bigr\} \qquad (n \to \infty), \tag{0.19}$$

из которой, в частности, следует, что

$$B_n \leqslant \exp\{C_1 n\}. \tag{0.20}$$

Иными словами, справедлива такая

Теорема. *Пусть* $n \geqslant 2$, $q \in \mathbb{N}$, $f \in K_n(q)$. *Тогда*

$$|S(f,q)| \leqslant \overline{B}_n\, q^{1-1/n}, \tag{0.21}$$

где

$$\overline{B} = \exp\bigl\{n + O(n/\ln n)\bigr\}. \tag{0.22}$$

Отметим, что если использовать в качестве оценок для $S(f,p)$ оценку А. Вейля (0.15), то асимптотику в показателе (0.19) нельзя улучшить.

Для доказательства (0.19) требуются оценки сумм $S(f,p^s)$, $\bigl(f \in K_n(p)\bigr)$, равномерные относительно $s \in \mathbb{N}$. История этой вспомогательной задачи такова. Хуа [12] (см. также [1, лемма 6, с. 37]) доказал в 1940 г., что

$$|S(f,p^s)| \leqslant n^{2n} p^{s(1-1/n)}, \tag{0.23}$$

а позже (см. [4, лемма 1.6]) он получил оценку

$$|S(f,p^s)| \leqslant n^3 p^{s(1-1/n)}.$$

Уточняя результаты из [16] и [19], В.И. Нечаев установил, что для всех $s \in \mathbb{N}$

$$|S(f,p^s)| \leqslant p^{s(1-1/n)} \qquad \text{при} \;\; p \geqslant (n-1)^{2n/(n-2)}, \tag{0.24}$$

и получил ряд новых оценок $S(f,p^s)$ для меньших значений p. В частности, из них вытекает, что

$$|S(f,p^s)| \leqslant n^2 p^{s(1-1/n)} \qquad (\forall\, p, \;\; \forall\, s \in \mathbb{N}).$$

Для доказательства (0.19) я существенно использую оценку (0.24) и усиливаю оценки В.И. Нечаева для $p \leqslant (n-1)^{2n/(n-2)}$. Например, здесь получен такой результат (теорема 1): *для всех* $n \geqslant 3$, $p \in \mathbb{P}$ *и* $s \in \mathbb{N}$

$$|S(f,p^s)| \leqslant C_2 p^{s(1-1/n)}. \tag{0.25}$$

Основным аппаратом исследования служат свойства кратных корней многочленов из кольца $\mathbb{F}_p[x]$ (лемма 2) и формула сравнения (лемма 3), которая сводит оценку сумм $S(f,p^s)$ к оценкам аналогичных сумм с меньшими показателями s.

В качестве приложения из (0.21) выводится следующая оценка для числа $\rho(f,m)$ различных решений сравнения

$$f(x) \equiv 0 \pmod{m}, \tag{0.26}$$

где $f\in\mathbb{Z}[x]$, $\deg f=n\geqslant 2$, $m\in\mathbb{N}$, $m\geqslant 3$, $(a_1,\ldots,a_n,m)=1$:

$$\rho(f,m)\leqslant m^{1-1/n}\exp\biggl\{C_3 n\biggl(\frac{(\ln m)^{1/n}}{\ln\ln m}+1\biggr)\biggr\}. \tag{0.27}$$

Автор выражает благодарность С.А. Степанову за консультацию по теории многочленов над конечными полями.

§ 1. Вспомогательные утверждения

1.1. Пусть $\mathbb{A}$ — коммутативное кольцо с единицей и $\mathbb{A}[x]$ — кольцо многочленов от одной переменной с коэффициентами из $\mathbb{A}$. Для любого $l\in\mathbb{Z}_+$ в кольце $\mathbb{A}[x]$ определяется операция дифференцирования порядка l: если

$$f(x)=\sum_{\nu=0}^{n}a_\nu x^\nu \qquad (a_\nu\in\mathbb{A}),$$

то

$$f^{[l]}(x)=\sum_{\nu=l}^{n}\binom{\nu}{l}a_\nu x^{\nu-l} \qquad (l\in\mathbb{Z}_+).$$

Ясно, что $f^{[l]}\in\mathbb{A}[x]$, и если кольцо многочленов есть $\mathbb{Z}[x]$, то $f^{[l]}=f^{(l)}/(l!)$. Поэтому вместо $f^{[1]}$ мы будем писать f'.

Лемма 1. *Для того чтобы элемент $a\in\mathbb{A}$ был корнем кратности $k\in\mathbb{N}$ многочлена $f\in\mathbb{A}[x]$, $f\neq 0$, необходимо и достаточно, чтобы выполнялись условия*

$$f^{[l]}(a)=0 \qquad (l=0,\ldots,k-1), \qquad f^{[k]}(a)\neq 0. \tag{1.1}$$

См. [20–22, 15]. Приведем простое доказательство.

Пусть $a\in\mathbb{A}$ есть корень кратности k многочлена f, т.е.

$$f(x)=(x-a)^k g(x), \quad \text{где} \quad g\in\mathbb{A}[x], \quad g(a)\neq 0. \tag{1.2}$$

По формуле Лейбница

$$f^{[l]}(x)=\sum_{\lambda=0}^{l}\bigl((x-a)^k\bigr)^{[\lambda]}g^{[l-\lambda]}(x)=\sum_{\lambda=0}^{l}\binom{l}{\lambda}(x-a)^{k-\lambda}g^{[l-\lambda]}(x) \qquad (l=0,1,\ldots,k),$$

откуда $f^{[l]}(a)=0$ $(l=0,\ldots,k-1)$, $f^{[k]}(a)=g(a)\neq 0$.

Обратно, если выполнены условия (1.1), то по формуле Тейлора

$$f(x)=\sum_{\nu=0}^{n}f^{[\nu]}(a)\,(x-a)^\nu=\sum_{\nu=k}^{n}f^{[\nu]}(a)\,(x-a)^\nu=$$

$$=(x-a)^k\sum_{\nu=k}^{n}f^{[\nu]}(a)\,(x-a)^{\nu-k}=(x-a)^k g(x),$$

где $g\in\mathbb{A}[x]$, $g(a)=f^{[k]}(a)\neq 0$, т.е. a есть корень кратности k многочлена f.

1.2. Пусть $f\in\mathbb{Z}[x]$, $p\in\mathbb{P}$ и $\varphi=\varphi_p$ есть редукция по модулю p кольца $\mathbb{Z}[x]$ на кольцо $\mathbb{F}_p[x]$. Положим $\overline{f}=\varphi(f)$. Число $a\in\mathbb{Z}$ называется *корнем кратности $k\in\mathbb{N}$ сравнения*

$$f(x)\equiv 0 \pmod p, \tag{1.3}$$

если $\overline{f} \neq 0$ и $\bar{a} = \varphi(a)$ есть корень кратности k многочлена $\overline{f} \in \mathbb{F}_p[x]$.

Это определение равносильно тому, что

$$f(x) = (x-a)^k g_1(x) + p\, g_2(x), \tag{1.4}$$

где $g_1, g_2 \in \mathbb{Z}[x]$, $g_1(a) \neq 0$. Корни $a_1, a_2 \in \mathbb{Z}$ сравнения (1.3) считаются различными, если $\bar{a}_1 \neq \bar{a}_2$. Через $N_p(f)$ будем обозначать число всех корней сравнения (1.3) с учетом их кратностей. Иными словами, если $a_1, \ldots, a_r$ $(r \in \mathbb{Z}_+)$ — все различные корни сравнения (1.3) и $k_1, \ldots, k_r$ — их кратности соответственно, то положим

$$N_p(f) = \sum_{\nu=1}^{r} k_\nu. \tag{1.5}$$

Хорошо известно, что всегда

$$0 \leqslant N_p(f) \leqslant \deg \overline{f} \leqslant \deg f. \tag{1.6}$$

1.3. Пусть $f \in \mathbb{Z}[x]$, $f \neq 0$, $p \in \mathbb{P}$. Обозначим через $u = u_p(f)$ наибольшую степень p, делящую все коэффициенты f. Ясно, что если положить $F(x) = p^{-u} f(x)$, то $F \in \mathbb{Z}[x]$ и $\overline{F} \neq 0$. Пусть, кроме того, $\deg f \geqslant 1$, так что $f' \neq 0$. Положим

$$t(f) = t_p(f) = u_p(f'), \qquad g(x) = p^{-t(f)} f'(x), \tag{1.7}$$

$$J(f) = J_p(f) = N_p(g), \tag{1.8}$$

$$h_a(x) = f(a + p\,x) - f(a) \qquad (a \in \mathbb{Z}), \tag{1.9}$$

$$m(a) = u_p(h_a), \qquad f_a(x) = p^{-m(a)} h_a(x). \tag{1.10}$$

Нам понадобится ряд свойств этих характеристик и многочленов.

Лемма 2. *Пусть $n \geqslant 2$, $f \in K_n(p)$. Тогда*:

1) $0 \leqslant t_p(f) \leqslant t = [\ln n / \ln p]$; (1.11)

в частности, $t_p(f) = 0$ при $p > n$;

2) $0 \leqslant J_p(f) \leqslant n - 1$; (1.12)

3) $1 \leqslant m(a) \leqslant n$ $(a \in \mathbb{Z})$; (1.13)

4) *если b есть корень кратности k сравнения*

$$g(x) \equiv 0 \pmod{p}, \tag{1.14}$$

то

$$0 \leqslant J_p(f_b) \leqslant k, \tag{1.15}$$

$$2 \leqslant m(b) \leqslant k + t_p(f) + 1. \tag{1.16}$$

За исключением неравенства

$$m(b) \leqslant k + t_p(f) + 1, \tag{1.17}$$

все эти свойства известны (см. [4, 18]).

Докажем оценку (1.17). По формуле Тейлора

$$h_b(x) = f(b + px) - f(b) = \sum_{\nu=1}^{n} p^\nu\, f^{[\nu]}(b)\, x^\nu.$$

Так как $k \leqslant \deg g \leqslant n - 1$, то коэффициент при x^{k+1} в этой формуле равен

$$p^{k+1} f^{[k+1]}(b) = p^{k+t(f)+1} \frac{g^{[k]}(b)}{k+1},$$

где по лемме 1 $g^{[k]}(b) \not\equiv 0 \pmod p$. Отсюда видно, что если $p^u \big| p^{k+1} f^{[k+1]}(b)$, то $u \leqslant k + t(f) + 1$, откуда и следует (1.17).

Обозначение

$$t = \left[\frac{\ln n}{\ln p}\right]$$

будет сохранено на протяжении всей работы.

1.4. Обозначим через $b_1, \ldots, b_r$ ($r \in \mathbb{Z}_+$) все различные корни сравнения (1.14), через $k_1, \ldots, k_r$ их кратности соответственно и положим

$$m_\nu = m(b_\nu), \quad \varphi_\nu(x) = f_{b_\nu}(x) \qquad (\nu = 1, \ldots, r). \tag{1.18}$$

Тогда в силу определения $f_a(x)$ и леммы 2 имеем

$$2 \leqslant m_\nu \leqslant n, \quad m_\nu \leqslant k_\nu + t_p(f) + 1, \tag{1.19}$$

$$\varphi_\nu \in K_n(p), \quad J_p(\varphi_\nu) \leqslant k_\nu \qquad (\nu = 1, \ldots, r), \tag{1.20}$$

$$0 \leqslant \sum_{\nu=1}^{r} k_\nu = J_p(f) \leqslant n - 1. \tag{1.21}$$

Лемма 3 (формула разбиения). *Пусть $f \in K_n(p)$, $s \in \mathbb{N}$,*

$$s \geqslant 2t_p(f) + 2. \tag{1.22}$$

Тогда

$$|S(f, p^s)| \leqslant \sum_{\nu=1}^{r} \left| \sum_{x=1}^{p^{s-1}} e\big(p^{m_\nu - s}\big)\, \varphi_\nu(x)\big) \right|; \tag{1.23}$$

в частности, если $J_p(f) = 0$ (т.е. сравнение (1.14) не имеет решений), то $S(f, p^s) = 0$.

См. [18, леммы 5 и 6] или [4, гл. I]. Отметим, что

$$\left| \sum_{x=1}^{p^{s-1}} e\big(p^{m_\nu - s}\big)\, \varphi_\nu(x)\big) \right| = \begin{cases} p^{m_\nu - 1} |S(\varphi_\nu p^{s - m_\nu})| & \text{при} \quad m_\nu < s, \\ p^{s-1} & \text{при} \quad m_\nu \geqslant s. \end{cases} \tag{1.24}$$

Таким образом,

$$|S(f, p^s)| \leqslant \sum_{\nu=1}^{r} p^{m_\nu - 1} |S(\varphi_\nu, p^{s - m_\nu})|, \tag{1.25}$$

если $m_\nu < s$ ($\nu = 1, \ldots, r$), т.е. в этом случае сумма $S(f, p^s)$ оценивается через суммы того же вида, но с меньшими показателями s.

Лемма 4. *Пусть $w \in \mathbb{R}$, $w \geqslant 2t + 2$ и для любого многочлена $f \in K_n(p)$ справедливо неравенство*

$$|S(f, p^s)| \leqslant J(f)\, \gamma_n(p)\, p^{s(1 - 1/n)} \quad \textit{при} \quad w \leqslant s < n + w. \tag{1.26}$$

Тогда для любого $f \in K_n(p)$

$$|S(f, p^s)| \leqslant J(f)\, \gamma_n(p)\, p^{s(1 - 1/n)} \quad \textit{при всех} \quad s \geqslant w. \tag{1.27}$$

Доказательство. Проведем индукцию по s. Пусть оценка (1.27) справедлива при $w \leqslant s < n + w_1$, где $w_1 \geqslant w$. Покажем, что тогда она верна и при

$n+w_1 \leqslant s < n+w_1+1$. Поскольку $s \geqslant n+w_1 \geqslant w \geqslant 2t+2$, то применима формула разбиения. Она показывает, что

$$|S(f,p^s)| \leqslant \sum_{\nu=1}^{r} p^{m_\nu - 1} |S(\varphi_\nu, p^{s-m_\nu})| \qquad \big(\varphi_\nu \in K_n(p)\big),$$

где в силу (1.19)

$$w \leqslant w_1 \leqslant s-n \leqslant s-m_\nu \leqslant s-2 < n+w_1+1-2 < n+w_1.$$

Поэтому применима оценка (1.26), и мы получаем

$$|S(f,p^s)| \leqslant \sum_{\nu=1}^{r} p^{m_\nu(1-1/n)} J(\varphi_\nu)\, \gamma_n(p)\, p^{(s-m_\nu)(1-1/n)} \leqslant$$
$$\leqslant \sum_{\nu=1}^{r} J(\varphi_\nu)\, \gamma_n(p)\, p^{s(1-1/n)} \leqslant J(f)\, \gamma_n(p)\, p^{s(1-1/n)};$$

лемма доказана.

§ 2. Оценки сумм $S(f,p^s)$

Лемма 5. *Пусть $f \in K_n(p)$, $s \in \mathbb{N}$, $k \in \mathbb{N}$. Положим*

$$q_1 = 0, \quad q_k = p^{k-1} + \ldots + p \qquad (k > 1). \tag{2.1}$$

Тогда

$$|S(f,p^s)| \leqslant J(f) p^{s-k} \quad \text{при} \quad s \geqslant q_k + (k+1)t + 2, \tag{2.2}$$

$$|S(f,p^s)| \leqslant \frac{J(f)}{s - q_k - (k+2)t - 2}\, p^{s-1} \tag{2.3}$$

при

$$q_k + (k+2)t + 2 < s \leqslant q_{k+1} + (k+2)t + 2. \tag{2.4}$$

Доказательство. В силу условий леммы $s \geqslant 2t + 2 \geqslant 2t(f) + 2$, откуда по формуле разбиения

$$|S(f,p^s)| \leqslant \sum_{\nu=1}^{t} \left| \sum_{x=1}^{p^{s-1}} e\big(p^{m_\nu - s} \varphi_\nu(x)\big) \right|. \tag{2.5}$$

Оценивая внутренние суммы в (2.5) тривиально, получаем

$$S(f,p^s) \leqslant r p^{s-1} \leqslant J(f)\, p^{s-1} \qquad \big(s \geqslant 2t(f) + 2\big), \tag{2.6}$$

что доказывает (2.2) для $k = 1$.

Далее, проведем индукцию по k. Допустим, что оценка (2.2) справедлива для некоторого $k \in \mathbb{N}$, и покажем, что тогда для этого k справедлива оценка (2.3), а оценка (2.2) справедлива для $k+1$. Пусть

$$s > q_k + (k+2)t + 2.$$

В сумме (2.5) область суммирования по ν разделим на две части: пусть в сумме $\sum_1$ $k_\nu \geqslant s - q_k - (k+2)t - 2$, а в сумме $\sum_2$ $k_\nu \leqslant s - q_k - (k+2)t - 3$. Положим

$$S_h = \sum\nolimits_h \left| \sum_{x=1}^{p^{s-1}} e\big(p^{m_\nu - s} \varphi_\nu(x)\big) \right|, \qquad J_h = \sum\nolimits_h k_\nu \qquad (h = 1, 2). \tag{2.7}$$

Тогда

$$|S(f,p^s)| \leqslant S_1 + S_2, \tag{2.8}$$

$$J_1 \geqslant 0, \quad J_2 \geqslant 0, \quad J_1 + J_2 = \sum_{\nu=1}^{r} k_\nu = J = J(f). \tag{2.9}$$

Оценим S_1. Пусть Q есть число членов в сумме $\sum_1$. Так как в сумме $\sum_1$ $k_\nu \geqslant s - q_k - (k+2)t - 2$, то

$$Q\big(s - q_k - (k+2)t - 2\big) \leqslant \sum\nolimits_1 k_\nu = J_1 \leqslant J,$$

откуда по тривиальной оценке

$$S_1 \leqslant Q\, p^{s-1} \leqslant \frac{J_1}{s - q_k - (k+2)t - 2}\, p^{s-1}. \tag{2.10}$$

Оценим S_2. В сумме $\sum_2$ $k_\nu \leqslant s - q_k - (k+2)t - 3$. Отсюда в силу (1.19) и определения t

$$m_\nu \leqslant k_\nu + t + 1 \leqslant s - q_k - (k+1)t - 2, \quad s - m_\nu \geqslant q_k + (k+1)t + 2 \qquad (k \in \mathbb{N}).$$

Поэтому
$$S_2 = \sum\nolimits_2 p^{m_\nu - 1} |S(\varphi_\nu, p^{s-m_\nu})|,$$
и к каждому члену справа применима оценка (2.2). Отсюда, учитывая (1.20) и (2.9), получаем
$$S_2 \leqslant \sum\nolimits_2 J(\varphi_\nu)\, p^{s-k-1} \leqslant \sum\nolimits_2 k_\nu\, p^{s-k-1} = J_2\, p^{s-k-1} = (J - J_1)\, p^{s-k-1}. \qquad (2.11)$$

Сопоставляя оценки (2.8), (2.10) и (2.11), получаем
$$|S(f, p^s)| \leqslant \frac{J_1}{s - q_k - (k+2)t - 2}\, p^{s-1} + (J - J_1) p^{s-k-1} =$$
$$= J_1 \left(\frac{1}{s - q_k - (k+2)t - 2} - \frac{1}{p^k} \right) p^{s-1} + J p^{s-k-1}.$$
Но $0 \leqslant J_1 \leqslant J$. Поэтому, если $s - q_k - (k+2)t - 2 \leqslant p^k$, т.е.
$$s \leqslant q_k + p^k + (k+2)t + 2 = q_{k+1} + (k+2)t + 2,$$
то
$$|S(f, p^s)| \leqslant J \left(\frac{1}{s - q_k - (k+2)t - 2} - \frac{1}{p^k} \right) p^{s-1} + J p^{s-k-1} =$$
$$= \frac{J(f)}{s - q_k - (k+2)t - 2}\, p^{s-1},$$
а если $s - q_k - (k+2)t - 2 \geqslant p^k$, т.е. $s \geqslant q_{k+1} + (k+2)t + 2$, то
$$|S(f, p^s)| \leqslant J(f)\, p^{s-k-1},$$
и лемма доказана.

Лемма 6. *Пусть $n \geqslant 3$, $f \in K_n(p)$, $s \in \mathbb{N}$, $s \geqslant 2t + 2$. Тогда*
$$|S(f, p^s)| \leqslant J(f)\, p^{(3t+3)/n-1}\, p^{s(1-1/n)} \quad \text{при} \quad p \leqslant (n-1)^{n/(n-2)}, \qquad (2.12)$$
$$|S(f, p^s)| \leqslant \frac{J(f)}{n-1}\, p^{1/n}\, p^{s(1-1/n)} \quad \text{при} \quad p \geqslant (n-1)^{n/(n-2)}. \qquad (2.13)$$

Доказательство. Прежде всего заметим, что
$$n < (n-1)^{n/(n-2)} \qquad (n \geqslant 3). \qquad (2.14)$$
Случай $n = 3$ проверяется непосредственно, а если $n \geqslant 4$, то
$$\ln \frac{n}{n-1} < \frac{1}{n-1} < \frac{2}{n-2} < \frac{2}{n-2} \ln(n-1),$$
что равносильно (2.14).

Покажем, что оценки (2.12) и (2.13) справедливы при
$$2t + 2 \leqslant s < n + 2t + 2, \qquad (2.15)$$
т.е. при $2t+2 \leqslant s \leqslant n+2t+1$. Для этого воспользуемся предыдущей леммой при $k = 1$ и $k = 2$.

Рассмотрим несколько различных случаев.

Если $2t + 2 \leqslant s \leqslant 3t + 2$, то по неравенству (2.2) с $k = 1$
$$|S(f, p^s)| \leqslant J(f)\, p^{s/n-1}\, p^{s(1-1/n)} \leqslant J(f)\, p^{(3t+2)/n-1}\, p^{s(1-1/n)}. \qquad (2.16)$$

Пусть
$$3t+3 \leqslant s \leqslant n+2t+1.$$
Неравенство (2.3) при $k=1$ можно записать в виде
$$|S(f,p^s)| \leqslant J(f)\frac{p^{s/n-1}}{s-3t-2}\,p^{s(1-1/n)} \qquad (3t+3 \leqslant s \leqslant p+3t+2). \tag{2.17}$$
Заметим, что функция $\psi(s)=p^{s/n-1}(s-3t-2)^{-1}$ выпукла, и поэтому ее максимум на отрезке $[\alpha,\beta]$ $(\alpha \geqslant 3t+3)$ достигается на одном из концов этого отрезка.

Пусть $p \geqslant n-t-1$, т.е. $n+2t+1 \leqslant p+3t+2$. Тогда отрезок $3t+3 \leqslant s \leqslant n+2t+1$ входит в область, где действует оценка (2.17). Поэтому
$$|S(f,p^s)| \leqslant J(f)\max\left\{p^{(3t+3)/n-1}, \frac{p^{(2t+1)/n}}{n-t-1}\right\}p^{s(1-1/n)} \qquad (3t+3 \leqslant s \leqslant n+2t+1).$$
Сопоставляя эту оценку с (2.16), получаем, что
$$|S(f,p^s)| \leqslant J(f)\max\left\{p^{(3t+3)/n-1}, \frac{p^{(2t+1)/n}}{n-t-1}\right\}p^{s(1-1/n)} \tag{2.18}$$
при
$$p \geqslant n-t-1, \qquad 2t+2 \leqslant s \leqslant n+2t+1. \tag{2.19}$$

Пусть теперь $p \leqslant n-t-2$, т.е. $p+3t+2 < n+2t+1$. Применим (2.17) на всем отрезке $3t+3 \leqslant s \leqslant p+3t+2$, а на оставшейся части $p+3t+2 \leqslant s \leqslant n+2t+1$ воспользуемся оценкой (2.3) при $k=2$. Получаем
$$|S(f,p^s)| \leqslant J(f)\max\{p^{(3t+3)/n-1}, p^{(p+3t+2)/n-2}\}p^{s(1-1/n)} \qquad (3t+3 \leqslant s \leqslant p+3t+2),$$
$$\begin{aligned}|S(f,p^s)| \leqslant J(f)\,p^{s-2} = J(f)\,p^{s/n-2}\,p^{s(1-1/n)} \leqslant J(f)\,p^{(n+2t+1)/n-2}\,p^{s(1-1/n)} = \\ = J(f)\,p^{(2t+1)/n-1}\,p^{s(1-1/n)} \qquad (p+3t+2 \leqslant s \leqslant n+2t+1).\end{aligned}$$
Отсюда на всем отрезке $3t+3 \leqslant s \leqslant n+2t+1$
$$|S(f,p^s)| \leqslant J(f)\max\left\{p^{(3t+3)/n-1},\ p^{(2t+1)/n-1}\right\}p^{s(1-1/n)},$$
т.е.
$$|S(f,p^s)| \leqslant J(f)\,p^{(3t+3)/n-1}\,p^{s(1-1/n)} \qquad (3t+3 \leqslant s \leqslant n+2t+1).$$
Сопоставляя эту оценку с (2.16), получаем, что
$$|S(f,p^s)| \leqslant J(f)\,p^{(3t+3)/n-1}\,p^{s(1-1/n)} \tag{2.20}$$
при
$$p \leqslant n-t-2, \qquad 2t+2 \leqslant s \leqslant n+2t+1. \tag{2.21}$$

Исследуем оценку (2.18). Пусть
$$n-t-1 \leqslant p \leqslant n.$$
Покажем, что тогда
$$\max\left\{p^{(3t+3)/n-1}, \frac{p^{(2t+1)/n}}{n-t-1}\right\} = p^{(3t+3)/n-1}. \tag{2.22}$$
Это утверждение равносильно неравенству
$$p^{(n-t-2)/n} \leqslant n-t-1 \qquad (n-t-1 \leqslant p \leqslant n). \tag{2.23}$$

Если $n = 3$, то возможны случаи $p = 2$, $t = 1$; $p = 3$, $t = 1$; а если $n = 4$, то возможны случаи $p = 2$, $t = 2$; $p = 3$, $t = 1$. Во всех этих случаях неравенство (2.23) справедливо. Поэтому пусть $n \geqslant 5$. Как нетрудно проверить,

$$n > \frac{\ln n}{\ln 2} + 2 \qquad (n \geqslant 5),$$

откуда

$$n > t + 2 \qquad (n \geqslant 5). \tag{2.24}$$

Отсюда вытекает, что при $n \geqslant 5$ (2.23) равносильно такому неравенству:

$$p \leqslant (n - t - 1)^{n/(n-t-2)} \qquad (n - t - 1 \leqslant p \leqslant n),$$

и для его доказательства достаточно установить, что

$$n \leqslant (n - t - 1)^{n/(n-t-2)} \qquad (n - t - 1 \leqslant p \leqslant n, \quad n \geqslant 5).$$

Для этого положим $\chi(\eta) = y^{1/(\eta-1)}$ $(\eta > 1)$. Имеем

$$\frac{\chi'}{\chi} = (\eta - 1)^{-2}\left(\frac{\eta - 1}{\eta} - \ln \eta\right) = (\eta - 1)^{-2}\left(\frac{\eta - 1}{\eta} - \int_1^\eta \frac{du}{u}\right) < 0 \qquad (\eta > 1),$$

т.е. функция $\chi(\eta)$ убывает при $\eta > 1$. Отсюда, учитывая (2.14) и (2.24), имеем

$$n < (n - 1)^{n/(n-2)} < (n - t - 1)^{n/(n-t-2)} \qquad (n \geqslant 5),$$

и неравенство (2.23) доказано. Из (2.18) и (2.22) вытекает, что

$$|S(f, p^s)| \leqslant J(f)\, p^{(3t+3)/n-1}\, p^{s(1-1/n)} \tag{2.25}$$

при

$$n - t - 1 \leqslant p \leqslant n, \qquad 2t + 2 \leqslant s \leqslant n + 2t + 1.$$

Оценки (2.20) и (2.25) склеиваются и показывает, что неравенство (2.25) справедливо для всех

$$p \leqslant n, \qquad 2t + 2 \leqslant s \leqslant n + 2t + 1.$$

Пусть теперь $p > n$. Тогда $t = 0$, и неравенство (2.18) приобретает вид

$$|S(f, p^s)| \leqslant J(f) \max\left\{p^{3/n-1}, \frac{p^{1/n}}{n - 1}\right\} p^{s(1-1/n)} \qquad (p > n, \ \ 2t + 2 \leqslant s \leqslant n + 2t + 1). \tag{2.26}$$

Здесь максимум равен $p^{3/n-1}$ при $p \leqslant (n - 1)^{n/(n-2)}$ и равен $p^{1/n}(n - 1)^{-1}$ при $p \geqslant (n - 1)^{n/(n-2)}$. Складывая оценки (2.25) и (2.26), получаем, что при $2t + 2 \leqslant$ $\leqslant s \leqslant n + 2t + 2$

$$|S(f, p^s)| \leqslant J(f)\, p^{(3t+3)/n-1}\, p^{s(1-1/n)} \qquad \big(p \leqslant (n - 1)^{n/(n-2)}\big),$$

$$|S(f, p^s)| \leqslant J(f) \frac{p^{1/n}}{n - 1}\, p^{s(1-1/n)} \qquad \big(p \geqslant (n - 1)^{n/(n-2)}\big).$$

Наконец, применяя лемму 4, убеждаемся, что эти неравенства справедливы для всех $s \geqslant 2t + 2$, и лемма полностью доказана.

Теперь мы можем получить оценки $S(f, p^s)$, справедливые для всех $s \in \mathbb{N}$.

Лемма 7. *Пусть $n \geqslant 3$, $f \in K_n(f)$, $s \in \mathbb{N}$. Тогда*

$$|S(f, p^s)| \leqslant \max\left\{p^{(2t+1)/n}, \ J(f) p^{(3t+3)/n-1}\right\} p^{s(1-1/n)} \quad \textit{при} \quad p \leqslant (n - 1)^{n/(n-2)}, \tag{2.27}$$

$$|S(f, p^s)| \leqslant p^{1/n}\, p^{s(1-1/n)} \quad \textit{при} \quad p \geqslant (n - 1)^{n/(n-2)}. \tag{2.28}$$

В частности,

$$|S(f,p^s)| \leqslant (n-1)\,p^{(3t+3)/n-1}\,p^{s(1-1/n)} \leqslant (n-1)n^{3/n}\,p^{3/n-1}\,p^{s(1-1/n)} \quad \text{\textit{при} } p \leqslant n, \tag{2.29}$$

$$|S(f,p^s)| \leqslant (n-1)\,p^{3/n-1}\,p^{s(1-1/n)} \quad \text{\textit{при}} \quad n < p \leqslant (n-1)^{n/(n-2)}. \tag{2.30}$$

Доказательство. В случае $1 \leqslant s \leqslant 2t+1$ применение тривиальной оценки дает

$$|S(f,p^s)| \leqslant p^s = p^{s/n}\,p^{s(1-1/n)} \leqslant p^{(2t+1)/n}\,p^{s(1-1/n)} \qquad (1 \leqslant s \leqslant 2t+1).$$

Сопоставляя эту оценку с леммой 6 и замечая, что всегда $J(f) \leqslant n-1$, получаем оценки (2.27) и (2.28).

Далее, при $p \leqslant (n-1)^{n/(n-2)}$

$$\max\left\{p^{(2t+1)/n},\ J(f)\,p^{(3t+3)/n-1}\right\} \leqslant \max\left\{p^{(2t+1)/n},\ (n-1)\,p^{(3t+3)/n-1}\right\} =$$
$$= (n-1)\,p^{(3t+3)/n-1} \leqslant \begin{cases} (n-1)\,n^{3/n}\,p^{3/n-1} & (p \leqslant n), \\ (n-1)\,p^{3/n-1} & (n < p \leqslant (n-1)^{n/(n-2)}), \end{cases}$$

откуда следуют оценки (2.29) и (2.30), и лемма доказана.

Мы будем пользоваться оценкой (2.28) при $p \leqslant (n-1)^{2n/(n-2)}$, а при $p \geqslant (n-1)^{2n/(n-2)}$ — более сильной оценкой (0.21).

Отметим, что для $(n-1)^{n/(n-2)} \leqslant p \leqslant (n-1)^{2n/(n-2)}$ В.И. Нечаев [18, лемма 9], используя (0.15), получил оценку

$$|S(f,p^s)| \leqslant (n-1)\,p^{1/n-1/2}\,p^{s(1-1/n)}; \tag{2.31}$$

она будет применяться в § 3 при доказательстве теоремы 1.

§ 3. Равномерная оценка $S(f,p^s)$

Из результатов § 2 без труда вытекает, что

$$|S(f,p^s)| \leqslant A_6(n)\,p^{s(1-1/n)} \qquad (f \in K_n(p),\ s \in \mathbb{N}),$$

где $A_6(n) = O(n)$, равномерно относительно p и s. Здесь мы докажем, что на самом деле $A_6(n) \leqslant C_4$.

Отметим, что этот результат не будет использован при доказательстве оценки (0.19).

Как это обычно бывает при получении равномерных оценок, область изменения параметров приходится делить на большое число частей, в каждой из которых действуют свои оценки. Уточним лемму 6 для малых p.

Лемма 8. *Пусть* $f \in K_n(p)$, $w = n/\ln p$, $s \in \mathbb{N}$,

$$n \geqslant C_5, \quad p \leqslant n, \quad s > w. \tag{3.1}$$

Тогда

$$|S(f,p^s)| \leqslant C_6\,J(f)\,n^{-1}\,p^{s(1-1/n)}. \tag{3.2}$$

Доказательство. 1) Покажем, что найдется константа C_5 такая, что для всех

$$n \geqslant C_5, \quad p \leqslant n, \quad w < s \leqslant n + w \tag{3.3}$$

выполняется неравенство

$$|S(f,p^s)| \leqslant C_7\,J(f)\,n^{-1}\,p^{s-1}. \tag{3.4}$$

Так как $t \leqslant \ln n/\ln p$ и $p \leqslant n$, то

$$2(3t+2) \leqslant w \qquad (n \geqslant C_8).$$

Пусть $n \geqslant C_8$. Найдем $k \in \mathbb{N}$ из условий

$$2\bigl(q_k + (k+2)t + 2\bigr) < s \leqslant 2\bigl(q_{k+1} + (k+3)t + 2\bigr) \tag{3.5}$$

и рассмотрим два случая. Пусть

$$2\bigl(q_k + (k+2)t + 2\bigr) < s \leqslant q_{k+1} + (k+2)t + 2. \tag{3.6}$$

Тогда применима оценка (2.3) из леммы 5, и так как в силу (3.6)

$$\bigl(s - q_k - (k+2)t - 2\bigr)^{-1} \leqslant 2s^{-1},$$

то

$$|S(f,p^s)| \leqslant \frac{J(f)}{s - q_k - (k+2)t - 2}\, p^{s-1} \leqslant 2J(f)s^{-1}p^{s-1}. \tag{3.7}$$

Пусть теперь

$$q_{k+1} + (k+2)t + 2 < s < 2\bigl(q_k + (k+3)t + 2\bigr). \tag{3.8}$$

Так как $p^k \leqslant q_{k+1} \leqslant 2p^k$ $(k \in \mathbb{N})$, то

$$p^k \leqslant q_{k+1} < s \leqslant n + w \leqslant C_9 n, \qquad k \leqslant C_{10}\frac{\ln n}{\ln p},$$

откуда

$$(k+3)t + 2 \leqslant C_{11}\frac{\ln^2 n}{\ln p} \leqslant \frac{w}{4} \leqslant \frac{s}{4} \qquad (n \geqslant C_{12}). \tag{3.9}$$

Отсюда и из (3.8)

$$s \leqslant 2\bigl(q_{k+1} + (k+3)t + 2\bigr) \leqslant 4p^k + \frac{s}{2} \qquad (n \geqslant C_{12}),$$

т.е.

$$s \leqslant 8^k \qquad (n \geqslant C_{12}).$$

В силу (3.8) применима оценка (2.2) леммы 5 (с заменой k на $k+1$), которая дает

$$|S(f,p^s)| \leqslant J(f)\, p^{s-k-1} \leqslant 8J(f)s^{-1}p^{s-1}. \tag{3.10}$$

Оценки (3.7) и (3.10) показывают, что (3.4) установлено с $C_6 = 8$, $C_5 = \max(C_8, C_{12})$.

2) Покажем теперь, что оценка (3.2) справедлива при

$$n \geqslant C_5, \qquad w < s \leqslant n + w.$$

Имеем по доказанному

$$|S(f,p^s)| \leqslant C_5\, J(f)\, s^{-1}\, p^{s-1} = C_6\, J(f)\, s^{-1}\, p^{s/n-1}\, p^{s(1-1/n)} \qquad (w < s \leqslant n + w).$$

Но $s^{-1}p^{s/n-1}$ есть выпуклая функция от s. Поэтому, учитывая, что $w = n/\ln p$, имеем

$$\max_{w \leqslant s \leqslant n+w} s^{-1}p^{s/n-1} = \max\bigl\{w^{-1}p^{w/n-1},\ (w+n)^{-1}p^{(w+n)/n-1}\bigr\} =$$

$$= \max\bigl\{n^{-1}\ln p \cdot e \cdot p^{-1},\ n^{-1}e\bigr\} \leqslant C_{12}n^{-1}. \tag{3.11}$$

Отсюда

$$|S(f,p^s)| \leqslant C_6\, C_{13} J(f)\, n^{-1} p^{s(1-1/n)} = \\ = C_6 J(f)\, n^{-1} p^{s(1-1/n)} \qquad (n \geqslant C_5,\ w < s \leqslant n+w). \quad (3.12)$$

Наконец, применяя лемму 4, убеждаемся, что оценка (3.12) справедлива для всех $s > w$, и лемма доказана.

Теорема 1. *Пусть* $n \geqslant 3$, $f \in K_n(p)$, $s \in \mathbb{N}$. *Тогда*

$$|S(f,p^s)| \leqslant C_2 p^{s(1-1/n)}. \qquad (3.13)$$

Доказательство. Рассмотрим два случая.

1) $p \leqslant n$. Если $3 \leqslant n \leqslant C_5$, то по лемме 7

$$|S(f,p^s)| \leqslant (n-1)\, n^{3/n}\, p^{3/n-1}\, p^{s(1-1/n)} \leqslant C_{14}\, p^{s(1-1/n)} \qquad (3 \leqslant n \leqslant C_3).$$

Пусть $n \geqslant C_5$. Если $s \leqslant w = n/\ln p$, то по тривиальной оценке

$$|S(f,p^s)| \leqslant p^s \leqslant p^{w/n}\, p^{s(1-1/n)} \leqslant e\, p^{s(1-1/n)} \qquad (s \leqslant w).$$

Если же $s > w$, то по предыдущей лемме

$$|S(f,p^s)| \leqslant C_6\, J(f)\, n^{-1}\, p^{s(1-1/n)} \leqslant C_6\, p^{s(1-1/n)} \qquad (s > w).$$

Из этих оценок вытекает, что

$$|S(f,p^s)| \leqslant C_{15}\, p^{s(1-1/n)} \qquad (n \geqslant 3,\ \ p \leqslant n). \qquad (3.14)$$

2) $p > n$. Если $n < p \leqslant (n-1)^{n/(n-2)}$, то согласно (2.30)

$$|S(f,p^s)| \leqslant (n-1) p^{3/n-1} p^{s(1-1/n)} \leqslant p^{3/n}\, p^{s(1-1/n)} \leqslant (n-1)^{3/(n-2)}\, p^{s(1-1/n)}.$$

Если $(n-1)^{n/(n-2)} < p \leqslant (n-1)^{2n/(n-2)}$, то согласно (2.28)

$$|S(f,p^s)| \leqslant p^{1/n}\, p^{s(1-1/n)} \leqslant (n-1)^{2/(n-2)} p^{s(1-1/n)}.$$

Если же $p \geqslant (n-1)^{2n/(n-2)}$, то согласно (0.21)

$$|S(f,p^s)| \leqslant p^{s(1-1/n)}.$$

Отсюда

$$|S(f,p^s)| \leqslant (n-1)^{3/(n-2)} p^{s(1-1/n)} \qquad (p > n); \qquad (3.15)$$

в частности,

$$|S(f,p^s)| \leqslant C_{16} p^{s(1-1/n)} \qquad (n \geqslant 3 \quad p > n). \qquad (3.16)$$

Сопоставляя оценки (3.14) и (3.16), убеждаемся, что для всех $n \geqslant 3$, $f \in K_n(f)$ и $s \in \mathbb{N}$

$$|S(f,p^s)| \leqslant C_2 p^{s(1-1/n)},$$

где $C_2 = \max(C_{15}, C_{16})$, и теорема доказана.

Из (0.10) и (3.15) вытекает, что

$$\sup_{s \in \mathbb{N}} \frac{H_n(p^s)}{p^{s(1-1/n)}} = 1 + O(n^{-1} \ln n) \qquad (3.17)$$

равномерно относительно $p > n$.

§ 4. Оценка сумм $S(f,q)$

Лемма 9 (мультипликативное свойство). *Пусть* $f\in K_n(q)$, *где*

$$q=d_1\dots d_l;\quad d_j\in\mathbb{N},\quad (d_i,d_j)=1\quad (i\ne j). \tag{4.1}$$

Тогда найдутся многочлены $\varphi_j\in K_n(d_j)$ $(j=1,\dots,l)$ *такие, что*

$$S(f,q)=\prod_{j=1}^{l}S(\varphi_j,d_j). \tag{4.2}$$

См. [1, лемма 1, с. 33].

Положим, как обычно,

$$\pi(x)=\sum_{p\leqslant x}1,\qquad \vartheta(x)=\sum_{p\leqslant x}\ln p\qquad (x\geqslant 1). \tag{4.3}$$

Нам понадобятся следующие классические оценки для этих функций:

$$\pi(x)=O\Big(\frac{x}{\ln x}\Big),\qquad \vartheta(x)=x+O\Big(\frac{x}{\ln x}\Big), \tag{4.4}$$

$$\pi(x)\ln x-\vartheta(x)=\int_1^x\pi(u)\,\frac{du}{u}=O\Big(\frac{x}{\ln x}\Big)\qquad (x\geqslant 2). \tag{4.5}$$

Теорема 2. *Пусть* $n\geqslant 3$, $f\in K_n(q)$. *Тогда*

$$|S(f,q)|\leqslant \overline{B}_n q^{1-1/n}, \tag{4.6}$$

где

$$\overline{B}_n=\exp\big\{n+O(n/\ln n)\big\}. \tag{4.7}$$

Доказательство. По лемме 9, если q имеет каноническое разложение

$$q=\prod_{j=1}^{l}p_j^{s_j}\qquad (p_j\in\mathbb{P},\ s_j\in\mathbb{N}),$$

то

$$S(f,q)=\prod_{j=1}^{l}S(\varphi_j,p_j^{s_j}),$$

где $\varphi_j\in K_n(p_j)$ $(j=1,\dots,l)$. Используя лемму 7 и (0.21) и полагая $X_n=(n-1)^{n/(n-2)}$, выводим отсюда

$$q^{1/n-1}|S(f,q)|=\prod_{p_j|q}p_j^{s_j(1/n-1)}|S(\varphi_j,p_j^{s_j})|\leqslant$$

$$\leqslant\prod_{p\leqslant n}(n-1)\,n^{3/n}\,p^{3/n-1}\prod_{n<p\leqslant X_n}(n-1)\,p^{3/n-1}\prod_{X_n<p\leqslant X_n^2}p^{1/n}=$$

$$=\prod_{p\leqslant X_n^2}p^{1/n}\prod_{p\leqslant X_n}(n-1)\,p^{2/n-1}\prod_{p\leqslant n}n^{3/n}=$$

$$=\exp\Big\{\frac1n\,\vartheta(X_n^2)+\ln(n-1)\,\pi(X_n)+\Big(\frac2n-1\Big)\vartheta(X_n)+\frac{3\ln n}{n}\,\pi(n)\Big\}=$$

$$=\exp\Big\{\frac1n\,\vartheta(X_n^2)+\Big(1-\frac2n\Big)\big(\pi(X_n)\ln X_n-\vartheta(X_n)\big)+\frac{3\ln n}{n}\,\pi(n)\Big\}.$$

Таким образом, можно положить

$$B_n = \exp\bigl\{F(n)\bigr\}, \tag{4.8}$$

где

$$F(n) = \frac{1}{n}\,\vartheta(X_n^2) + \Bigl(1-\frac{2}{n}\Bigr)\bigl(\pi(X_n)\ln X_n - \vartheta(X_n)\bigr) + \frac{3\ln n}{n}\,\pi(n). \tag{4.9}$$

Оценим $F(n)$. Имеем

$$n < X_n = (n-1)^{n/(n-2)} = n + O(\ln n), \qquad X_n^2 = n^2 + O(n\ln n),$$

откуда, учитывая (4.4) и (4.5), имеем

$$F(n) = \frac{1}{n}\left(X_n^2 + O\Bigl(\frac{X_n^2}{\ln X_n^2}\Bigr)\right) + O\left(\frac{X_n}{\ln X_n}\right) + O(1) =$$
$$= \frac{1}{n}\bigl(n^2 + O(n\ln n)\bigr) + O\left(\frac{n}{\ln n}\right) + O\left(\frac{n}{\ln n}\right) + O(1) = n + O\left(\frac{n}{\ln n}\right).$$

Поэтому

$$\overline{B}_n = \exp\bigl\{n + O(n/\ln n)\bigr\},$$

и теорема доказана.

Следствие. *Пусть* $n \geqslant 2$, $f \in K_n(q)$. *Тогда*

$$|S(f,q)| \leqslant e^{C_1 n}\, q^{1-1/n}. \tag{4.10}$$

Если $p \leqslant (n-1)^2$, то для $S(f,p)$ известны нетривиальные оценки, справедливые для произвольных многочленов $f \in K_n(p)$. Но тогда, полагая,

$$q = \prod_{p \leqslant (n-1)^2} p$$

и пользуясь мультипликативным свойством $S(f,q)$, мы получим для $S(f,q)$ только тривиальную оценку

$$|S(f,q)| \leqslant q = \Bigl\{\prod_{p \leqslant (n-1)^2} p\Bigr\}^{1/n} q^{1-1/n}. \tag{4.11}$$

В силу (4.4) множитель при $q^{1-1/n}$ равен

$$\Bigl\{\prod_{p \leqslant (n-1)^2} p\Bigr\}^{1/n} = \exp\Bigl\{\frac{1}{n}\,\vartheta\bigl((n-1)^2\bigr)\Bigr\} = \exp\bigl\{n + o(n)\bigr\},$$

т.е. имеет вид правой части (4.7). Таким образом, дальнейшее усиление теоремы 2 невозможно без предварительного усиления оценок для $S(f,p)$.

§ 5. О числе решений сравнения $f(x) \equiv 0 \pmod{m}$

Пусть

$$f \in \mathbb{Z}[x], \qquad \deg f = n \geqslant 2, \qquad m \in \mathbb{N}, \qquad (a_1, \ldots, a_n, m) = 1.$$

Обозначим через $\rho(f,m)$ число различных решений сравнения

$$f(x) \equiv 0 \pmod{m}. \tag{5.1}$$

Как известно, $\rho(f,p) \leqslant n$, откуда

$$\rho(f,p^s) \leqslant np^{s-1} \qquad (s \in \mathbb{N}). \tag{5.2}$$

При $1 \leqslant s \leqslant n$ эта оценка является достижимой в смысле порядка по p, так как сравнение

$$\overline{f}(x) = x^n \equiv 0 \pmod{p}^s,$$

где $1 \leqslant s \leqslant n$, имеет p^{s-1} решений. В частности,

$$\rho(\overline{f},\overline{m}) = \overline{m}^{1-1/n} \tag{5.3}$$

для чисел m вида p^n.

Э. Камке [9] доказал, что для любых $m \in \mathbb{N}$

$$\rho(f,m) \leqslant d^{n-1}(m)\, m^{1-1/n}, \tag{5.4}$$

где $d(m)$ — число делителей m. В силу известных оценок для функции $d(m)$ из (5.4) следует, что

$$\rho(f,m) \leqslant m^{1-1/n} \exp\left\{C_{17}\, n\, \frac{\ln m}{\ln\ln m}\right\} \qquad (m \geqslant 3). \tag{5.5}$$

Для многочленов с отличным от нуля дискриминантом другие оценки $\rho(f,m)$ были получены Оре и Нагеллем (см. [23, гл. III]).

В качестве приложения установленных в § 4 оценок для $S(f,q)$ здесь будет доказана еще одна оценка для $\rho(f,m)$, которая несравнима с (5.4), но сильнее (5.5).

Нам понадобятся две простые леммы, относящиеся к классическим функциям теории чисел.

Лемма 10. *Пусть $x > 1$, $0 \leqslant \alpha < 1$. Тогда*

$$\sum_{p \leqslant x} p^{-\alpha} \leqslant C_{18}\left\{\frac{x^{1-\alpha}}{(1-\alpha)\ln x} + \ln\frac{1}{1-\alpha}\right\}. \tag{5.6}$$

Доказательство. Достаточно рассмотреть случай $x \geqslant 2$. Так как $\pi(u) \leqslant C_{19} u/\ln u$ $(u \geqslant 2)$, то имеем

$$\sum_{p \leqslant x} p^{-\alpha} = \int_{2-0}^{x} u^{-\alpha}\, d\pi(u) = x^{-\alpha}\pi(x) + \alpha \int_2^x \pi(u)\, u^{-\alpha-1}\, du \leqslant$$
$$\leqslant C_{19}\left\{\frac{x^{1-\alpha}}{\ln x} + \int_2^x \frac{du}{u^\alpha \ln u}\right\} \qquad (x \geqslant 2). \tag{5.7}$$

Оценим интеграл

$$I(x) = \int_2^x u^{-\alpha}(\ln u)^{-1}\, du.$$

Для этого положим $B = \exp\{2/(1-\alpha)\}$ и рассмотрим два случая.

Пусть $2 \leqslant x \leqslant B$. Тогда $u^{1-\alpha} \leqslant e^2$ $(2 \leqslant u \leqslant x)$ и

$$I(x) \leqslant e^2 \int_2^x u^{-1}(\ln u)^{-1}\, du = e^2(\ln\ln x - \ln\ln 2) \leqslant$$
$$\leqslant e^2\left(\ln\frac{2}{1-\alpha} + \ln\frac{1}{\ln 2}\right) \leqslant C_{20} \ln\frac{2}{1-\alpha} \qquad (2 \leqslant x \leqslant B). \tag{5.8}$$

Пусть теперь $x \geqslant B$. Имеем в силу (5.8)

$$I(x) = \int_2^B + \int_B^x \leqslant C_{20} \ln \frac{2}{1-\alpha} + \int_B^x u^{-\alpha} (\ln u)^{-1} du.$$

Но в силу определения B

$$\int_B^x u^{-\alpha}(\ln u)^{-1} du = \frac{u^{1-\alpha}}{(1-\alpha)\ln u}\bigg|_B^x + \frac{1}{1-\alpha}\int_B^x u^{-\alpha}(\ln u)^{-2} du \leqslant$$

$$\leqslant \frac{1}{1-\alpha}\left\{\frac{x^{1-\alpha}}{\ln x} + \frac{1}{\ln B}\int_B^x u^{-\alpha}(\ln u)^{-1} du\right\} \leqslant \frac{x^{1-\alpha}}{(1-\alpha)\ln x} + \frac{1}{2}\int_B^x u^{-\alpha}(\ln u)^{-1} du,$$

откуда

$$\int_B^x u^{-\alpha}(\ln u)^{-1} du \leqslant \frac{2x^{1-\alpha}}{(1-\alpha)\ln x} \qquad (x \geqslant B)$$

и

$$I(x) \leqslant \frac{2x^{1-\alpha}}{(1-\alpha)\ln x} + C_{20}\ln\frac{2}{1-\alpha} \qquad (x \geqslant B). \tag{5.9}$$

Сопоставляя оценки (5.7)–(5.9), получаем, что

$$\sum_{p \leqslant x} p^{-\alpha} \leqslant C_{21}\left\{\frac{x^{1-\alpha}}{(1-\alpha)\ln x} + \ln\frac{2}{1-\alpha}\right\} \qquad (x \geqslant 2). \tag{5.10}$$

Наконец, если $0 \leqslant \alpha \leqslant 1/2$, то в оценке (5.10) первый член поглощает второй, а если $1/2 < \alpha < 1$, то

$$\ln\frac{2}{1-\alpha} \leqslant C_{22}\ln\frac{1}{1-\alpha},$$

откуда вытекает (5.6) для всех $x \geqslant 2$, и лемма доказана.

Лемма 11. *Пусть $m \geqslant 3,\ 1/2 \leqslant \alpha < 1$. Тогда*

$$\sigma_{-\alpha}(m) = \sum_{d|m} d^{-\alpha} \leqslant \exp\left\{C_{23}\left(\frac{(\ln m)^{1-\alpha}}{(1-\alpha)\ \ln\ln m} + \ln\frac{1}{1-\alpha}\right)\right\}. \tag{5.11}$$

Доказательство. Пусть каноническое разложение m имеет вид

$$m = \prod_{s=1}^{\omega} p_{k_s}^{a_s}.$$

Так как $\ln(1-p^{-\alpha}) \leqslant C_{24}p^{-\alpha}\quad (1/2 \leqslant \alpha < 1)$, то имеем

$$\sigma_{-\alpha}(m) = \prod_{s=1}^{\omega}\frac{1-p_{k_s}^{-\alpha(a_s+1)}}{1-p_{k_s}^{-\alpha}} < \prod_{p|m}(1-p^{-\alpha})^{-1} = \exp\left\{\sum_{p|m}\ln(1-p^{-\alpha})^{-1}\right\} \leqslant$$

$$\leqslant \exp\left\{C_{24}\sum_{p|m}p^{-\alpha}\right\} \qquad \left(\frac{1}{2} \leqslant \alpha < 1\right). \tag{5.12}$$

Далее,

$$m = \prod_{s=1}^{\omega} p_{k_s}^{a_s} \geqslant \prod_{s=1}^{\omega} p_{k_s} \geqslant \prod_{p \leqslant p_\omega} p,$$

откуда

$$\ln m \geqslant \sum_{p\leqslant p_\omega} \ln p = \vartheta(p_\omega) \geqslant C_{25}p_\omega, \qquad p_\omega \leqslant C_{26}\,\ln m,$$

где $C_{26} > 1$. Используя предыдущую лемму, выводим отсюда

$$\sum_{p|m} p^{-\alpha} \leqslant \sum_{p\leqslant p_\omega} p^{-\alpha} \leqslant \sum_{p\leqslant C_{26}\ln m} p^{-\alpha} \leqslant C_{18}\left\{\frac{(C_{26}\ln m)^{1-\alpha}}{(1-\alpha)\ln\ln m} + \ln\frac{1}{1-\alpha}\right\} \leqslant$$

$$\leqslant C_{27}\left\{\frac{(\ln m)^{1-\alpha}}{(1-\alpha)\ln\ln m} + \ln\frac{1}{1-\alpha}\right\} \qquad (0\leqslant\alpha<1). \quad (5.13)$$

Сопоставляя эту оценку с (5.12), получаем (5.11), и лемма доказана.

Теорема 3. *Пусть*

$$f\in\mathbb{Z}[x], \quad \deg f = n\geqslant 2, \quad m\geqslant 3, \quad (a_1,\ldots,a_n,m)=1. \qquad (5.14)$$

Тогда

$$\rho(f,m) \leqslant m^{1-1/n}\exp\left\{C_3 n\left(\frac{(\ln m)^{1/n}}{\ln\ln m}+1\right)\right\}. \qquad (5.15)$$

Доказательство. Имеем (см. [24, с. 60])

$$\rho(f,m) = \frac{1}{m}\sum_{n=1}^{m}\sum_{k=1}^{m} e\Big(\frac{a}{m}\,f(k)\Big) = \frac{1}{m}\sum_{d|m}\sum_{a(d)}{}^{*}\sum_{k=1}^{m} e\Big(\frac{a}{d}\,f(k)\Big),$$

где $*$ обозначает суммирование по приведенной системе вычетов по $\pmod d$. Используя обозначения введения, выводим отсюда

$$\rho(f,m) \leqslant \frac{1}{m}\sum_{d|m}\varphi(d)\,\frac{m}{d}\,H_n(d) = \sum_{d|m}\frac{\varphi(d)}{d}\,H_n(d), \qquad (5.16)$$

где $\varphi(d)$ — функция Эйлера. Но

$$H_n(d) \leqslant B_n d^{1-1/n}$$

и

$$\varphi(d) \leqslant d.$$

Поэтому

$$\rho(f,m) \leqslant B_n\sum_{d|m} d^{1-1/n} = B_n\, m^{1-1/n}\,\sigma_{1/n-1}(m). \qquad (5.17)$$

Далее, согласно следствию из теоремы 2 $B_n \leqslant \exp(C_1 n)$. Отсюда и из леммы 11

$$\rho(f,m) \leqslant m^{1-1/n}\exp\left\{C_1 n + C_{23} n\left(\frac{(\ln m)^{1/n}}{\ln\ln m}+\ln n\right)\right\} \leqslant$$

$$\leqslant m^{1-1/n}\exp\left\{C_3 n\left(\frac{(\ln m)^{1/n}}{\ln\ln m}+1\right)\right\},$$

и теорема доказана.

Отметим, что функция

$$\psi(m) = \frac{(\ln m)^{1/n}}{\ln\ln m} + 1$$

обладает тем свойством, что

$$\psi(m) \leqslant C_{28} \quad \text{при} \quad 3 \leqslant m \leqslant \exp\bigl\{(n \ln n)^n\bigr\},$$

откуда

$$\rho(f, m) \leqslant e^{C_{29}n}\, m^{1-1/n} \qquad \bigl(3 \leqslant m \leqslant \exp\bigl\{(n \ln n)^n\bigr\}\bigr). \tag{5.18}$$

Не исключено, что эта оценка справедлива для всех m.

СПИСОК ЛИТЕРАТУРЫ

1. *Виноградов И.М.* Метод тригонометрических сумм в теории чисел. — М.: Наука, 1971.
2. *Хуа Ло-кен.* Аддитивная теория простых чисел // Труды МИАН. 1947. Т. 22.
3. *Хуа Ло-кен.* Метод тригонометрических сумм и его применения в теории чисел. — М.: Мир, 1964.
4. *Hua Loo-keng.* Additive Primzahltheorie. — Leipzig: Teubner, 1959.
5. Суммирование некоторых рядов особого вида // *Гаусс К.Ф.* Труды по теории чисел. — М.: Изд-во АН СССР, 1959. — С. 594–635.
6. *Hardy G.H.* Collected papers V. 1. — Oxford, 1966.
7. *Weyl H.* Über die Gleichverteilung von Zahlen mod. Eines // Math. Ann. 1916. V. 77. P. 313-152; Ges. Abh. Bd. 1. — Berlin: Springer-Verlag. 1968. — S. 563–599.
8. *Landau E.* Vorlesungen über Zahlentheorie Bd. 1. — Leipzig: Hirzel, 1927.
9. *Kamke E.* Zur Arithmetik der Polynome // Math. Z. 1924. V. 19. P. 247–264.
10. *Mordell L.J.* On a sum of analogous to Gauss's sum // Quart. J. Math. 1932. V. 3. P. 161–167.
11. *Davenport H.* On certain exponential sums // J. reine und anew. Math. 1933. V. 169. P. 158–176.
12. *Hua L.K.* On an exponential sum // J. Chinese Math. Soc. 1940. V. 2. P. 301–312.
13. *Weil A.* On some exponential sums // Proc. Nat. Acad. sci. USA. 1948. V. 34, № 5. P. 204–207.
14. *Weil A.* Sur les courbes algebriques et les variétés qui s'en deduisent. — Paris: Hermann, 1948.
15. *Степанов С.А.* Об оценке рациональных тригонометрических сумм с простым знаменателем // Труды МИАН СССР. 1971. Т. 112. С. 346–371.
16. *Нечаев В.И.* О представлении натуральных чисел суммой слагаемых вида $x(x+1)\ldots(x+n-1)/n!$ // Изв. АН СССР. Сер. матем. 1953. Т. 17. С. 485–498.
17. *Карацуба А.А.* Об оценках полных тригонометрических сумм // Матем. заметки. 1967. Т. 1, вып. 2. С. 199–208.
18. *Нечаев В.А.* Оценка полной рациональной тригонометрической суммы // Матем. заметки. 1975. Т. 17, вып. 6. С. 839–849.
19. *Chen Chinq-jun.* On the representation of natural number as sum of terms of the form $x(x+1)\ldots(x+n-1)/n!$ // Acta math. sinica. 1959. V. 9, № 3. P. 264–270.
20. *Hasse H.* Theorie der höheren Differential in einem algebraischen Funktionenkörper mit vollkommenen Konstantenkörper bei beliebiger Charakterstik // J. reine und angew. Math. 1936. V. 175. P. 50–54.
21. *Hasse H., Schmidt F.K.* Noch eine Begründung der Theorie der höheren Differentialquotienten in einem algebraischen Funktionenkörper einer Unbestimmten // J. reine und angew. Math. 1937. V. 177. P. 215–237.
22. *Teichmüller O.* Differentialrechunung bei Charakteristik p // J. reine und angew. Math. 1936. V. 175. P. 89–99.
23. *Nagell T.* Introduction to number theory. — Stockholm: Almqvist und Wiksell, 1951.
24. *Виноградов И.М.* Основы теории чисел. — М.: Наука, 1972.