

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 25. Выпуск 2.

УДК 511

DOI 10.22405/2226-8383-2024-25-2-181-207

Об оценках Хуа Ло-Кэна тригонометрических сумм в полях алгебраических чисел

Х. Аль-Ассад

Хафез Аль-Ассад — Московский государственный университет им. М. В. Ломоносова (г. Москва).

e-mail: 1hbrh0@gmail.com

Аннотация

В настоящей работе дано обобщение метода Хуа Ло-Кэна оценки рациональных тригонометрических сумм с многочленом в экспоненте в алгебраических числовых полях, которые являются расширением поля рациональных чисел. В кольце целых этого алгебраического поля были рассмотрены целые и дробные идеалы. Для полной системы вычетов по любому целому идеалу Хуа Ло-Кен доказал аналог формулы Эйлера – Фурье, которая позволяет с помощью утверждения о кратности корней полиномиального сравнения по простому идеалу (“деревьев Хуа Ло-Кэна”) свести к задаче p -адического подъема решений. Последнее обстоятельство позволяет привести оценку суммы к получению оценок числа решений полиномиальных сравнений по модулю степени простого идеала. Далее, следуя оценкам Чень Джин-Руна в поле рациональных чисел, в работе найдены более точные константы для подобных оценок в алгебраических числовых полях.

Ключевые слова: Оценка Хуа Ло-Кэна, деревья Хуа Ло-Кэна, тригонометрические суммы, поля алгебраических чисел.

Библиография: 15 названий.

Для цитирования:

Х. Аль-Ассад. Об оценках Хуа Ло-Кэна тригонометрических сумм в полях алгебраических чисел // Чебышевский сборник, 2024, т. 25, вып. 2, с. 181–207.

CHEBYSHEVSKII SBORNIK

Vol. 25. No. 2.

UDC 511

DOI 10.22405/2226-8383-2024-25-2-181-207

On Hua Loo-Keng's Estimates of Exponential Sums in Algebraic Number Fields

H. Al-Assad

Hafez Al-Assad — Lomonosov Moscow State University (Moscow).

e-mail: 1hbrh0@gmail.com

Abstract

This paper provides a generalization of the Hua Loo-Keng estimation method of rational trigonometric sums with a polynomial in exponent in algebraic number fields, which are extensions of the field of rational numbers. In the ring of integers of this algebraic number field we consider integer and fractional ideals. For a complete system of residues for any integer ideal, Hua Loo-Keng proved an analogue of the Euler–Fourier formula, which, using results regarding the multiplicity of roots of a polynomial congruence modulo a prime ideal (“Hua Loo-Keng trees”), allows the problem to be reduced to the p-adic lifting of solutions, and this allows us to reduce the problem of estimating the sum to estimating the number of solutions of polynomial congruences modulo a power of a prime ideal. Furthermore, building upon Chen Jingrun’s estimates in the field of rational numbers, we obtain improved constants for similar estimates in algebraic numeric fields.

Keywords: Hua Loo-Keng’s Estimate, Hua Loo-Keng Trees, Exponential sums, Algebraic number fields.

Bibliography: 15 titles.

For citation:

H. Al-Assad, 2024, “On Hua Loo-Keng’s estimates of exponential sums in algebraic number fields”, *Chebyshevskii sbornik*, vol. 25, no. 2, pp. 181–207.

1. Введение

Рациональные тригонометрические суммы многочленов представляют собой суммы вида

$$S(f, q) = \sum_{x \bmod q} e^{2\pi i \frac{f(x)}{q}},$$

где $q \geq 1$ — рациональное целое число, и

$$f(x) = \alpha_m x^m + \dots + \alpha_1 x$$

многочлен с целыми коэффициентами, такой что $(\alpha_m, \dots, \alpha_1, q) = 1$.

Эти суммы уже давно представляют интерес из-за их глубокой связи с модулярной арифметикой в кольце вычетов по модулю q .

В частности, они возникают в методе круга Харди-Литтлвуда-Виноградова для оценки числа решений диофантовых уравнений. В частности, рассматривается разрешимость данного уравнения во-первых в действительных числах, а во-вторых, по модулю любого рационального целого q . Последняя часть обычно бывает более глубокой и трудной, и существенную роль в ней играют рациональные тригонометрические суммы; они эффективно отвечают за разрешимость по модулю q .

В 1940 г. Хуа Ло-Кен [4] нашел оптимальную оценку

$$S(f, q) = O_{m, \epsilon}(q^{1 - \frac{1}{m} + \epsilon}),$$

где $\epsilon > 0$ произвольное. Последующие работы Ченя Чжун-руна [11], [12] и Василия Нечаева [13] убрали ϵ из оценки. В 1984 г. Ци Мингао и Дин Пин [14] получили оценку

$$|S(f, q)| \leq e^{2m} q^{1 - \frac{1}{m}}.$$

В 1949 г. Хуа Ло-Кен [2] обобщил этот результат на случай поля алгебраических чисел степени d , получив оценку

$$S(f, Q) = \sum_{x \bmod Q} e^{2\pi i T(f(x))} = O_{m, \epsilon, d}(N(Q)^{1 - \frac{1}{m} + \epsilon}),$$

где T и N обозначают след и норму соответственно, Q — целый идеал, а идеал $A(f) = (\alpha_m, \dots, \alpha_1)$ удовлетворяет $A(f) = \frac{B\delta^{-1}}{Q}$, где δ — дифферента, а B — целый идеал с $(B, Q) = 1$.

В данной работе мы получим более сильный результат в случае $Q = P^l$, где P — простой идеал, в виде

$$|S(f, P^l)| \leq C_d(m) N(P)^{l(1 - \frac{1}{m})},$$

где $C_d(m)$ — константа, зависящая только от d и m .

Кроме того, мы будем использовать наш усиленный результат, чтобы убрать ϵ и вычислить константу в символе O , когда данное числовое поле имеет число классов равно 1 (т.е. кольцо целых является кольцом главных идеалов), а идеал $A(f)$ удовлетворяет условию $A(f) = \frac{B}{Q}$, для некоторых целых идеалов B и Q , где Q такой, что $(Q, \delta) = 1$.

В частности, для таких идеалов мы получаем

$$|S(f, Q)| \leq e^{\frac{5}{2}d^2(2d+1)} e^{3.442md} N(Q)^{1 - \frac{1}{m}}.$$

В другом направлении Хуа Ло-Кен в [3] (см. также [10]) использовал метод «дерева» для построения решений полиномиальных сравнений по модулю рационального простого числа, что позволило ему решить проблему сходимости особого ряда в проблеме Пруэ-Тэрри-Эскотта. Для этого он рассмотрел элемент x по модулю p^l , где p — рациональное простое число, в виде

$$x = x_1 + x_2 p + \dots + x_s p^s,$$

где $0 \leq x_j < p$ для $1 \leq j \leq s$, и использовал это представление для построения решений полиномиальных сравнений по модулю p^l .

Это позволило ему получить новую оценку вида

$$|S(f, p^l)| \leq m p^{l-h},$$

где h — положительное целое число, зависящее от делимости коэффициентов f на p .

В данной работе мы обобщим этот метод на кольцо целых полей алгебраических чисел и впоследствии получим аналогичную оценку

$$|S(f, P^l)| \leq (m-1) N(P)^{l-h}.$$

Наконец, мы объединим наши оценки, чтобы получить новую оценку в теореме 8.1.

Данная статья расширяет работу В.Н. Чубарикова в [1], опираясь преимущественно на идеи Хуа Ло-Кэна в [2], В.Н. Чубариков, А.А. Карацуба и Г.И. Архипов в [5], и Ван Юань в [6].

2. Определения и терминология

Обозначим через $\mathbb{K}$ поле алгебраических чисел с дифферентой δ и степенью d .

Обозначим R кольцо целых $\mathbb{K}$.

Обозначим функции следа и нормы $\mathbb{K}$ через

$$T(u) = \sum_{j=1}^d \sigma_j(u), \quad N(u) = \prod_{j=1}^d \sigma_j(u).$$

Определением

$$E(u) = e^{2\pi i T(u)}.$$

Для любого многочлена $f(x) = \alpha_m x^m + \dots + \alpha_1 x$ с коэффициентами из $\mathbb{K}$ обозначим $A(f) = (\alpha_m, \dots, \alpha_1)$ дробный идеал, порожденный коэффициентами f .

На протяжении всей работы P всегда будет обозначать простой идеал.

Для любого идеала Q мы определим $V_P(Q)$ как наибольшее рациональное целое такое, что $Q \in P^{V_P(Q)}$ (см., например, [8], с.438), и полагаем

$$e = V_P(\delta),$$

так что $e + 1$ — индекс ветвления P .

Обозначим через q рациональное простое число в $\mathbb{Z}$ такое, что $N(P) = q^c$, для некоторого $c \geq 1$ (см., например, [7], с.276-277).

3. Полиномиальные сравнения по модулю простого идеала

В этом разделе мы приводим результаты о числе решений полиномиальных сравнений по модулю простого идеала, аналогичны подобным результатам в случае сравнений по рациональному простому модулю.

ЛЕММА 1. ([6], с.15). Пусть $A = (\alpha_m, \dots, \alpha_0)$ — целый идеал $\mathbb{K}$, и пусть P — простой идеал такой, что $P \nmid A$.

Тогда число решений сравнения

$$f(x) = \alpha_m x^m + \dots + \alpha_1 x + \alpha_0 \equiv 0 \pmod{P},$$

учитывая их кратность, не превосходит m .

ДОКАЗАТЕЛЬСТВО. В этом доказательстве под корнем многочлена понимается корень данного многочлена по модулю P .

Докажем лемму индукцией по m .

Базовый случай $m = 1$ выполняется из-за условия $P \nmid A$ и поскольку P — простой идеал. Предположим, что лемма справедлива для $m - 1$.

Предположим, что f имеет h несравнимые корни $r_1, \dots, r_h$, так что

$$r_{j_1} \not\equiv r_{j_2} \pmod{P}, \forall j_1 \neq j_2.$$

Предположим, что r_j имеет кратность λ_j , и что $\sum_{j=1}^h \lambda_j > m$.

Без ограничения общности будем считать, что корень r_1 имеет минимальную кратность $\lambda_1 \geq 1$. Рассмотрим многочлен

$$f(x) - f(r_1) = \alpha_m (x^m - r_1^m) + \dots + \alpha_1 (x - r_1) = (x - r_1)g(x),$$

где g — многочлен степени $m - 1$ со старшим коэффициентом α_m .

Поскольку для всех $2 \leq j \leq h$ имеем

$$f(r_j) \equiv f(r_1) \equiv 0 \pmod{P}, \quad r_j \not\equiv r_1 \pmod{P},$$

тогда, поскольку P простой идеал, отсюда следует, что

$$g(r_j) \equiv 0 \pmod{P}.$$

Сначала мы покажем, что r_1 является корнем g с кратностью $\lambda_1 - 1$, причем некорень считается имеющим кратность 0.

Действительно, из определения g имеем

$$f^{(k)}(x) = (x - r_1)g^{(k)}(x) + (k - 1)g^{(k-1)}(x).$$

Если $\lambda_1 = 1$, то r_1 не является корнем f' и, следовательно, не является корнем g . В противном случае мы увидим, что для всех $k \leq \lambda_1$, r_1 является корнем $f^{(k)}$ и, следовательно, является корнем $g^{(k-1)}$. Для $k = \lambda_1 + 1$ мы знаем, что r_1 не является корнем $f^{(\lambda_1+1)}$ и поэтому не может быть корнем $g^{(\lambda_1)}$.

Таким образом, мы показали, что r_1 является корнем g кратности $\lambda_1 - 1$. Аналогичное рассуждение показывает, что r_j является корнем g кратности λ_j для $2 \leq j \leq h$.

Отсюда следует, что корни $r_1, \dots, r_h$ группы g имеют общую кратность

$$\left(\sum_{j=1}^h \lambda_j \right) - 1 > m - 1,$$

но поскольку $\deg(g) = m - 1$, то это противоречит предположению индукции. $\square$

В качестве простого, но полезного следствия из предыдущей леммы получаем следующее предложение.

PROPOSITION 1. ([6], с.15). Пусть $A = (\alpha_m, \dots, \alpha_1)$ — дробный идеал такой, что $A\delta = \frac{R}{P^l}$, где R — целый идеал, P — простой идеал такой, что $(R, P) = 1$ и $l \geq 1$ — рациональное целое число. Пусть

$$f(x) = \alpha_m x^m + \dots + \alpha_1 x.$$

Тогда число решений сравнения

$$f(x) \equiv 0 \pmod{P^{-l+1}},$$

учитывая их кратность, не превосходит m .

ЛЕММА 2. ([6], с.15). Пусть P — простой идеал, а f — многочлен с целыми коэффициентами. Пусть a — корень кратности λ сравнения $f(x) \equiv 0 \pmod{P}$.

Пусть $\pi \in R$ — целое, которое делится на P , но не делится на P^2 , и пусть v — наибольшее рациональное целое число такое, что

$$P^u | f(\pi x + a) - f(a).$$

Пусть

$$g(x) = \pi^{-u} (f(\pi x + a) - f(a)).$$

Тогда $u \leq \lambda$, и число решений сравнения

$$g(x) \equiv 0 \pmod{P},$$

учитывая их кратность, не превосходит λ .

ДОКАЗАТЕЛЬСТВО. Сначала мы покажем, что, поскольку a является корнем кратности λ сравнения $f(x) \equiv 0 \pmod{P}$, то мы можем записать f как

$$f(x) = (x - a)^\lambda h(x) + \pi_1 r(x), \quad (1)$$

для некоторого $\pi_1 \in P$, такого, что $P \nmid h(a)$ и $\deg(r) < \lambda$.

Действительно, по формуле Тейлора имеем

$$f(x) = \sum_{j=0}^m \frac{f^{(j)}(a)}{j!} (x-a)^j = (x-a)^\lambda h(x) + r_1(x), \quad (2)$$

где

$$h(x) = \sum_{j=\lambda}^m \frac{f^{(j)}(a)}{j!} (x-a)^{j-\lambda}, \quad r_1(x) = \sum_{j=0}^{\lambda-1} \frac{f^{(j)}(a)}{j!} (x-a)^j, \quad \deg(r_1) < \lambda.$$

Легко видеть, что $P \nmid h(a)$, поскольку

$$h(a) = \frac{f^{(\lambda)}(a)}{\lambda!} \not\equiv 0 \pmod{P}.$$

Более того, поскольку a имеет кратность λ , мы знаем, что существует h_1 такой, что

$$f(x) \equiv (x-a)^\lambda h_1(x) \pmod{P}. \quad (3)$$

Сравнивая (2) и (3) по модулю P , получаем

$$(x-a)^\lambda h(x) + r_1(x) \equiv (x-a)^\lambda h_1(x) \pmod{P},$$

что, поскольку $\deg(r_1) < \lambda$, означает, что $r_1(x) \equiv 0 \pmod{P}$, и поэтому r_1 можно записать как $r_1 = \pi_1 \cdot r$ для $\pi_1 \in P$, где $\deg(r) < \lambda$, что и это доказывает (1).

Следовательно, имеем

$$\begin{aligned} \pi^{-u}(f(\pi x + a) - f(a)) &= \pi^{-u}\left((\pi x)^\lambda h(\pi x + a) + \pi_1(r(\pi x + a) - r(a))\right) = \\ &= \pi^{\lambda-u} x^\lambda h(\pi x + a) + (\pi_1 \pi^{-u})(r(\pi x + a) - r(a)). \end{aligned}$$

Отсюда ясно, что $v \leq \lambda$, что и доказывает первое утверждение леммы. Более того, это показывает, что $\deg(h) \leq \lambda$, и поэтому второе утверждение леммы следует из применения леммы 3.1 к h . $\square$

4. Свойства ортогональности и мультипликативности тригонометрических сумм

В этом разделе мы приводим результаты, касающиеся свойств ортогональности и мультипликативности тригонометрических сумм, аналогичны подобным результатам в рациональном случае. Последнее позволит нам ограничить наше внимание тригонометрическими суммами над идеалами, равными степени простого идеала.

ЛЕММА 3. ([6], с.16). Пусть Q — целый идеал, а $\alpha \in R$ — целое число. Пусть η пробегает полную систему вычетов $(Q\delta)^{-1}$ по модулю δ^{-1} . Тогда

$$\sum_{\eta} E(\alpha\eta) = \sum_{\eta} e^{2\pi i T(\alpha\eta)} = \begin{cases} N(Q) & \text{если } Q|\alpha, \\ 0 & \text{если } Q \nmid \alpha. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Если $Q|\alpha$, то $\alpha\eta \in \delta^{-1}$, что дает $E(\alpha\eta) = 1$, и тогда

$$\sum_{\eta} E(\eta\alpha) = N(Q).$$

Предположим, что $Q \nmid \alpha$. Сначала мы покажем, что существует некоторый $\eta \in (Q\delta)^{-1}$, скажем η_0 , такой, что $\eta\alpha \notin \delta^{-1}$.

Если $\eta\alpha \in \delta^{-1}$ для всех $\eta \in (Q\delta)^{-1}$, то $\delta^{-1}|\alpha(Q\delta)^{-1}$, и поэтому $Q|\alpha$, что является противоречием.

По определению δ^{-1} существует целое число γ такое, что $E(\gamma\eta_0\alpha) \neq 1$. Поскольку $\gamma\eta_0 \in (Q\delta)^{-1}$, имеем

$$\sum_{\eta} E(\eta\alpha) = \sum_{\eta} E(\gamma\eta_0\alpha + \eta\alpha) = E(\gamma\eta_0\alpha) \sum_{\eta} E(\eta\alpha),$$

которые, поскольку $E(\gamma\eta_0\alpha) \neq 1$, дает

$$\sum_{\eta} E(\eta\alpha) = 0.$$

□

ЛЕММА 4. ([6], p.16). Пусть $A = (\alpha_m, \dots, \alpha_1)$, Q, Q_1, Q_2, B — целые идеалы такие, что

$$Q = Q_1 Q_2, (Q_1, Q_2) = 1, A = \frac{B\delta^{-1}}{Q}, (B, Q) = 1,$$

и пусть

$$f(x) = \alpha_m x^m + \dots + \alpha_1 x.$$

Тогда существуют многочлены

$$f_j(x) = \alpha_{m,j} x^m + \dots + \alpha_{1,j} x,$$

для $j = 1, 2$, с идеалами $A_j = (\alpha_{j,m}, \dots, \alpha_{j,1})$, такими, что существуют целые идеалы B_1, B_2 с

$$A_1 = \frac{B_1\delta^{-1}}{Q_1}, A_2 = \frac{B_2\delta^{-1}}{Q_2}, (B_1, Q_1) = (B_2, Q_2) = 1,$$

и так, что

$$S(f, Q) = S(f_1, Q_1)S(f_2, Q_2).$$

ДОКАЗАТЕЛЬСТВО. Поскольку $(Q_1, Q_2) = 1$, то существуют целые числа k_1, k_2 такие, что

$$(k_1, Q) = Q_1, (k_2, Q) = Q_2.$$

Полагая $k = \lambda_1 k_1 + \lambda_2 k_2$, мы видим по китайской теореме об остатках, что при пробегании λ_1, λ_2 по полным системам вычетов по модулю Q_1, Q_2 соответственно, k пробегает полную систему вычетов по модулю Q .

Следовательно, имеем

$$S(f, Q) = \sum_{k \bmod Q} E(f(k)) = \sum_{\lambda_1 \bmod Q_1} \sum_{\lambda_2 \bmod Q_2} E(f(\lambda_1 k_1 + \lambda_2 k_2)) =$$

$$= \sum_{\lambda_1 \bmod Q_1} E(f(\lambda_1 k_1)) \sum_{\lambda_2 \bmod Q_2} E(f(\lambda_2 k_2)) = S(f_1, Q_1) S(f_2, Q_2),$$

где $f_j(k) = f(kk_j)$. Утверждение об идеалах B_1 и B_2 очевидно. $\square$

5. Метод деревьев Хуа Ло-Кена для тригонометрических сумм по идеалам, равным степени простого идеала

В этом разделе мы представляем обобщение метода деревьев Хуа Ло-Кена, на основе [1], и получаем соответствующую оценку тригонометрических сумм по идеалам, равным степени простого идеала. Мы также представим результаты по тригонометрическим суммам, которые будут использоваться в последующих разделах.

Благодаря теореме об уникальной факторизации идеалов в полях алгебраических чисел, лемма 4.2 позволяет нам ограничить наши рассмотрения идеалами, равными степени простого идеала, поскольку любой целый идеал может быть однозначно выражен как произведение таких идеалов.

Таким образом, в остальной части работы, пусть $A(f) = (\alpha_m, \dots, \alpha_1)$ — дробный идеал такой, что

$$A = \frac{B\delta^{-1}}{P^l}; (B, P) = 1 \quad (4)$$

где B — целый идеал, P — простой идеал, и $l \geq 1$ — рациональное целое число.

Более того, π всегда обозначает элемент R такой, что $\pi \in P, \pi \notin P^2$ (см., например, [8], с.441).

Пусть

$$f(x) = \alpha_m x^m + \dots + \alpha_1 x.$$

Будем рассматривать полные тригонометрические суммы

$$S(f, P^l) = \sum_{x \bmod P^l} E(f(x)).$$

Пусть t — наибольшее рациональное целое число такое, что $P^t | A(f')A(f)^{-1}$. Поскольку $A(f) | A(f')$, имеем $t \geq 0$.

Очевидно, что каждый $x \bmod P^l$ однозначно выражается как $x = y + \pi^{l-t-1}z$ для $y \bmod P^{l-t-1}, z \bmod P^{t+1}$, и поэтому имеем

$$S(f, P^l) = \sum_{y \bmod P^{l-t-1}} \sum_{z \bmod P^{t+1}} E(f(y + \pi^{l-t-1}z)) = \sum_{v \bmod P} S_v, \quad (5)$$

где

$$S_v = \sum_{\substack{y \bmod P^{l-t-1} \\ y \equiv v \bmod P}} \sum_{z \bmod P^{t+1}} e^{2\pi i T(f(y + \pi^{l-t-1}z))}.$$

ЛЕММА 5. ([1], с.9). Если $l \geq 2(t+1)$, и v не является решением сравнения $\pi^{l-t}f'(v) \equiv 0 \bmod P$, то

$$S_v = 0.$$

ДОКАЗАТЕЛЬСТВО. Используя формулу Тейлора, получаем

$$f(y + \pi^{l-t-1}z) = \sum_{j=0}^m \frac{f^{(j)}(y)}{j!} (\pi^{l-t-1}z)^j \equiv f(y) + \pi^{l-t-1}zf'(y) \pmod{P^{l-t}},$$

что, поскольку $l \geq 2(t+1)$, дает

$$\begin{aligned} S_v &= \sum_{\substack{y \pmod{P^{l-t-1}} \\ y \equiv v \pmod{P}}} \sum_{z \pmod{P^{t+1}}} e^{2\pi i T(f(y) + \pi^{l-t-1}zf'(y))} = \\ &= \sum_{\substack{y \pmod{P^{l-t-1}} \\ y \equiv v \pmod{P}}} e^{2\pi i T(f(y))} \sum_{z \pmod{P^{t+1}}} e^{2\pi i T(\pi^{l-t}f'(v)\pi^{-1}z)}. \end{aligned}$$

Применение леммы 4.1 к внутренней сумме дает

$$\sum_{z \pmod{P^{t+1}}} e^{2\pi i T(\pi^{l-t}f'(v)\pi^{-1}z)} = 0 \implies S_v = 0.$$

□

Для каждого решения v сравнения $\pi^{l-t}f'(v) \equiv 0 \pmod{P}$ положим

$$\tilde{f}_1(y) = f(y+v) - f(v) = \sum_{j=1}^m \tilde{\alpha}_{j,1} y^j.$$

Тогда имеем тождества

$$\tilde{\alpha}_{j,1} = \sum_{l=0}^{m-j} \alpha_{j+l} \binom{j+l}{j} v^l; 1 \leq j \leq m. \quad (6)$$

Определим теперь

$$f_1(y) = \tilde{f}_1(\pi y) = \sum_{j=1}^m \pi^j \tilde{\alpha}_{j,1} y^j = \sum_{j=1}^m \alpha_{j,1} y^j, \quad (7)$$

и определим индекс $u = u(v)$ как наибольшее рациональное целое число такое, что $P^u | A(f_1)A(f)^{-1}$.

Из (6) ясно, что $A(f)|A(f_1)$, и поэтому $u \geq 0$. Более того, из определения u следует, что

$$A(f_1) = \frac{B_1 \delta^{-1}}{P^{l-u}}; (B_1, P) = 1$$

для какого-то целого идеала B_1 .

ЛЕММА 6. ([1], с. 9). Если $l \geq 2(t+1)$, тогда

$$S(f, P^l) = \sum_v' N(P^{u-1}) E(f(v)) S(f_1, P^{l-u}),$$

где апостроф означает, что суммирование ведется по решениям сравнения $\pi^{l-t}f'(v) \equiv 0 \pmod{P}$ в полной системы вычетов по модулю P .

ДОКАЗАТЕЛЬСТВО. Если v является решением сравнения $\pi^{l-t}f'(v) \equiv 0 \pmod{P}$, тогда

$$\begin{aligned}
S_v &= \sum_{\substack{y \pmod{P^{l-t-1}} \\ y \equiv v \pmod{P}}} \sum_{z \pmod{P^{t+1}}} E(f(y + \pi^{l-t-1}z)) = \\
&= \sum_{\substack{y \pmod{P^{l-t-1}} \\ y \equiv v \pmod{P}}} E(f(y)) \sum_{z \pmod{P^{t+1}}} E(f(y + \pi^{l-t-1}z) - f(y)) = \\
&= \sum_{\substack{y \pmod{P^{l-t-1}} \\ y \equiv v \pmod{P}}} E(f(y)) \sum_{z \pmod{P^{t+1}}} E(\pi^{l-t-1}f'(y)z) = \\
&= N(P^{t+1}) \sum_{\substack{y \pmod{P^{l-t-1}} \\ y \equiv v \pmod{P}}} E(f(y)) = N(P^{t+1})E(f(v)) \sum_{y \pmod{P^{l-t-2}}} E(f(\pi y + v) - f(v)) = \\
&= N(P^{t+1})E(f(v)) \sum_{y \pmod{P^{l-t-2}}} E(f_1(y)) = N(P^{u-1})E(f(v))S(f_1, P^{l-u}).
\end{aligned}$$

Если v не является решением сравнения $\pi^{l-t}f'(v) \equiv 0 \pmod{P}$, то лемма 5.1 дает $S_v = 0$, и тогда утверждение леммы следует от (5). $\square$

Определим w как наибольшее рациональное целое число такой, что $P^w | k$ для некоторого $1 \leq k \leq m$. В лемме 6.2 мы покажем, что

$$w = (e + 1) \left\lfloor \frac{\ln m}{\ln q} \right\rfloor.$$

Следующая конструкция является обобщением метода Хуа Ло-Кена.

Полагая $f_0 = f$ и $u_1(v_0) = u(v)$, мы индуктивно определяем функции f_k и индексы $u_k = u_k(v_{k-1})$ аналогично построению f_1 и $u(v)$ перед леммой 5.2.

Предположим, что для $k \geq 1$

$$f_{k-1}(y) = \alpha_{m,k-1}y^m + \dots + \alpha_{1,k-1}y; \quad A(f_{k-1}) = \frac{B_{k-1}\delta^{-1}}{P^{l-u_1-\dots-u_{k-1}}} \quad (8)$$

уже определена, где B_{k-1} — целый идеал такой, что $(B_{k-1}, P) = 1$, и пусть t_{k-1} — наибольшее рациональное целое число такое, что $P^{t_{k-1}} | A(f'_{k-1})A(f_{k-1})^{-1}$.

Поскольку $A(f_{k-1}) | A(f'_{k-1})$, имеем $t_{k-1} \geq 0$.

Для каждого решения v_{k-1} сравнения

$$\pi^{l-u_1-\dots-u_{k-1}-t_{k-1}} f'_{k-1}(x) \equiv 0 \pmod{P},$$

положим

$$\tilde{f}_k(y) = f_{k-1}(y + v_{k-1}) - f_{k-1}(v_{k-1}) = \sum_{j=1}^m \tilde{\alpha}_{j,k} y^j.$$

Тогда имеем тождества

$$\tilde{\alpha}_{j,k} = \sum_{l=0}^{m-j} \alpha_{j+l,k-1} \binom{j+l}{j} v_{k-1}^l. \quad (9)$$

Определим теперь

$$f_k(y) = \tilde{f}_k(\pi y) = \sum_{j=1}^m \pi^j \tilde{\alpha}_{j,k} y^j = \sum_{j=1}^m \alpha_{j,k} y^j, \quad (10)$$

и определим индекс $u_k = u_k(v_{k-1})$ как наибольшее рациональное целое число такое, что $P^{u_k} | A(f_k) A(f_{k-1})^{-1}$.

От (9) следует, что $A(f_{k-1}) | A(f_k)$, и поэтому $u_k \geq 0$. Более того, из определения u_k следует, что

$$A(f_k) = \frac{B_k \delta^{-1}}{P^{l-u_1-\dots-u_k}}. \quad (11)$$

Для удобства положим

$$U_k = \sum_{j=1}^k u_j, \quad l_k = l - U_k, \quad l_0 = l.$$

Повторяем эту конструкцию до шага с номером h , который определяется условиями

$$l - U_{h-1} \geq 2(w+1), \quad l - U_h < 2(w+1).$$

PROPOSITION 2. Для $1 \leq k \leq h-1$, имеем неравенство

$$t_k \leq w.$$

ДОКАЗАТЕЛЬСТВО. По построению мы знаем, что

$$A(f_k) = \frac{B_k \delta^{-1}}{P^{l_k}},$$

для некоторого целого идеала B_k с $(B_k, P) = 1$, и поэтому $V_P(A(f_k)) = -l_k - e$.

По определению w мы видим, что

$$V_P(A(f'_k)) \leq w + V_P(A(f_k)) = w - l_k - e \implies w \geq l_k + V_P(A(f'_k)) = t_k.$$

□

ТЕОРЕМА 1. Если $h > 0$, то

$$S(f, P^l) = \sum'_{v_0, \dots, v_{h-1}} N(P^{U_h-h}) E(f_0(v_0) + \dots + f_{h-1}(v_{h-1})) S(f_h, P^{l-U_h}).$$

где апостроф означает, что суммирование ведется по решениям сравнений $\pi^{l_k-t_k} f'_k(v_k) \equiv 0 \pmod{P}$, для $0 \leq k \leq h-1$, в полной системы вычетов по модулю P .

ДОКАЗАТЕЛЬСТВО. Докажем утверждение теоремы повторным применением леммы 5.2.

Поскольку $h > 0$, имеем $l \geq 2(w+1)$, и поэтому для $1 \leq k \leq h-1$ имеем $w \geq t_k$ по предложению 5.1, что по определению h показывает, что $l_k \geq 2(t_k+1)$.

Следовательно, индуктивно, для $1 \leq k \leq h-1$ предположим, что имеем

$$S(f, P^l) = \sum'_{v_0, \dots, v_{k-1}} N(P^{U_k-k}) E(f_0(v_0) + \dots + f_{k-1}(v_{k-1})) S(f_k, P^{l-U_k}).$$

Поскольку $l_k \geq 2(t_k+1)$, то можем применить лемму 5.2 и получить

$$S(f_k, P^{l-U_k}) = \sum_{v_k}^I N(P^{u_{k+1}-1}) E(f_k(v_k)) S(f_{k+1}, P^{l-U_{k+1}}).$$

□

ЛЕММА 7. *Количество наборов индексов $\{u_1, \dots, u_h\}$ не превосходит $m - 1$.*

ДОКАЗАТЕЛЬСТВО. Пусть $\{v_{0,j_0}\}_{j_0=1}^{J_0}$ — множество несравнимых решений сравнения $\pi^{l-t} f'_0(x) \equiv 0 \pmod{P}$, где v_{0,j_0} имеет кратность λ_{0,j_0} . По предложению 3.1 мы знаем, что

$$\sum_{j_0=1}^{J_0} \lambda_{0,j_0} \leq m - 1.$$

Теперь для каждого v_{0,j_0} пусть, $\{v_{1,j_0,j_1}\}_{j_1=1}^{J_1(j_0)}$ — множество несравнимых решений сравнения $\pi^{l_1-t_1} f'_1(x) \equiv 0 \pmod{P}$, где v_{1,j_0,j_1} имеет кратность λ_{1,j_0,j_1} .

Индуктивно предположим, что

$$\sum_{j_0=1}^{J_0} \cdots \sum_{j_{k-1}=1}^{J_{k-1}(j_0, \dots, j_{k-2})} \lambda_{k-1, j_0, \dots, j_{k-1}} \leq m - 1. \quad (12)$$

По лемме 3.2 мы знаем, что

$$\sum_{j_k=1}^{J_k(j_0, \dots, j_{k-1})} \lambda_{k, j_0, \dots, j_k} \leq \lambda_{k-1, j_0, \dots, j_{k-1}}. \quad (13)$$

Следовательно, по (12) и (13) имеем

$$\sum_{j_0=1}^{J_0} \cdots \sum_{j_k=1}^{J_k(j_0, \dots, j_{k-1})} \lambda_{k, j_0, \dots, j_k} \leq \sum_{j_0=1}^{J_0} \cdots \sum_{j_{k-1}=1}^{J_{k-1}(j_0, \dots, j_{k-2})} \lambda_{k-1, j_0, \dots, j_{k-1}} \leq m - 1.$$

По индукции мы видим, что

$$\sum_{j_0=1}^{J_0} \sum_{j_1=1}^{J_1(j_0)} \cdots \sum_{j_{h-1}=1}^{J_{h-1}(j_0, \dots, j_{h-2})} \lambda_{h-1, j_0, \dots, j_{h-1}} \leq m - 1,$$

а поскольку $\lambda_{h-1, j_0, \dots, j_{h-1}} \geq 1$, количество множеств $\{v_{0,j_0}, \dots, v_{h-1, j_0, \dots, j_{h-1}}\} = \{v_0, \dots, v_{h-1}\}$ не превосходит $m - 1$, что эквивалентно утверждению леммы, по определению u_k . □

PROPOSITION 3. *Имеем*

$$\{j; V_P(\pi^{l_{k-1}+e} \tilde{\alpha}_{j,k}) = 0\} \neq \emptyset, \quad \{j; V_P(\pi^{l_k+e} \alpha_{j,k}) = 0\} \neq \emptyset.$$

ДОКАЗАТЕЛЬСТВО. Имеем

$$\alpha_{j,k} \in A(f_k) \implies A(f_k) | \alpha_{j,k} \implies V_P(\alpha_{j,k}) \geq V_P(A(f_k)) = -l_k - e. \quad (14)$$

Поскольку $V_P(A(f_{k-1})) = -l_{k-1} - e$, то не может быть, что $V_P(\alpha_{j,k-1}) > -l_{k-1} - e$ для всех $1 \leq j \leq m$.

Поэтому, по (14) (для $k - 1$), можем положить $s' = \max \{j; V_P(\alpha_{j,k-1}) = -l_{k-1} - e\}$, и тогда (9) дает

$$V_P(\tilde{\alpha}_{s',k}) = V_P(\alpha_{s',k-1}) = -l_{k-1} - e \implies V_P(\pi^{l_{k-1}+e}\tilde{\alpha}_{s',k}) = 0,$$

что показывает, что первое множество в утверждении теоремы непусто.

Аналогично, поскольку $V_P(A(f_k)) = -l_k - e$, то не может быть, что $V_P(\alpha_{j,k}) > -l_k - e$ для всех $1 \leq j \leq m$.

Применяя (14) видим, что мы можем положить $r' = \max\{j; V_P(\alpha_{j,k}) = -l_k - e\}$, и тогда

$$V_P(\pi^{l_k+e}\alpha_{r,k}) = 0,$$

что показывает, что второе множество в утверждении теоремы непусто. $\square$

ЛЕММА 8. *Имеем цепочку неравенств*

$$m \geq u_1 \geq \dots \geq u_h \geq 2.$$

ДОКАЗАТЕЛЬСТВО. Сначала мы докажем, что $m \geq u_k \geq u_{k+1}$ для $1 \leq k \leq h-1$.

По предположению 5.2, пусть

$$s = \max\{j; V_P(\pi^{l_{k-1}+e}\tilde{\alpha}_{j,k}) = 0\},$$

тогда ясно, что $m \geq s$, и по (10) имеем

$$\pi^s(\pi^{l_{k-1}+e}\tilde{\alpha}_{s,k}) = \pi^{l_{k-1}+e}\alpha_{s,k}. \quad (15)$$

По определению s , (14) и (15) имеем

$$\begin{aligned} s &= V_P(\pi^s(\pi^{l_{k-1}+e}\tilde{\alpha}_{s,k})) = V_P(\pi^{l_{k-1}+e}\alpha_{s,k}) = l_{k-1} + e + V_P(\alpha_{s,k}) = \\ &= l_{k-1} + e - l_k - e = u_k, \end{aligned}$$

что дает

$$m \geq s \geq u_k. \quad (16)$$

Теперь, снова по предположению 5.2, пусть

$$r = \max\{j; V_P(\pi^{l_k+e}\alpha_{j,k}) = 0\},$$

и тогда (10) дает

$$\pi^r(\pi^{l_k+e}\tilde{\alpha}_{r,k}) = \pi^{l_k+e}\alpha_{r,k}. \quad (17)$$

Кроме того, согласно (9) имеем

$$\tilde{\alpha}_{j,k} \in A(f_{k-1}) \implies A(f_{k-1})|\tilde{\alpha}_{j,k} \implies V_P(\tilde{\alpha}_{j,k}) \geq V_P(A(f_{k-1})) = -l_{k-1} - e. \quad (18)$$

По определению r и (17), применяя (18) с $j = r$ дает

$$\begin{aligned} 0 &= V_P(\pi^{l_k+e}\alpha_{r,k}) = V_P(\pi^{l_k+e+r}\tilde{\alpha}_{r,k}) = l_k + e + r + V_P(\tilde{\alpha}_{r,k}) \geq \\ &\geq l_k + e + r - l_{k-1} - e = r - u_k \implies u_k \geq r. \end{aligned} \quad (19)$$

По (9) имеем тождество

$$\tilde{\alpha}_{r,k+1} = \sum_{l=0}^{m-j} \alpha_{r+l,k} \binom{r+l}{r} v_k^l,$$

итак, по определению r (в частности, его максимальность) это показывает, что $V_P(\pi^{l_k+e}\tilde{\alpha}_{r,k+1}) = 0$, что согласно (17) дает

$$\begin{aligned} r &= V_P(\pi^r(\pi^{l_k+e}\tilde{\alpha}_{r,k+1})) = V_P(\pi^{l_k+e}\alpha_{r,k+1}) = l_k + e + V_P(\alpha_{r,k+1}) \geq \\ &\geq l_k + e - l_{k+1} - e = u_{k+1} \implies r \geq u_{k+1}. \end{aligned} \quad (20)$$

В силу (16), (19) и (20) имеем цепочку неравенств

$$m \geq s \geq u_k \geq r \geq u_{k+1}. \quad (21)$$

Теперь мы покажем, что $u_k \geq 2$.

Мы знаем из (10) и (11), что

$$u_k = r' + V_P(\tilde{\alpha}_{r',k}) + l_{k-1} + e,$$

где

$$r' + V_P(\tilde{\alpha}_{r',k}) = \min \{j + V_P(\tilde{\alpha}_{j,k}); 1 \leq j \leq m\}.$$

Из (9) и 14 (при $k-1$) сразу видно, что

$$V_P(\tilde{\alpha}_{j,k}) \geq V_P(A(f_{k-1})) = -l_{k-1} - e,$$

так что если $r' \geq 2$, то будем иметь

$$u_k = r' + V_P(\tilde{\alpha}_{r',k}) + l_{k-1} + e \geq r' \geq 2. \quad (22)$$

Если $r' = 1$, тогда знаем, что

$$\tilde{\alpha}_{1,k} = f'_{k-1}(v_{k-1}) \implies V_P(\tilde{\alpha}_{1,k}) \geq 1 - l_{k-1},$$

что дает

$$u_k = 1 + V_P(\tilde{\alpha}_{1,k}) + l_{k-1} + e \geq 2 + e \geq 2. \quad (23)$$

Заметим, что (22) и (23) показывают, что $u_k \geq 2$, что вместе с (21) завершает доказательство леммы. $\square$

ТЕОРЕМА 2. *Справедлива оценка*

$$|S(f, P^l)| \leq (m-1)N(P^{l-h}).$$

ДОКАЗАТЕЛЬСТВО. Если $l < 2(w+1)$, то $h = 0$ и утверждение теоремы тривиально. Предположим, что $l \geq 2(w+1)$, и тогда $h > 0$.

Применяя теорему 5.1, видим, что

$$S(f, P^l) = \sum_{v_0, \dots, v_{h-1}} N(P^{U_h-h}) E(f_0(v_0) + \dots + f_{h-1}(v_{h-1})) S(f_h, P^{l-U_h}).$$

По лемме 5.3 мы знаем, что количество наборов $\{u_1, \dots, u_k\}$ не превосходит $m-1$, что вместе с тривиальными оценками $|S(f_h, P^{l-U_h})| \leq N(P^{l-U_h})$ и $|E(x)| = 1$ дает

$$|S(f, P^l)| \leq (m-1)N(P^{U_h-h})N(P^{l-U_h}) = (m-1)N(P^{l-h}).$$

$\square$

6. Усиленная форма оценки Хуа Ло-Кэна в случае идеала, равного степени простого идеала

В этом разделе мы представляем более сильную форму оценки Хуа Ло-Кэна [2] в случае идеала, равного степени простого идеала, основываясь на [5], глава 2 (оригинальная работа в [11]). Начнем с представления некоторых вспомогательных результатов.

PROPOSITION 4. ([5], с.56). Пусть $N > 1$ – вещественное число, а $k, r, \lambda_1, \dots, \lambda_r$ – рациональные целые числа такие, что $1 \leq r \leq k$ и $\lambda_1, \dots, \lambda_r > 0$. Тогда

$$\max_{\lambda_1 + \dots + \lambda_r = k} \sum_{j=1}^r N^{\lambda_j} \leq \max(kN, N^k).$$

ДОКАЗАТЕЛЬСТВО. Для $\lambda' \geq \lambda \geq 1$, поскольку $N > 1$, имеем

$$(N^{\lambda'} - N)(N^{\lambda-1} - 1) > 0 \implies N^{\lambda'+\lambda-1} + N \geq N^{\lambda'} + N^{\lambda}.$$

Следовательно, имеем

$$\sum_{j=1}^r N^{\lambda_j} \leq N^{\lambda_1+\lambda_2-1} + \sum_{j=3}^r N^{\lambda_j} + N,$$

и повторное применение этого рассуждения дает

$$\sum_{j=1}^r N^{\lambda_j} \leq N^{\lambda_1+\dots+\lambda_r-r+1} + (r-1)N,$$

что дает оценку

$$\max_{\lambda_1+\dots+\lambda_r=k} \sum_{j=1}^r N^{\lambda_j} \leq N^{k-r+1} + (r-1)N = h(r).$$

Так как $N > 1$, то $h''(r) = N^{k-r+1}(\ln N)^2 > 0$, и поэтому в отрезке $[1, k]$ у нас есть

$$\max_{\lambda_1+\dots+\lambda_r=k} \sum_{j=1}^r N^{\lambda_j} \leq \max(h(1), h(k)) = \max(kN, N^k).$$

□

ЛЕММА 9. Если $q > m$, то $t = 0$.

ДОКАЗАТЕЛЬСТВО. Предположим, $(\alpha_j) = \frac{B_j}{P^{s_j}}$, где B_j – дробный идеал такой, что $V_P(B_j) = 0$. Тогда у нас есть

$$A(f) = \sum_{j=1}^m \frac{B_j}{P^{s_j}}. \quad (24)$$

По дистрибутивному свойству сложения идеалов мы можем сгруппировать равные степени P в (24), что дает

$$A(f) = \sum_{j=1}^{m'} \frac{\tilde{B}_j}{P^{r_j}}; \quad \tilde{B}_j = \sum_{k; V_P(\alpha_k) = -r_j} B_k,$$

где рациональные целые числа $r_1 > \dots > r_{m'}$ — разные элементы набора индексов $\{s_j\}_{j=1}^m$. Покажем, что $V_P(\tilde{B}_j) = 0$.

Если $V_P(\tilde{B}_j) = V \neq 0$, то для каждого $1 \leq k \leq m$ пишем $B_k = \frac{C_k}{D_k}$, где C_k, D_k — целые идеалы с $(C_k, D_k) = 1$. Теперь, поскольку $V_P(B_k) = 0$, имеем $V_P(D_k) = 0$. Определим целый идеал

$$\tilde{D}_k = \prod_{k'; V_P(\alpha_{k'}) D_{k'} = -r_j, k' \neq k} \implies V_P(\tilde{D}_k) = 0.$$

Ясно, что

$$\tilde{B}_j \prod_{k; V_P(\alpha_k) = -r_j} D_k = \sum_{k; V_P(\alpha_k) = -r_j} C_k \tilde{D}_k,$$

и поэтому

$$\begin{aligned} V_P(\tilde{B}_j) = V &\implies V_P(\tilde{B}_j \prod_{k; V_P(\alpha_k) = -r_j} D_k) = V \implies \\ &\implies V_P(\sum_{k; V_P(\alpha_k) = -r_j} C_k \tilde{D}_k) = V \implies V > 0 \end{aligned}$$

поскольку $\sum_{k; V_P(\alpha_k) = -r_j} C_k \tilde{D}_k$ — целый идеал.

Кроме того, имеем

$$\begin{aligned} V_P(\sum_{k; V_P(\alpha_k) = -r_j} C_k \tilde{D}_k) = V &\implies \sum_{k; V_P(\alpha_k) = -r_j} C_k \tilde{D}_k \subseteq P^V \implies \\ &\implies C_k \tilde{D}_k \subseteq P^V \implies V_P(C_k \tilde{D}_k) \geq V, \end{aligned}$$

что является противоречием тому, что $V_P(C_k) = V_P(\tilde{D}_k) = 0$.

Следовательно, имеем $V_P(\tilde{B}_j) = 0$ и тогда

$$V_P(A(f)) = -r_1. \quad (25)$$

Мы знаем, что

$$A(f') = \sum_{j=1}^m \frac{j B_j}{P^{s_j}},$$

и аналогично (24) запишем

$$A(f) = \sum_{j=1}^{m'} \frac{\tilde{B}_j}{P^{r_j}}; \quad \tilde{B}_j = \sum_{k; V_P(\alpha_k) = -r_j} k B_k.$$

Так как $q > m$ и q — рациональное простое число в $\mathbb{Z}$, то $(k, q) = 1$ для всех $1 \leq k \leq m$, откуда следует, что $(k, P) = 1$, и поэтому $(k B_k, P) = 1$.

Аналогично видим, что $V_P(\tilde{B}_j) = 0$ и, следовательно, что

$$V_P(A(f')) = -r_1. \quad (26)$$

Таким образом, согласно (25) и (26), по определению t имеем

$$V_P(A(f)) = V_P(A(f')) \implies t = 0.$$

□

ЛЕММА 10. *Справедливо тождество*

$$w = (e + 1) \left\lfloor \frac{\ln m}{\ln q} \right\rfloor.$$

ДОКАЗАТЕЛЬСТВО. Мы знаем (см., например, [8], с.427), что

$$P \cap \mathbb{Z} = (q),$$

и что

$$q = P^{e+1}Q; (Q, P) = 1 \implies q \in P^{e+1}, q \notin P^{e+2},$$

для некоторого целого идеала Q , и тогда $V_P(q) = e + 1$.

Рассмотрим рациональное целое число k с $1 \leq k \leq m$. Запишем $k = q^{r(k)}k'$, где $(k', q) = 1$, и тогда имеем

$$V_P(k) = V_P(q^{r(k)}) + V_P(k') = V_P(q^{r(k)}) = r(k)V_P(q) = r(k)(e + 1). \quad (27)$$

Легко видеть, что

$$\max \{r(k); 1 \leq k \leq m\} = \left\lfloor \frac{\ln m}{\ln q} \right\rfloor,$$

откуда, вместе с (27), непосредственно следует утверждение леммы. $\square$

ТЕОРЕМА 3. Пусть $N(P) = q^c$, где $c \geq 1$ рациональное целое число. Справедлива общая оценка

$$|S(f, P^l)| \leq C_d(m)N(P)^{l(1-\frac{1}{m})},$$

где

$$C_d(m) = \begin{cases} m^d & \text{если } q > m, N(P) \geq (m-1)^{\frac{m}{m-2}}, \\ \frac{m-1}{m} m^{\frac{3}{m}} & \text{если } q > m, N(P) \leq (m-1)^{\frac{m}{m-2}}, \\ m^{\frac{d(2d+1)}{m}} & \text{если } q \leq m, N(P) \geq (m-1)^{\frac{m}{m-2}}, \\ (m-1)m^{\frac{d(2d+1)}{m}} & \text{если } q \leq m, N(P) \leq (m-1)^{\frac{m}{m-2}}. \end{cases}$$

Более того, справедлива конкретная оценка

$$|S(f, P^l)| \leq C_d(m, P)N(P)^{l(1-\frac{1}{m})},$$

где

$$C_d(m, P) = \begin{cases} m^d & \text{если } q > m, N(P) \geq (m-1)^{\frac{m}{m-2}}, \\ \frac{m-1}{m} m^{\frac{3}{m}} & \text{если } q > m, N(P) \leq (m-1)^{\frac{m}{m-2}}, \\ m^{\frac{c(2e+3)}{m}} & \text{если } q \leq m, N(P) \geq (m-1)^{\frac{m}{m-2}}, \\ (m-1)m^{\frac{c(2e+3)}{m}} & \text{если } q \leq m, N(P) \leq (m-1)^{\frac{m}{m-2}}. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Сначала мы докажем конкретную оценку, а затем из нее выведем общую оценку.

Для удобства положим $N = N(P)$. Мы рассматриваем несколько случаев. Во всех случаях доказательство будет проводиться индукцией по l .

Случай 1. $q > m$:

По лемме 6.2 имеем $t = 0$. Если $l < 2(t + 1)$, то $l = 1$, и лемма следует из оценки Морделла ([6], с.17, а оригинальная работа в [15]).

$$|S(f, P)| \leq m^d N^{1-\frac{1}{m}}. \quad (28)$$

Предположим, что $l \geq 2$. Пусть $v_1, \dots, v_r$ — несравнимые решения сравнения $\pi^l f'(v) \equiv 0 \pmod{P}$ такие, что v_j имеет кратность λ_j , и пусть $\sum_{j=1}^r \lambda_j = n$. Далее, обозначим через $\sigma_j = u(v_j)$ индексы в конструкции после леммы 5.1.

Используя разложение в ряд Тейлора

$$g_j(y) = f(\pi y + v_j) - f(v_j) = \sum_{k=1}^m \frac{\pi^k y^k}{k!} f^{(k)}(v_j),$$

лемму 3.2 и (11), видим, что

$$V_P \left(\frac{\pi^{\lambda_j+1}}{(\lambda_j+1)!} \pi^{l+e} f^{(\lambda_j+1)}(v_j) \right) \leq \lambda_j + 1 \implies \sigma_j \leq \lambda_j + 1. \quad (29)$$

По лемме 3.1 мы знаем, что

$$n \leq m - 1. \quad (30)$$

Применение неравенства треугольника к (5) дает

$$|S(f, P^l)| \leq \sum_{j=1}^r |S_{v_j}|. \quad (31)$$

Если $l > \sigma_j$, то в доказательстве леммы 5.2 было показано, что

$$|S_{v_j}| = N^{\sigma_j-1} |S(g_j, P^{l-\sigma_j})|. \quad (32)$$

Случай 1а. $N \geq (m-1)^{\frac{m}{m-2}}$:

По (28) и предположению индукции в (32), имеем

$$|S_{v_j}| \leq m^d N^{\sigma_j-1} N^{(l-\sigma_j)(1-\frac{1}{m})}, \quad (33)$$

причем эта оценка верна и в том случае, если $\sigma_j \geq l$, так как в этом случае она следует из тривиальной оценки $|S_{v_j}| \leq N^{l-1}$.

Следовательно, по (31) и (33), получаем

$$\begin{aligned} |S(f, P^l)| &\leq m^d \sum_{j=1}^r N^{\sigma_j-1} N^{(l-\sigma_j)(1-\frac{1}{m})} = \\ &= m^d N^{l(1-\frac{1}{m})} \sum_{j=1}^r N^{-1+\frac{\sigma_j}{m}}. \end{aligned} \quad (34)$$

Поскольку по (29) и лемма 3.1 имеем $\sigma_j \leq \lambda_j + 1 \leq m$, то предложение 6.1 дает

$$\sum_{j=1}^r N^{-1+\frac{\sigma_j}{m}} \leq N^{-1+\frac{1}{m}} \sum_{j=1}^r N^{\frac{\lambda_j}{m}} \leq N^{-1+\frac{1}{m}} \max((m-1)N^{\frac{1}{m}}, N^{1-\frac{1}{m}}). \quad (35)$$

Легко видеть, что

$$N \geq (m-1)^{\frac{m}{m-2}} \implies \max((m-1)N^{\frac{1}{m}}, N^{1-\frac{1}{m}}) = N^{1-\frac{1}{m}}. \quad (36)$$

Подстановка (35) и (36) в (34) дает

$$\sum_{j=1}^r N^{-1+\frac{\sigma_j}{m}} \leq 1 \implies |S(f, P^l)| \leq m^d N^{l(1-\frac{1}{m})},$$

что и доказывает утверждение теоремы в данном случае.

Случай 16. $N \leq (m-1)^{\frac{m}{m-2}}$:

Сначала докажем оценку

$$|S(f, P^l)| \leq n N^{-1+\frac{3}{m}} N^{l(1-\frac{1}{m})}. \quad (37)$$

По определению сразу видно, что $r \leq n$, поэтому базовый случай $l = 2$ следует из тривиальной оценки

$$|S(f, P^2)| \leq \sum_{j=1}^r |S_{v_j}| \leq r N \leq n N^{1+\frac{1}{m}}.$$

Предполагая, что (37) справедлива для всех $2 \leq l \leq L$, мы докажем, что она справедлива для $l = L + 1$.

По определению σ_j и поскольку в силу (29) имеем $\sigma_j \leq \lambda_j + 1$, мы видим, что

$$g_j(y) \equiv \sum_{k=1}^{\lambda_j+1} \frac{\pi^k y^k}{k!} f^{(k)}(v_j) \bmod P,$$

и значит, по лемме 3.1 число решений сравнения $\pi^{l-\sigma_j} g'_j(y) \equiv 0 \bmod P$ не превосходит λ_j .

Если $\sigma_j < L$, то предположение индукции дает

$$\begin{aligned} |S_{v_j}| &= N^{\sigma_j-1} |S(g_j, P^{L+1-\sigma_j})| \leq \lambda_j N^{\sigma_j-2+\frac{3}{m}+(L+1-\sigma_j)(1-\frac{1}{m})} \leq \\ &\lambda_j N^{-2+\frac{\lambda_j+1}{m}+\frac{3}{m}} N^{(L+1)(1-\frac{1}{m})}. \end{aligned} \quad (38)$$

Если $\sigma_j \geq L$, используем тривиальную оценку $|S_{v_j}| \leq N^L$.

Сначала предположим, что $L > \sigma_j$ для всех $1 \leq j \leq r$. Тогда, поскольку $\lambda_j \leq m-1$ по лемме 3.1, то подстановка (38) в (31) дает

$$\begin{aligned} |S(f, P^{L+1})| &\leq \sum_{j=1}^r |S_{v_j}| \leq N^{-2+\frac{3}{m}} N^{(L+1)(1-\frac{1}{m})} \sum_{j=1}^r \lambda_j N^{\frac{\lambda_j+1}{m}} \leq \\ &\leq N^{-1+\frac{3}{m}} N^{(L+1)(1-\frac{1}{m})} \sum_{j=1}^r \lambda_j = n N^{-1+\frac{3}{m}} N^{(L+1)(1-\frac{1}{m})}, \end{aligned}$$

что завершает доказательство (37) если $L > \sigma_j$ для всех $1 \leq j \leq r$.

Предположим теперь, не ограничивая общности, что $\sigma_1 \geq \dots \geq \sigma_{r_1} \geq L > \sigma_{r_1+1} \geq \dots \geq \sigma_r$.

Положим $\sum_{j=1}^{r_1} \lambda_j = n_1$ и $\sum_{j=r_1+1}^r \lambda_j = n_2$, а тогда $n_1 + n_2 = n$.

Для $1 \leq j \leq r_1$ по (29) имеем

$$\lambda_j + 1 \geq \sigma_j \geq L \implies n_1 + r_1 \geq r_1 L \implies \frac{n_1}{r_1} + 1 \geq L,$$

что дает

$$L = (L+1)(1-\frac{1}{m}) - 1 + \frac{2}{m} + \frac{L-1}{m} \leq (L+1)(1-\frac{1}{m}) - 1 + \frac{2}{m} + \frac{n_1}{r_1 m}.$$

Положим $h_1(y) = yN^{\frac{n_1}{ym}}$. Тогда имеем

$$h'_1(y) = N^{\frac{n_1}{ym}} \left(1 - \frac{n_1 \ln(N)}{ym}\right) \implies h''_1(y) = N^{\frac{n_1}{ym}} \frac{n_1^2 (\ln(N))^2}{y^3 m^2},$$

и поэтому $h''_1(y) \geq 0$, что дает

$$r_1 N^{\frac{n_1}{r_1 m}} \leq \max(N^{\frac{n_1}{m}}, n_1 N^{\frac{1}{m}}) \quad (39)$$

Теперь мы покажем, что $n_1 N^{\frac{1}{m}} \geq N^{\frac{n_1}{m}}$.

Положим $h_2(y) = yN^{\frac{1}{m}} - N^{\frac{y}{m}}$. Тогда имеем

$$h'_2(y) = N^{\frac{1}{m}} - \frac{1}{m} \ln(N) N^{\frac{y}{m}} \implies h''_2(y) = \frac{-1}{m^2} (\ln(N))^2 N^{\frac{y}{m}},$$

и поэтому $h''_2(y) \leq 0$, $h_2(1) = 0$.

Более того, поскольку $(m-1)^{\frac{m}{m-2}} \geq N > m$, то $h'_2(1) \geq 0$ и $h_2(m-1) \geq 0$.

Следовательно, имеем $h_2(y) \geq 0$ для $1 \leq y \leq m-1$, и поскольку по (30) и определению n_1 имеем $n_1 \leq n \leq m-1$, то это дает

$$n_1 N^{\frac{1}{m}} \geq N^{\frac{n_1}{m}}. \quad (40)$$

Поэтому, подставив (40) в (39), учитывая (31), (38) и тривиальную оценку $|S_{v_j}| \leq N^L$, получим

$$\begin{aligned} |S(f, P^{L+1})| &\leq \sum_{j=1}^{r_1} |S_{v_j}| + \sum_{j=r_1+1}^r |S_{v_j}| \leq r_1 N^L + N^{-2+\frac{3}{m}} N^{(L+1)(1-\frac{1}{m})} \sum_{j=r_1+1}^r \lambda_j N^{\frac{\lambda_j+1}{m}} \leq \\ &\leq N^{-1+\frac{2}{m}} N^{(L+1)(1-\frac{1}{m})} \left(r_1 N^{\frac{n_1}{r_1 m}} + \sum_{j=r_1+1}^r \lambda_j N^{\frac{\lambda_j+1}{m}-1+\frac{1}{m}} \right) \leq \\ &\leq N^{-1+\frac{2}{m}} N^{(L+1)(1-\frac{1}{m})} (n_1 N^{\frac{1}{m}} + n_2 N^{\frac{1}{m}}) \leq n N^{-1+\frac{3}{m}} N^{(L+1)(1-\frac{1}{m})}, \end{aligned}$$

что завершает доказательство (37) если $\sigma_1 \geq \dots \geq \sigma_{r_1} \geq L > \sigma_{r_1+1} \geq \dots \geq \sigma_r$.

Так как $q > m$, то $N \geq m$, а так как $-1 + \frac{3}{m} \leq 0$, учитывая (30), то в силу (37) имеем

$$|S(f, P^l)| \leq n N^{-1+\frac{3}{m}} N^{l(1-\frac{1}{m})} \leq \frac{m-1}{m} m^{\frac{3}{m}} N^{l(1-\frac{1}{m})},$$

что и доказывает утверждение теоремы в данном случае.

Случай 2. $q \leq m$:

Предположим сначала, что $l < 2(t+1)$. В этом случае воспользуемся тривиальной оценкой

$$|S(f, P^l)| \leq N^l = N^{\frac{l}{m}} N^{l(1-\frac{1}{m})} \leq N^{\frac{2t+1}{m}} N^{l(1-\frac{1}{m})},$$

что в силу предложения 5.1, леммы 6.2 и того факта, что $q \leq m$, дает

$$\begin{aligned} |S(f, P^l)| &\leq N^{\frac{2(e+1)\ln(m)}{m\ln(q)} + \frac{\ln(m)}{m\ln(q)}} N^{l(1-\frac{1}{m})} = \\ &= m^{\frac{2(e+1)\ln(N)}{m\ln(q)} + \frac{\ln(N)}{m\ln(q)}} N^{l(1-\frac{1}{m})} = m^{\frac{c(2e+3)}{m}} N^{l(1-\frac{1}{m})}. \end{aligned} \quad (41)$$

Для $l \geq 2(t+1)$ доказываем индукцией по l .

Случай 2а. $N \geq (m-1)^{\frac{m}{m-2}}$:

Этот случай аналогичен случаю 1а. По предположению индукции (41) получаем

$$|S_{v_j}| = m^{\frac{c(2e+3)}{m}} N^{\sigma_j-1} |S(g_j, P^{l-\sigma_j})| \leq N^{\sigma_j-1} N^{(l-\sigma_j)(1-\frac{1}{m})}, \quad (42)$$

причем эта оценка верна и в том случае, если $\sigma_j \geq l$, так как в этом случае она следует из тривиальной оценки $|S_{v_j}| \leq N^{l-1}$.

Подстановка (42) в (31) дает

$$\begin{aligned} |S(f, P^l)| &\leq m^{\frac{c(2e+3)}{m}} \sum_{j=1}^r N^{\sigma_j-1} N^{(l-\sigma_j)(1-\frac{1}{m})} = \\ &= m^{\frac{c(2e+3)}{m}} N^{l(1-\frac{1}{m})} \sum_{j=1}^r N^{-1+\frac{\sigma_j}{m}}. \end{aligned} \quad (43)$$

Поскольку $\sigma_j \leq \lambda_j + 1 \leq m$ в силу (29) и леммы 3.1, то предложение 6.1 дает

$$\sum_{j=1}^r N^{-1+\frac{\sigma_j}{m}} \leq N^{-1+\frac{1}{m}} \sum_{j=1}^r N^{\frac{\lambda_j}{m}} \leq N^{-1+\frac{1}{m}} \max((m-1)N^{\frac{1}{m}}, N^{1-\frac{1}{m}}). \quad (44)$$

Мы знаем, что

$$N \geq (m-1)^{\frac{m}{m-2}} \implies \max((m-1)N^{\frac{1}{m}}, N^{1-\frac{1}{m}}) = N^{1-\frac{1}{m}}, \quad (45)$$

и поэтому подстановка (44) и (45) в (43) дает

$$\sum_{j=1}^r N^{-1+\frac{\sigma_j}{m}} \leq 1 \implies |S(f, P^l)| \leq m^{\frac{c(2e+3)}{m}} N^{l(1-\frac{1}{m})},$$

что и доказывает утверждение теоремы в данном случае.

Случай 2б. $N \leq (m-1)^{\frac{m}{m-2}}$:

По предположению индукции (41), если $l > \sigma_j$, получим

$$|S_{v_j}| = N^{\sigma_j-1} |S(g_j, P^{l-\sigma_j})| \leq m^{\frac{c(2e+3)}{m}} \lambda_j N^{\sigma_j-1} N^{(l-\sigma_j)(1-\frac{1}{m})}, \quad (46)$$

и эта оценка справедлива и в том случае, если $\sigma_j \geq l$, так как в этом случае она следует из тривиальной оценки $|S_{v_j}| \leq N^{l-1}$.

Следовательно, поскольку $\sigma_j \leq \lambda_j + 1 \leq m$ в силу (29) и леммы 3.1, то подстановка (46) в (31) дает

$$|S(f, P^l)| \leq m^{\frac{c(2e+3)}{m}} N^{l(1-\frac{1}{m})} N^{-1} \sum_{j=1}^r \lambda_j N^{\frac{\lambda_j+1}{m}} \leq nm^{\frac{c(2e+3)}{m}} N^{l(1-\frac{1}{m})},$$

что, поскольку $n \leq m-1$ по (30), дает

$$|S(f, P^l)| \leq (m-1)m^{\frac{c(2e+3)}{m}} N^{l(1-\frac{1}{m})},$$

что и доказывает утверждение теоремы в данном случае.

Этим завершается доказательство конкретной оценки во всех случаях.

Общая оценка непосредственно следует из неравенств $c \leq d$ и $e \leq d-1$, оба из которых легко следуют из применения теоремы об уникальной факторизации идеалов в полях алгебраических чисел к (q) :

$$(q) = \prod_{j=1}^{s'} \tilde{P}_j^{e_j-1} \implies q^d = \prod_{j=1}^{s'} N(\tilde{P}_j^{e_j+1}) = q^{\sum_{j=1}^{s'} c_j(e_j+1)} \implies d = \sum_{j=1}^{s'} c_j(e_j+1),$$

где $e_j + 1$ — индекс ветвления простого идеала $\tilde{P}_j$. $\square$

7. Усиленная форма оценки Хуа Ло-Кена для определенного класса многочленов, когда число классов равен 1

В этом разделе мы получим более сильную форму теоремы 6.1 в частном случае, когда $\mathbb{K}$ имеет число классов равен 1, а идеал A имеет вид

$$A = \frac{B}{P^l}; (B, P) = 1,$$

для некоторого целого идеала B , что позволит получить более сильную форму оценки Хуа Ло-Кена в [2] для идеалов Q , удовлетворяющих $(Q, \delta) = 1$.

Начнем со вспомогательной леммы, которая будет играть роль, аналогичную лемме 4.1.

ЛЕММА 11. *Пусть P — простой идеал такой, что $P \nmid \delta$, а $\alpha \in R$ — целое число. Пусть η пробегает полную систему вычетов P^{-c} по модулю R , где $c \geq 1$ — некоторое рациональное целое число.*

Тогда

$$\sum_{\eta} E(\alpha\eta) = \sum_{\eta} e^{2\pi i T(\alpha\eta)} = \begin{cases} N(P^c) & \text{если } P^c | \alpha, \\ 0 & \text{если } P^c \nmid \alpha. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Если $P^c | \alpha$, то $\alpha\eta \in R$, что дает $E(\alpha\eta) = 1$, и тогда

$$\sum_{\eta} E(\eta\alpha) = N(P^c).$$

Мы покажем, что существует $\eta \in P^{-c}$, скажем η_0 , такая, что $\eta\alpha \notin \delta^{-1}$.

Если $\eta\alpha \in \delta^{-1}$ для всех $\eta \in P^{-c}$, то $\delta^{-1} | \alpha P^{-c}$, и тогда $P^c | \alpha \delta^{-1}$.

Поскольку P — простой идеал и $P^c \nmid \alpha$, то $P^{c'} | \delta^{-1}$ для некоторого $c' \geq 1$, что является противоречием.

По определению δ^{-1} существует целое число γ такое, что $E(\gamma\eta_0\alpha) \neq 1$. Поскольку $\gamma\eta_0 \in P^{-c}$, имеем

$$\sum_{\eta} E(\eta\alpha) = \sum_{\eta} E(\gamma\eta_0\alpha + \eta\alpha) = E(\gamma\eta_0\alpha) \sum_{\eta} E(\eta\alpha) \implies \sum_{\eta} E(\eta\alpha) = 0,$$

поскольку $E(\gamma\eta_0\alpha) \neq 1$. $\square$

ТЕОРЕМА 4. *Пусть $N(P) = q^c$, где $c \geq 1$ — целое рациональное число. Тогда мы имеем общую оценку*

$$|S(f, P^l)| \leq C_d(m) N(P)^{l(1-\frac{1}{m})},$$

где

$$C_d(m) = \begin{cases} 1 & \text{если } q > m, N(P) \geq (m-1)^{\frac{2m}{m-2}}, \\ (m-1)^{\frac{2}{m}} & \text{если } q > m, (m-1)^{\frac{2m}{m-2}} > N(P) \geq (m-1)^{\frac{m}{m-2}}, \\ \frac{m-1}{m} m^{\frac{3}{m}} & \text{если } q > m, N(P) < (m-1)^{\frac{m}{m-2}}, \\ m^{\frac{d(2d+1)}{m}} & \text{если } q \leq m, N(P) \geq (m-1)^{\frac{m}{m-2}}, \\ (m-1)m^{\frac{d(2d+1)}{m}} & \text{если } q \leq m, N(P) < (m-1)^{\frac{m}{m-2}}. \end{cases}$$

ДОКАЗАТЕЛЬСТВО. Доказательство полностью аналогично доказательству теоремы 6.1, за исключением случая 1а, где вместо использования оценки Морделла ([6], с.17) мы теперь можем использовать оценку Вейля для экспоненциальных сумм над конечными полями [9].

Действительно, поскольку P простой идеал, то R/P — конечное поле. Более того, поскольку число классов $\mathbb{K}$ равен 1, мы знаем, что P — главный идеал, скажем, с $P = (\pi)$.

Поскольку $A = \frac{B}{P}$, то каждое α_j можно выразить как

$$\alpha_j = \frac{b_j}{\pi},$$

и имеем

$$e^{2\pi i T(\frac{b_j + r\pi}{\pi} x^j)} = e^{2\pi i T(\frac{b_j}{\pi} x^j)}$$

для любого $r \in R$, откуда следует, что $\chi(y) = e^{2\pi i T(\frac{y}{\pi})}$ — аддитивный характер конечного поля R/P .

Следовательно, сумма действительно является экспоненциальной суммой по конечному полю, и оценка Вейля [9] в этом случае дает

$$|S(f, P)| \leq (m-1)N^{\frac{1}{2}} \iff |S(f, P)| \leq \min(N^{\frac{1}{m}}, (m-1)N^{\frac{-1}{2} + \frac{1}{m}})N^{1 - \frac{1}{m}},$$

где эквивалентность следует из тривиальной оценки $|S(f, P)| \leq N$.

Как и в случае 1а теоремы 6.1, получаем

$$|S(f, P^l)| \leq \max(1, \min(N^{\frac{1}{m}}, (m-1)N^{\frac{-1}{2} + \frac{1}{m}}))N^{l(1 - \frac{1}{m})}. \quad (47)$$

Если $N \leq (m-1)^2$, то

$$\min(N^{\frac{1}{m}}, (m-1)N^{\frac{-1}{2} + \frac{1}{m}}) = N^{\frac{1}{m}} \quad 1 \leq N^{\frac{1}{m}} \leq (m-1)^{\frac{2}{m}}, \quad (48)$$

и поэтому подстановка (48) в (47) дает

$$|S(f, P^l)| \leq (m-1)^{\frac{2}{m}} N^{l(1 - \frac{1}{m})}.$$

Если $N \geq (m-1)^2$ и $N \leq (m-1)^{\frac{2m}{m-2}}$, то

$$\min(N^{\frac{1}{m}}, (m-1)N^{\frac{-1}{2} + \frac{1}{m}}) = (m-1)N^{\frac{-1}{2} + \frac{1}{m}}, \quad 1 \leq (m-1)N^{\frac{-1}{2} + \frac{1}{m}} \leq (m-1)^{\frac{2}{m}}, \quad (49)$$

и поэтому в этом случае также подстановка (49) в (47) дает

$$|S(f, P^l)| \leq (m-1)^{\frac{2}{m}} N^{l(1 - \frac{1}{m})}.$$

Наконец, если $N \geq (m-1)^{\frac{2m}{m-2}}$, то $N \geq (m-1)^2$, и поэтому

$$\min(N^{\frac{1}{m}}, (m-1)N^{\frac{-1}{2} + \frac{1}{m}}) = (m-1)N^{\frac{-1}{2} + \frac{1}{m}} \leq 1, \quad (50)$$

и подстановка (50) в (47) дает

$$|S(f, P^l)| \leq N^{l(1 - \frac{1}{m})}.$$

□

PROPOSITION 5. Пусть $\tilde{q}$ — рациональное простое число. Тогда число простых идеалов $\tilde{P}_j$ в R , у которых $N(\tilde{P}_j) = q^{c_j}$ для некоторого $c_j \geq 1$, не превосходит d

ДОКАЗАТЕЛЬСТВО. По теореме об уникальной факторизации идеалов в полях алгебраических чисел, имеем

$$(\tilde{q}) = \prod_{j=1}^{s'} \tilde{P}_j^{e_j+1} \implies q'^d = \prod_{j=1}^{s'} N(\tilde{P}_j^{e_j+1}) \implies d = \sum_{j=1}^{s'} c_j(e_j + 1) \geq s'$$

где e_j — индекс ветвления простого идеала $\tilde{P}_j$. $\square$

Теперь сформулируем и докажем следующую усиленную форму теоремы Хуа Ло-Кена, в нашем частном случае.

ТЕОРЕМА 5. Пусть Q — целый идеал с $(Q, \delta) = 1$. Тогда справедлива оценка

$$|S(f, Q)| \leq e^{\frac{5}{2}d^2(2d+1)} e^{3.442md} N(Q)^{1-\frac{1}{m}}.$$

ДОКАЗАТЕЛЬСТВО. По теореме об уникальной факторизации идеалов в полях алгебраических чисел мы знаем, что Q однозначно выражается как

$$Q = \prod_{j=1}^s P_j^{r_j}, \quad r_j \geq 0, \quad (51)$$

где P_j — различные простые идеалы, а $r_j \in \mathbb{Z}$.

Следовательно, по (51) и лемме 4.2 имеем

$$S(f, Q) = \prod_{j=1}^s S(f_j, P_j^{r_j}),$$

для некоторых многочленов f_j степени m (а не многочленов из построения деревьев Хуа Ло-Кена в разделе 5, хоть обозначения совпадают), и поэтому, поскольку $(P_j, \delta) = 1$ для $1 \leq j \leq s$, то по теореме 4 это дает

$$|S(f, Q)| \leq \prod_{j=1}^s C_{d,j}(m) N(P_j^{r_j})^{1-\frac{1}{m}} = N(Q)^{1-\frac{1}{m}} \prod_{j=1}^s C_{d,j}(m), \quad (52)$$

где $C_{d,j}(m)$ — константа из теоремы 7.1, соответствующая P_j .

Для любого натурального числа $x \in \mathbb{Z}$, обозначаем через $\pi(x)$ обычную рациональную функцию распределения простых чисел в $\mathbb{Z}$,

$$\pi(x) = |\{k \in \mathbb{Z}; k \leq x, k \text{ является простым в } \mathbb{Z}\}|,$$

и обозначаем через $\tilde{\pi}(x)$ функция распределения простых идеалов в R ,

$$\tilde{\pi}(x) = |\{P \subseteq R; N(P) \leq x, P \text{ является простым идеалом в } R\}|.$$

Мы знаем, что $N(P) = q^c$, где q — простое число в $\mathbb{Z}$, и поэтому предложение 7.1 дает

$$N(P) \leq x \implies q \leq x \implies \tilde{\pi}(x) \leq d\pi(x). \quad (53)$$

Положим $A = (m-1)^{\frac{2m}{m-2}}$ и $B = (m-1)^{\frac{m}{m-2}}$.

Теперь оценим $\prod_{j=1}^s C_{d,j}(m)$. Из формулировки теоремы 7.1 непосредственно следует, что

$$\prod_{j=1}^s C_{d,j}(m) \leq ((m-1)^{\frac{2}{m}})^{\tilde{\pi}(A)-\tilde{\pi}(B)} \left(\frac{m-1}{m} m^{\frac{3}{m}}\right)^{\tilde{\pi}(B)} \left(m^{\frac{d(2d+1)}{m}}\right)^{d\pi(m)} ((m-1)m^{\frac{d(2d+1)}{m}})^{d\pi(m)}, \quad (54)$$

где степень $d\pi(m)$ следует из предложения 7.1.

Поэтому, по (53) имеем

$$\prod_{j=1}^s C_{d,j}(m) \leq e^{F(m)}, \quad (55)$$

где

$$\begin{aligned} F(m) = \ln(m) & \left(\left(\frac{3}{m} - 1 \right) d\pi(B) + d\pi(m) \left(\frac{2d(2d+1)}{m} \right) \right) + \\ & + \ln(m-1) \left(\frac{2d}{m} \pi(A) + \left(1 - \frac{2}{m} \right) d\pi(B) + d\pi(m) \right). \end{aligned} \quad (56)$$

Имеем $\frac{3}{m} - 1 \leq 0$, и используя известную оценку $\pi(x) \leq \frac{5x}{4\ln(x)}$ при $x \geq 3$ (см., например, [5], с.61) в (56) получим

$$F(m) \leq \frac{5}{2} d^2 (2d+1) + \ln(m-1) \left(\frac{5dA}{2m \ln(A)} + \frac{5dB(m-2)}{4m \ln(B)} + \frac{5dm}{4 \ln(m)} \right). \quad (57)$$

Вычисляем

$$\frac{5dA \ln(m-1)}{2m \ln(A)} = md \left(\frac{5(m-2)(m-1)^{\frac{2m}{m-2}}}{4m^3} \right) \leq 0.792md, \quad (58)$$

где последнее неравенство следует из элементарного математического анализа.

Аналогичным образом получим

$$\frac{5dB(m-2) \ln(m-1)}{4m \ln(B)} = md \left(\frac{5(m-2)^2(m-1)^{\frac{m}{m-2}}}{4m^3} \right) \leq 1.4md, \quad (59)$$

и

$$\frac{5dm \ln(m-1)}{4 \ln(m)} \leq 1.25dm. \quad (60)$$

Поэтому подстановка (58), (59) и (60) в (57) дает

$$F(m) \leq \frac{5}{2} d^2 (2d+1) + 3.442md,$$

что вместе с (55) завершает доказательство. $\square$

8. Новая оценка и некоторые наблюдения

Заметим, что константу $e^{\frac{5}{2}d^2(2d+1)}e^{3.442md}$ в теореме 7.2 можно существенно улучшить, используя более точные оценки $\pi(x)$ и $\tilde{\pi}(x)$, а также числа простых идеалов, удовлетворяющих каждому из случаев теоремы 7.1.

Заметим также, что для доказательства аналога теоремы 7.2 в общем случае нам не обязательно нужна столь сильная оценка, как у Вейля. Действительно, если бы мы имели какую-либо оценку вида

$$|S(f, P)| \leq C' N^{1-\frac{1}{m}-\epsilon}; \quad \epsilon > 0,$$

для некоторой постоянной C' , то аналогично доказательству теоремы 7.1, в тех же терминах получаем, что

$$N^\epsilon \geq C' \implies C_d(m) = 1.$$

Наконец, отметим, что объединение теоремы 5.1 и теоремы 6.1 дает следующую новую оценку.

ТЕОРЕМА 6. *Справедлива оценка*

$$|S(f, P^l)| \leq C_d(m)(m-1)N(P)^{l(1-\frac{1}{m})+\frac{U_h}{m}-h}.$$

Легко видеть, что теорема 8.1 дает лучшую оценку, чем теорема 5.2, поскольку $l \geq U_h$, и также лучшую оценку, чем теорема 6.1, поскольку по лемме 5.4 $mh \geq U_h$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. В.Н. Чубариков. О кратных рациональных тригонометрических суммах над полем алгебраических чисел // Чебышевский сборник, 22:4 (2021), 306–323.
2. Hua L-K. On Exponential Sums Over an Algebraic Number Field // Canadian Journal of Mathematics. 1951;3:44-51. doi:10.4153/CJM-1951-006-4.
3. Hua L-K. On the number of solutions of Tarry's problem // Acta Sci. Sinica. — 1952. — V.1. — P.1–76.
4. Hua, L. On An Exponential Sum. Journal of the London Mathematical Society, 1938, s1-13: 54-61. <https://doi.org/10.1112/jlms/s1-13.1.54>
5. Архипов Г.И., Карацуба А.А., Чубариков В.Н. Теория кратных тригонометрических сумм // М.: Наука. Физматлит. 1987.
6. Wang Yuan. Diophantine Equations and Inequalities in Algebraic Number Fields. Springer Verlag, Berlin, Heidelberg, 1991.
7. Anthony Knapp. Advanced Algebra // Birkhäuser Boston, 2006.
8. Anthony Knapp, Basic Algebra // Birkhäuser Boston, 2006.
9. Weil, A. (1948). On Some Exponential Sums // Proceedings of the National Academy of Sciences of the United States of America, 34(5), 204–207. <http://www.jstor.org/stable/88420>.
10. Чубариков В. Н. Деревья Хуа Ло-кена в теории сравнений // Математические вопросы кибернетики. Вып. 16. — М.: ФИЗМАТЛИТ, 2007. — С. 73–78.
11. Chen Jingrun. On Professor Hua's Estimate of Exponential Sums // Scientia Sinica, 20 (1977), 6: 711-719.
12. Chen Jingrun. On the representation of natural number as a sum of terms of the form $\frac{x(x+1)\cdots(x+k-1)}{k!}$ // Acta Mathematica Sinica, (1959), 264-270.
13. Nechaev V.I. An estimate of the complete rational trigonometric sum // Math. Notes, 17 (1975), No. 6, 504-511.
14. Qi Minggao and Ding Ping. On Estimate of complete trigonometric sums // China Ann. Math. B 6 (1985) 109-120.
15. Mordell, L. J. On a sum analogous to a Gauss's sum, Quart // J. Math., (Oxford), vol. 3 (1932), 161–167.

REFERENCES

1. Chubarikov, V. N., 2021. “On multiple rational trigonometric sums over a field of algebraic numbers”, *Chebyshevskii Sbornik*, Vol. 22, Iss. 4, pp. 306–323.
2. Hua, L-K., 1951. “On Exponential Sums Over an Algebraic Number Field”, *Canadian Journal of Mathematics*, 3:44-51. doi:10.4153/CJM-1951-006-4.
3. Hua, L-K., 1952. “On the number of solutions of Tarry’s problem”, *Acta Sci. Sinica*, Vol. 1. pp. 1–76.
4. Hua, L-K., 1938. “On An Exponential Sum”, *Journal of the London Mathematical Society*, s1-13:54-61. <https://doi.org/10.1112/jlms/s1-13.1.54>.
5. Arkhipov, G. I., Karatsuba, A. A., Chubarikov, V. N., 1987. “Theory of multiple trigonometric sums”, *M.: Nauka. Fizmatlit*.
6. Wang Yuan, 1991. “Diophantine Equations and Inequalities in Algebraic Number Fields”, *Springer Verlag, Berlin, Heidelberg*.
7. Anthony Knapp, 2006. “Advanced Algebra”, *Birkhäuser Boston*.
8. Anthony Knapp, 2006. “Basic Algebra”, *Birkhäuser Boston*, 2006.
9. Weil, A., 1948. “On Some Exponential Sums”, *Proceedings of the National Academy of Sciences of the United States of America*, 34(5), pp. 204–207. <http://www.jstor.org/stable/88420>.
10. Chubarikov, V. N., 2007. “Hua Lo-ken trees in the theory of comparisons”, *Mathematical issues of cybernetics*, Iss. 16. — *M.: FIZMATLIT*, pp. 73–78.
11. Chen Jingrun, 1977. “On Professor Hua’s Estimate of Exponential Sums”, *Scientia Sinica*, 20, 6: pp. 711-719.
12. Chen Jingrun, 1959. “On the representation of natural number as a sum of terms of the form $\frac{x(x+1)\cdots(x+k-1)}{k!}$ ”, *Acta Mathematica Sinica*, pp. 264–270.
13. Nechaev, V. I., 1975. “An estimate of the complete rational trigonometric sum”, *Math. Notes*, 17, № . 6, pp. 504–511.
14. Qi Minggao & Ding Ping, 1985. “On Estimate of complete trigonometric sums”, *China Ann. Math.* Vol. 6, pp. 109–120.
15. Mordell, L. J., 1932. “On a sum analogous to a Gauss’s sum”, *Quart. J. Math. (Oxford)*, Vol. 3, pp. 161–167.

Получено: 27.03.2024

Принято в печать: 28.06.2024