ДОКЛАДЫ РОССИЙСКОЙ АКАДЕМИИ НАУК. МАТЕМАТИКА, ИНФОРМАТИКА, ПРОЦЕССЫ УПРАВЛЕНИЯ, 2024, том 517, с. 30–32

МАТЕМАТИКА

УДК 511

ПРИМЕНЕНИЕ ФОРМУЛЫ А. Г. ПОСТНИКОВА В ПОЛЯХ АЛГЕБРАИЧЕСКИХ ЧИСЕЛ

© 2024 г. Х. Аль-Ассад[1, *]

Представлено академиком РАН В.А. Садовничим
Получено 19.04.2024 г.
После доработки 04.05.2024 г.
Принято к публикации 18.05.2024 г.

Получен новый результат, обобщающий формулу А.Г. Постникова об индексах на случай степени числа 2. Исследована мультипликативная структура приведённых систем вычетов по модулю степени простого идеала. Установлены оценки некоторых сумм характеров в полях алгебраических чисел.

Ключевые слова: формула Постникова, поля алгебраических чисел, суммы характеров, кольца вычетов по модулю степени простого идеала

DOI: 10.31857/S2686954324030048, **EDN:** YBNQFB

1. ФОРМУЛА А.Г. ПОСТНИКОВА ДЛЯ СТЕПЕНЕЙ НЕЧЕТНЫХ ПРОСТЫХ ЧИСЕЛ

Пусть q – нечетное простое число, $n \ge 1$ – целое число, и пусть g – примитивный корень в $(\mathbb{Z} / q^n\mathbb{Z})^\times$. Обозначим через $\mathrm{ind}_g(\cdot)$ соответствующую функцию индекса.

Если n представляется в виде $n = \alpha q^{\tilde f} - \mu(\tilde f)$, где $\tilde f, \mu(\tilde f)$ – целые, и $0 \le \mu(\tilde f) \le \tilde f - 1$ и $(\alpha, q) = 1$, тогда положим f, равному максимальному значению среди таких $\tilde f$. Определим $\mu = \mu(f)$ если $n = \alpha q^{\tilde f} - \mu(\tilde f)$, и $\mu = -1$ в противном случае.

Теорема 1. *Существует многочлен* $f(u) = a_{n+\mu}u^{n+\mu} + \cdots + a_1 u$ *степени* $n + \mu$ *с целыми коэффициентами такой, что при любом целом* u *справедливо сравнение*

$$\frac{\mathrm{ind}_g(1 + qu)}{q - 1} \equiv \Lambda f(u) \bmod q^{n-1}.$$

Пусть $k = k'q^\tau$, *где* $\tau, k' \in \mathbb{Z}$, *и* $(k', q) = 1$. *Тогда* $a_k = (-1)^{k+1} q^{k-1-\tau} x_k$, *где* x_k *есть решение сравнения* $k' x_k \equiv 1 \bmod q^{n-k+\tau}$. *Более того,* Λ – *решение сравнения* $\dfrac{\mathrm{ind}_g(1 + qu)}{q - 1} \equiv \Lambda f(1) \bmod q^{n-1}$ *и* $(\Lambda, q) = 1$.

Кроме того, при любом целом u *справедливо сравнение*

$$\mathrm{ind}_g(a + qu) \equiv \mathrm{ind}_g(a) + \Lambda(q - 1) f(a'u) \bmod q^{n-1};$$
$$aa' \equiv 1 \bmod q.$$

2. ОБОБЩЕНИЕ ФОРМУЛЫ А. Г. ПОСТНИКОВА НА СТЕПЕНИ ПРОСТОГО ЧИСЛА 2

Пусть $n \ge 3$ – целое число, и g порождающий элемент подгруппы $(\mathbb{Z} / 2^n\mathbb{Z})_1^\times \subset (\mathbb{Z} / 2^n\mathbb{Z})^\times$ вычетов, сравнимых с 1 по модулю 4.

Пусть $d = \left\lfloor \dfrac{n-1}{2} \right\rfloor$. Положим $\varepsilon(n) = 1$, если n четное, и $\varepsilon(n) = 0$, если n нечетное. Если d представляется в виде $d = \alpha 2^{\tilde f} - \mu(\tilde f)$, где $\tilde f, \mu(\tilde f)$ – целые, и $0 \le \mu(\tilde f) \le \dfrac{\tilde f + \varepsilon(n)}{2}$ и α нечетное, тогда положим f, равному максимальному значению среди таких $\tilde f$. Определим $\mu = \mu(f)$ если $d = \alpha 2^{\tilde f} - \mu(\tilde f)$, и $\mu = 0$ в противном случае.

Теорема 2. *Существует многочлен* $f(u) = a_{d+\mu}u^{d+\mu} + \cdots + a_2 u^2 + a_1 u$ *степени* $d + \mu$ *с целыми коэффициентами такой, что при любом целом* u *и справедливо сравнение*

$$\mathrm{ind}_g(1 + 4u) \equiv \Lambda f(u) \bmod 2^{n-2}.$$

Пусть $k = 4^\tau k'$, где $\tau, k' \in \mathbb{Z}$, и $(k', 4) \le 2$. Тогда $a_k = (-1)^{k+1} 4^{k-1-\tau} x_k$ если $(k', 4) = 1$, и

[1] *Московский государственный университет имени М.В. Ломоносова, Москва, Россия*
[*] *E-mail: 1hbrh0@gmail.com*

$a_k = (-1)^{k+1}\frac{4^{k-1-\tau}}{2}x_k$ если $(k',4)=2$, где x_k есть решение сравнения $k'x_k \equiv 1 \bmod 2^{n-2}$ если $(k',4)=1$, и $\frac{k'}{2}x_k \equiv 1 \bmod 2^{n-2}$ если $(k',4)=2$. Более того, Λ — решение сравнения $\mathrm{ind}_g(5) \equiv \Lambda f(1) \bmod 2^{n-2}$ и Λ нечетное.

3. МУЛЬТИПЛИКАТИВНАЯ СТРУКТУРА ПРИВЕДЕННЫХ СИСТЕМ ВЫЧЕТОВ ПО МОДУЛЮ СТЕПЕНИ ПРОСТОГО ИДЕАЛА

В оставшейся части данной работы пусть $\mathbb{K}$ — поле алгебраических чисел с дискриминантом Δ, а R — кольцо целых чисел в нем. Пусть P — простой идеал с $N(P)=q^r$ для некоторого рационального простого q и рациональное целого $r \geq 1$. Пусть $n \geq 1$, если $q \neq 2$, или $n \geq 2$, если $q=2$ — рациональное целое. Рассматриваем мультипликативную группу приведенных вычетов по модулю P^n, обозначаемую $(R/P^n)^\times$. Пусть $(R/P^n)_1^\times \subset (R/P^n)^\times$ — подгруппа вычетов, сравнимых с 1 по модулю P.

Теорема 3. *Имеет место изоморфизм*

$$(R/P^n)^\times \cong (R/P^n)_1^\times \oplus (R/P)^\times.$$

Более того, структура $(R/P^n)_1^\times$, имеет вид

$$(R/P^n)_1^\times \cong \bigoplus_{j=1}^{L} \mathbb{Z}/q^{k_j}\mathbb{Z},$$

где подгруппы справа аддитивные, а целые числа L, k_j зависят от n и q (в частности, они зависят от того, четно или нет q, и $q \mid \Delta$ или нет (разветвляется ли q или нет), а если $q \mid \Delta$, то от того, насколько велик n по сравнению с индексом ветвления) [3], [4].

Следствие 1. *Каждый $u \in (R/P^n)^\times$ представляется в виде $u=(a,u_1,\ldots,u_L)$, где $a \in (R/P)^\times$ и $u_j \in \mathbb{Z}/q^{k_j}\mathbb{Z}$.*

4. МЕТОД ПОЛУЧЕНИЯ ОЦЕНОК ДЛЯ НЕКОТОРЫХ СУММ ХАРАКТЕРОВ

Следствие 2. *Пусть q — нечетное рациональное простое число, $n \geq 1$ — рациональное целое и χ — мультипликативный характер по модулю q^n. Тогда в терминах теоремы 1*

$$\chi(u) = \theta e^{2\pi i m \Lambda \frac{f(u)}{q^{n-1}}}; \quad |\theta| = 1,$$

где m — рациональное целое, а θ зависит только от вычета u по модулю q.

Следствие 3. *Пусть $n \geq 3$ — рациональное целое и χ — мультипликативный характер по модулю 2^n. Тогда в терминах теоремы 2*

$$\chi(u) = \pm e^{2\pi i m \Lambda \frac{f(u)}{2^{n-2}}}; \quad |\theta| = 1,$$

где m — рациональное целое, и знак зависит только от вычета u по модулю 4.

Теорема 4 (*И. М. Виноградов*).

Пусть $m, L \in \mathbb{Z}$ с $m, L > 0$ и $f(u)$ — многочлен степени $D+1$ с вещественными коэффициентами такой, что некоторый коэффициент $b_{d'}$ удовлетворяет $b_{d'} = \frac{a}{q} + \frac{\theta}{q^2}$; $(a,q)=1$, $|\theta| < 1$.

Полагая $\tau = \frac{\ln q}{\ln L}$ если $1 < q \leq L$, $\tau = 1$ если $L < q \leq L^{d'-1}$ и $\tau = d' - \frac{\ln q}{\ln L}$ если $L^{d'-1} < q < L^{d'}$, а $\tilde{l} = \ln\left(\frac{12(d+\mu-1)(d+\mu)}{\tau}\right)$, $\rho = \frac{1}{3D^2\tilde{l}}$, то имеет место оценка

$$\left|\sum_{u=1}^{L} e^{2\pi i m f(u)}\right| < (8D)^{D\tilde{l}/2} m^{2\rho} L^{1-\tau\rho}.$$

Используя теорему 4, следствия 2 и 3 с известным изоморфизмом $\mathbb{Z}/q^{k_j}\mathbb{Z} \cong (\mathbb{Z}/q^{k_j-1}\mathbb{Z})_1^\times$, где группа справа — мультипликативная подгруппа вычетов по модулю q^n, сравнимых с 1 по модулю q если $q \neq 2$, а сравнимых с 1 по модулю 4 если $q=2$, получим основной результат данной работы.

Теорема 5. *Пусть $1 \leq h \leq L$ — рациональное целое, и $\{k_{j_1},\ldots,k_{j_h}\} \subseteq \{k_1,\ldots,k_L\}$, так, что $k_{j_t} \geq 4$, если $q=2$, и $k_{j_t} \geq 3$ если $q \neq 2$. Пусть $A \subseteq (R/P)^\times, A' \subseteq \bigoplus_{t=1}^{h} \mathbb{Z}/q^{k_{j_t}}\mathbb{Z}$ — некоторые подмножества, и пусть, для $j \notin \{j_1,\ldots,j_h\}$, b_j, c_j — рациональные целые такие, что $0 \leq b_j \leq c_j < q^{k_j}$. Пусть*

$$S = \{u \in (R/P^n)^\times; a \in A, (u_{j_1},\ldots,u_{j_h}) \in$$

$$\in A', b_j \leq u_j \leq c_j \leq q^{k_j}; j \notin \{j_1\ldots,j_h\}\}.$$

Пусть $l = n - 1 + \mu$, тогда, полагая $K_1 = \sum_{j \notin \{j_1 \ldots, j_h\}} k_j, K_2 = \sum_{t=1}^{h} k_{j_t}$, справедлива общая оценка

$$\left|\sum_S \chi(u)\right| \le 2^{L-h}(8l)^{\frac{(L-h)l}{2}\ln(12l(l+1)(n-2))} \times$$

$$\times (q^r - 1)q^{\left(1-\frac{1}{3l^2(n-2)\ln(12l(l+1)(n-2))}\right)K_1+K_2},$$

и l удовлетворяет неравенствам $n - 2 \le l \le n - 2 + \frac{\ln(\frac{9n}{8})}{\ln q}$.

Кроме того, полагая $\tau(x) = 1$ если $q^{1+\frac{1}{n-2}} \le x \le q^2$, и $\tau(x) = \frac{\ln q}{\ln \frac{x}{q}}$ если $x \ge q^2$, а $w(x) = \frac{\tau(x)}{3l^2 \ln(\frac{12l(l+1)}{\tau(x)})}$, то справедлива конкретная оценка

$$\left|\sum_S \chi(u)\right| \le |A||A'| \prod_{j \notin \{j_1 \ldots, j_h\}} \left((8l)^{\frac{\tau(b_j)}{6lw(b_j)}} b_j^{1-w(b_j)} + (8l)^{\frac{\tau(c_j)}{6lw(c_j)}} c_j^{1-w(c_j)} \right).$$

СПИСОК ЛИТЕРАТУРЫ

1. *Постников А.Г.* О сумме характеров по модулю, равного степени простого числа // Изв. АН СССР. Сер. матем. 1955. Т. 19. № 1. С. 11–16.
2. *Аль-Ассад Х.* О сумме характеров по модулю, равного степени простого числа 2 // Чебышевский сб. 2022. Т. 23. № 2. С. 201–208.
3. *Elia M.J., Interlando C., Rosenbaum R.* On the Structure of Residue Rings of Prime Ideals in Algebraic Number Fields. Part I: Unramified Primes // International Mathematical Forum. 2010. V. 5. № 56. С. 2795–2808.
4. *Elia M.J., Interlando C., Rosenbaum R.* On the Structure of Residue Rings of Prime Ideals in Algebraic Number Fields. Part II: Ramified Primes // International Mathematical Forum. 2011. V. 6. № 12. С. 565–589.
5. *Виноградов И.М.* Избранные труды . М.: Издательство Академии наук СССР, 1952. 428 с.
6. *Архипов Г.И., Карацуба А.А., Чубариков В.Н.* Теория кратных тригонометрических сумм. М.: Наука; Физматлит, 1987. 368 с.

APPLYING A. G. POSTNIKOV'S FORMULA IN ALGEBRAIC NUMBER FIELDS

H. Al-Assad[a]

Presented by Academician of the RAS V.A. Sadovnichiy

[a] *Lomonosov Moscow State University, Moscow, Russia*

A new result has been obtained generalizing A.G. Postnikov's formula on indices for the case of a power of 2. The multiplicative structure of the reduced residue systems modulo the degree of a prime ideal is investigated. Estimates of some sums of characters in the fields of algebraic numbers are established.

Keywords: Postnikov's formula, algebraic number fields, character sums, residue rings modulo prime-power ideals