MSC 11L05

ОБ ОБРАЩЕНИИ В НУЛЬ СУММЫ ПРОИЗВЕДЕНИЙ ХАРАКТЕРА ГРУППЫ КЛАССОВ ИДЕАЛОВ МНИМОГО КВАДРАТИЧНОГО ПОЛЯ НА ДВОЙНЫЕ СУММЫ ГАУССА

Р.А. Дохов

Кабардино-Балкарский государственный университет,
ул. Чернышевского, 173, Нальчик, 360004, Россия, e-mail: dohov.rezuan@yandex.ru

Аннотация. В работе, применяя теорию композиции классов бинарных квадратичных форм, доказывается, что сумма $\sum\limits_{A\in Cl}\Psi(A)G_A(q,l)$ произведений мультипликативного характера ψ группы классов идеалов любого мнимого квадратичного поля $F=Q\left(\sqrt{d}\right)$, $d<0$ на двойные суммы Гаусса $G_A(q,l)$ равна нулю.

Ключевые слова: характер группы, класс идеалов, двойная сумма Гаусса, композиция классов, бинарная квадратичная форма, мнимое квадратичное поле.

1. Введение. Пусть $F=Q\left(\sqrt{d}\right)$ — мнимое квадратичное поле, где $d<0$ — свободно от квадратов. Дискриминант δ_F поля F определяется равенством

$$\delta_F=\begin{cases} d & \text{при } d\equiv 1 \pmod 4\,;\\ 4d & \text{при } d\equiv 2;\ 3 \pmod 4\,.\end{cases}$$

Обозначим через Cl_F группу классов идеалов квадратичного поля F. Хорошо известно, что Cl_F — конечная абелева группа (см. например [1,2]) и ее порядок равен числу классов эквивалентных идеалов поля F. Через ψ обозначаем комплексный характер группы классов идеалов Cl_F кольца Z_F целых чисел поля F.

В нашей работе будем использовать следующее свойство для суммы значений характера ψ на всех элементах $A\in Cl_F$,

$$\sum_{A\in Cl_F}\psi(A)=0\,.$$

Известно также, что каждому классу A эквивалентных идеалов из Cl_F взаимно однозначно соответствует положительно определенная примитивная бинарная квадратичная форма с целыми коэффициентами

$$Q_A(m_1,m_2)=am_1^2+bm_1m_2+cm_2^2$$

с дискриминантом D, равным дискриминанту δ_F поля F, т.е. $D=\delta_F=b^2-4ac$; при этом число d, через которое определяется поле F связано с дискриминантом соотношением

$$d=\begin{cases} D & \text{при } d\equiv 1 \pmod 4\,,\\ D/4 & \text{при } d\equiv 2;\ 3 \pmod 4\,.\end{cases}$$

Пусть $l,\ q$ — целые числа и $(l,\ q)=1,\quad q>1$. Определим двойную сумму Гаусса по модулю q, соответствующую форме Q_A:

$$G_A\left(q,l\right)=\sum_{m_1=1}^{q}\ \sum_{m_2=1}^{q}e^{2\pi i\frac{lQ_A(m_1,m_2)}{q}}. \tag{1}$$

Мы будем рассматривать сумму вида

$$\sum_{A\in Cl_F}\psi\left(A\right)G_A\left(q,l\right), \tag{2}$$

где суммирование проводится по всем элементам A группы классов идеалов поля F.

Аналогичная сумма произведений в случае однократной суммы Гаусса для конечных полей служит для определения коэффициентов Фурье в разложении мультипликативного характера ψ по аддитивным характерам конечного поля F_q и, тем самым, суммы Гаусса для конечных полей служат инструментом для перехода от аддитивной структуры к мультипликативной структуре конечного поля (см. [3]).

Ставится вопрос: верно ли, что для любого квадратичного поля $F=Q\left(\sqrt{d}\right)$ и для любых l и $q>1$ сумма (2) равна 0. Решению этого вопроса посвящена настоящая работа.

При решении этого вопроса в случае нечетного q используется следующий результат о двойных гауссовых суммах вида (1) из [6].

Теорема 1. *Пусть q — нечетное положительное число, l,a — целые числа, взаимно простые с q, причем $(\delta_F,q)\geq 1$. Тогда:*

1). Если $q|\,\delta_F$, то

$$G_A(q,l)=\left(\frac{la}{d}\right)\cdot\left(\frac{-D'}{q'}\right)i^S\sqrt{d}q\,,$$

где $d=(\delta_F,q)$;

$$S=\begin{cases}0,\text{если}\quad q,q'\equiv\ \ \ 1(\mathrm{mod}4)\,;\\ 1,\text{если}\quad q\cdot q'\equiv-1(\mathrm{mod}4)\,;\\ 2,\text{если}\quad q,q'\equiv\ -1(\mathrm{mod}4)\,;\end{cases}$$

$$D'=\frac{D}{d},\quad q'=\frac{q}{d},\quad \left(\frac{*}{d}\right),\quad \left(\frac{*}{q'}\right)\ \text{— символы Якоби}\,.$$

2). Если $q|\,\delta_F$, то

$$G_A(q,l)=\left(\frac{la}{d}\right)i^{\left(\frac{q-1}{2}\right)^2}q\sqrt{q}\,.$$

В случае четного q будут использованы следующие результаты из [6].

Теорема 2. *Пусть $q=2^\alpha\cdot q_1$ — целое положительное число; q_1 нечетно; D – дискриминант примитивной бинарной квадратичной формы $Q_A\left(m_1,m_2\right)$, соответствующей идеалу квадратичного поля F дискриминанта $\delta_F=D$, причем $\frac{|D|}{4}\equiv\pm1\ \ (\mathrm{mod}4)$. Тогда*

$$G_A\left(q;l\right)=\begin{cases}\gamma_d\left(q,l,D\right)i^{q_1la}\left(\frac{a}{d}\right) & \text{при}\ \ |D|/4\equiv 1\ \ (\mathrm{mod}4)\ ;\\ \gamma_d\left(q,l,D\right)\left(\frac{a}{d}\right) & \text{при}\ \ |D|/4\equiv -1\ \ (\mathrm{mod}4)\ ,\end{cases}$$

где

$$\gamma_d\left(q,l,D\right)=\left(\frac{2^{\alpha}}{d}\right)\cdot\left(\frac{|D|\ :\ d}{q_1}\right)\ i^{S}\cdot(-1)^{\ \frac{((D):4)^2-1}{8}\alpha}\cdot 2^{\alpha+1}\sqrt{d}\,,$$

$d =$НОД(q_1, D); a — первый коэффициент формы $Q_A\left(m_1, m_2\right)$.

Теорема 3. *Пусть $q = 2^{\alpha}\cdot q_1$ — целое положительное число; q_1 — нечетно; D — дискриминант примитивной бинарной квадратичной формы $f = Q_A(m_1, m_2)$, соответствующей идеалу мнимого квадратичного поля F дискриминанта $\delta_F = D$, причем $|D|/8 \equiv \pm 1(\mathrm{mod} 4)$.*

Тогда

$$G_A(q;l)=\begin{cases}\gamma_d(q,D,l)i^{q_1 la}\left(\dfrac{a}{d}\right) & \text{при } |D|/8\equiv\ \ 1(\mathrm{mod}4)\,,\\ \gamma_d(q,D,l) & \text{при } |D|/8\equiv -1(\mathrm{mod}4)\,,\end{cases}$$

где

$$\gamma_d(q,l,D)=\left(\frac{2^{\alpha}}{d}\right)\cdot\left(\frac{|D|:d}{q_1:d}\right)i^{S}\sqrt{d}\cdot q_1\cdot 2^{\alpha+1}\sqrt{2}\,.$$

Используя наряду с теоремами 1-3 и основную теорему о конечных абелевых группах, мы докажем основной результат пашей работы о том, что

$$\sum_{A\in Cl}\Psi(A)G_A(q,l)=0.$$

2. Вычисление суммы $\sum\limits_{A\in Cl}\psi\left(A\right)G_A\left(q,l\right)$ в случаях нечетного q и цикличности группы Cl_F. Докажем, что в случае $(q,\delta_F) > 1$, где q — нечетно и циклической группы классов идеалов Cl_F сумма (2) равна пулю. Для этого мы воспользуемся теоремой 1 и гауссовой теорией композиции бинарных квадратичных форм [4,5].

Пусть Cl_F — циклическая группа порядка h. Так как ψ — мультипликативный характер группы Cl_F то $\psi\left(A\right)\in U_h$, где U_h — группа корней h-й степени из 1.

Будем сопоставлять $\psi\left(A\right)$ примитивную бинарную квадратичную форму $Q_A\left(m_1, m_2\right)$. В силу мультипликативности характера ψ имеем $\psi\left(A^h\right) = \left(\psi\left(\dot{A}\right)\right)^h = 1$ и значит, $\psi\left(A\right)\in U_h$.

Композиция классов идеалов в группе Cl_F определяется следующим образом. Все идеалы поля $F = Q\left(\sqrt{d}\right)$ разбиваются на классы эквивалентно идеалов. Операция умножения классов идеалов индуцируется операцией умножения идеалов, при этом результат операции умножения двух классов идеалов не зависит от выбора идеалов в этих классах.

Единичным элементом в группе Cl_F является главный класс, состоящий из всех ненулевых главных идеалов поля F.

Если E — главный класс группы Cl_F, то для любого класса идеала $[A]$ выполняется равенство $[A]^h = E$, т.е. A^h есть главный идеал, где $h = |Cl_F|$.

Мы воспользуемся хорошо известным взаимно однозначным соответствием между классами идеалов квадратичных полей и классами примитивных бинарных квадратичных форм (см., напр., [1], где вместо идеалов используются классы подобных полных модулей; но это одно и то же, так как идеал в максимальном порядке O_F есть полный модуль в поле $F = Q\left(\sqrt{d}\right)$, для которого порядок O_F является кольцом множителей).

Это соответствие в случае мнимого квадратичного поля определяется следующим образом. Пусть — идеал в максимальном порядке O_F квадратичного поля F и α, β — его базис, удовлетворяющий условию

$$-i\begin{vmatrix} \alpha & \beta \\ \alpha' & \beta' \end{vmatrix} > 0,$$

где штрих означает сопряжение в поле $F = Q\left(\sqrt{d}\right)$. Рассмотрим примитивную бинарную квадратичную форму

$$f\left(x,y\right) = \frac{N\left(\alpha x + \beta y\right)}{N\left(A\right)} = ax^2 + bxy + cy^2\,,$$

при этом получается, что $D = b^2 - 4ac$, где $N\left(A\right)$ — норма идеала A.

Тогда соответствие

$$A \leftrightarrow f\left(x,y\right) = Q_A\left(m_1, m_2\right)$$

есть изоморфизм между группой классов идеалов квадратичного поля F дискриминанта δ_F и группой классов собственно эквивалентных примитивных бинарных квадратичных форм дискриминанта D (при этом операция в последней группе есть гауссова композиция бинарных квадратичных форм).

Так как по нашему условию группа классов идеалов Cl_F является циклической порядка h, и она изоморфна циклической группе U_h корней h-й степени из 1, то считая класс $[A]$ образующим элементом, поставим ему в соответствие первообразный корень ε степени h из 1.

В силу указанного выше изоморфизма группа классов собственно эквивалентных бинарных квадратичных форм дискриминанта $D = \delta_F$ также является циклической порядка h относительно гауссовой композиции. Тогда, если

$$A \leftrightarrow Q_A\left(m_1, m_2\right)\,,$$

то

$$\varepsilon \leftrightarrow \left(a,\ b,\ c\right)\,,$$

где $(a,\ b,\ c)$ — образующий элемент группы классов квадратичных форм, при этом $\varepsilon = \psi\left(A\right)$.

Из теории композиции бинарных квадратичных форм известно (см. напр. [4], гл. 14), или [7], гл. 8, где используется китайская теорема об остатках), что если

$$f_j\left(x,y\right) = a_j x^2 + b_j xy + c_j y^2 \quad (j = 1,\ 2,\ 3)$$

— три примитивные формы дискриминанта D с одинаковым средним коэффициентом b и если $a_3 = a_1 a_2$, то соответствующие классы форм удовлетворяют равенству

$$K_3 = K_1 K_2\,,$$

причем это определение не зависит от выбора $f_j \in K_j$. Мы будем пользоваться более упрощенным подходом Дирихле (см. [4]) при определении композиции форм. Именно, мы будем говорить, что две примитивные формы

$$f_j = (a_i,\ b_j,\ c_j)\ ,\quad j = 1,\ 2$$

дискриминанта D являются согласными если выполняются условия:

1) $a_1 a_2 \neq 0$;

2) их средние коэффициенты одинаковы: $b_1 = b_2 = b$;

3) форма $f_j = (a_1\ a_2,\ b, *)$ — целочисленна. причем, как уже было отмечено, форма f_3 примитивна. Тогда форма f_3 называется композицией форм f_1 и f_2 (звездочкой $*$ обозначен коэффициент, величина которого для нас не важна).

Итак, если $Q_A\,(m_1, m_2) = (a,\ b,\ c)$ — образующий элемент в циклической группе классов бинарных квадратичных форм, то

$$\varepsilon \leftrightarrow (a,\ b,\ c)$$

и, значит, но определению композиции но Дирихле $\varepsilon^k \leftrightarrow \left(a^k, *, *\right)$, где $k = 1, ..., h$, при этом компонируются только согласные формы.

Теперь мы в состоянии вычислить сумму (2) в случае $d = (\delta_F, q) > 1$, где q — нечетное положительное число. Для этого пользуясь теоремой 1 и учитывая, что $\psi\,(A_0) = \varepsilon$, выбирается первообразным корнем степени h из 1, будем иметь

$$\sum_{A \in Cl_F} \psi\,(A)\, G_A\,(q, l) = \sum_{k=1}^{h} \psi\left(A_0^k\right) \sum_{m_1, m_2 = 1}^{q} e^{2\pi i \frac{l Q_{A_0^k}(m_1, m_2)}{q}} =$$

$$= \sum_{k=1}^{h} \psi^k\,(A_0) \sum_{m_1, m_2 = 1}^{q} e^{2\pi i \frac{l\left(a^k, *, *\right)}{q}} = \sum_{k=0}^{h-1} \varepsilon^k \left(\frac{l a^k}{d}\right) \cdot \left(\frac{-D'}{q'}\right)\, i^s \sqrt{d} \cdot q\,.$$

Но $\displaystyle\sum_{k=0}^{h-1} \varepsilon^k \left(\frac{a}{d}\right)^k = \frac{\varepsilon^h \left(\frac{a^h}{d}\right) - 1}{\varepsilon \left(\frac{a}{d}\right) - 1} = 0$, т.к. форма $\left(a^h, *, *\right) \sim f_0$ и $\varepsilon \neq 1$, где f_0 — главная форма дискриминанта D, т.е.

$$f_0 = \begin{cases} x^2 + \dfrac{1}{4}\,|D|\, y^2, & \text{если } D \text{ — четное}\,; \\[2ex] x^2 + xy + \dfrac{1 + |D|}{4} y^2, & \text{если } D \text{ — нечетное}\,. \end{cases}$$

при этом также учитывается, что характеры формы f не зависят от представляемых чисел этой формой, т.е. в данном случае $\left(\dfrac{a^h}{p}\right) = \left(\dfrac{1}{p}\right) = 1 \quad \forall p\,|D$.

3. Общий случай абелевой группы Cl_F при нечетном q. Мы будем пользоваться следующим результатом: *каждая конечная (мультипликативная) абелева группа является прямым произведением циклических групп.* (см. [2])

Итак, пусть

$$Cl_F = G_1 \times ... \times G_k \,,$$

где G_j — циклические группы, $1 \leq j \leq k$. Обозначим через r_j порядок группы G_j и через A_j ее образующий элемент. Тогда для порядка h группы классов идеалов Cl_F имеет место равенство

$$h = r_1 r_2 \cdot ... \cdot r_k$$

и каждый элемент A (он может рассматриваться и как класс идеалов и как представитель этого класса) может быть единственным образом представлен в виде

$$A = A_1^{t_1} A_2^{t_2} \cdot \ldots \cdot A_k^{t_k} \,,$$

где $0 \leq t_j \leq r_j - 1$, $j = 1, ..., k$. Тогда, если $A_j \leftrightarrow (a_j, *, *)$, $j = 1, ..., k$, то

$$\sum_{A \in Cl_F} \psi(A) \cdot G_A(q, l) = \sum_{\substack{0 \leq t_1 \leq r_1 - 1, \\ \cdots \\ 0 \leq t_k \leq r_k - 1}} \psi(A_1)^{t_1} ... \psi(A_k)^{t_k} \sum_{m_1, m_1 = 1}^{q} e^{2\pi i} l Q_{A_1} \cdot Q_{A_k} =$$

$$= \sum_{\substack{0 \leq t_1 \leq r_1 - 1, \\ \cdots \\ 0 \leq t_k \leq r_k - 1}} \psi(A_1)^{t_1} ... \psi(A_k)^{t_k} \sum_{m_1, m_2 = 1}^{q} e^{2\pi i \dfrac{l Q_{A_1^{t_1}}(\bar{m}) \cdot ... \cdot Q_{A_k^{t_k}}(\bar{m})}{q}} \,,$$

где $Q_{A_1^{t_1}}(\bar{m}) \cdot ... \cdot Q_{A_k^{t_k}}(\bar{m})$ есть гауссова композиция бинарных квадратичных форм; $\bar{m} = (m_1; m_2)$.

По определению композиции бинарных квадратичных форм, теперь получаем

$$\sum_{A \in Cl_F} \psi(A) Q_A(q; l) = \sum_{\substack{0 \leq t_1 \leq r_1 - 1, \\ \cdots \\ 0 \leq t_k \leq r_k - 1}} \psi(A_1)^{t_1} ... \psi(A_k)^{t_k} \sum_{m_1, m_2 = 1}^{q} e^{2\pi i \dfrac{l\left(a_1^{t_1} ... a_k^{t_k}, *, *\right)}{q}} .$$

Применяя к этому соотношению теорему1, будем иметь

$$\sum_{A \in Cl_F} \psi(A) G_A(q; l) = i^s \sqrt{d} \cdot q \left(\frac{l}{d}\right) \sum_{\substack{0 \leq t_1 \leq r_1 - 1, \\ \cdots \\ 0 \leq t_k \leq r_k - 1}} \psi(A_1)^{t_1} ... \psi(A_k)^{t_k} \left(\frac{a_1}{q}\right)^{t_1} ... \left(\frac{a_k}{q}\right)^{t_k} =$$

$$= i^s \sqrt{d} \cdot q \left(\frac{l}{d}\right) \prod_{j=1}^{k} \sum_{0 \leq t_j \leq r_j - 1} \psi(A_j)^{t_j} \cdot \left(\frac{a_j}{q}\right)^{t_j} .$$

Но $\sum_{t_j=0}^{r_j-1} \psi(A_j)^{t_j} \left(\frac{a_j}{q}\right)^{t_j} = 0$, так как эта сумма соответствует циклической группе классов идеалов, и значит,

$$\sum_{A\in Cl_F} \psi(A)\, G_A(q;l) = 0\,.$$

4. Общий случай абелевой группы Cl_F при четном q. Если $2||q$, то, в силу леммы 13 из статьи [6], сразу же получаем, что

$$\sum_{A\in Cl_F} \psi(A)\, G_A(q;l) = 0\,.$$

Поэтому нам достаточно рассмотреть лишь случаи $q \equiv 0 \pmod 4$. При таких четных q мы будем рассматривать случай $|D|/4 \equiv \pm 1 \,(\mathrm{mod} 4)$ и $|D|/8 \equiv \pm 1 \,(\mathrm{mod} 4)$ и значит, $(q, D) > 1$.

Как и в случае нечетного q и циклической группы Cl_F, проведя аналогичные рассуждения, в силу теоремы 2, относящейся к случаю $|D|/4 \equiv \pm 1 \,(\mathrm{mod} 4)$, будем иметь

$$\sum_{A\in Cl_F} \psi(A)\, G_A(q;l) = \gamma_d \sum_{k=0}^{h-1} \varepsilon^k i^{q_1 l a^k} \cdot \left(\frac{a^k}{d}\right) =$$

$$= \gamma_d \cdot i^{\pm q_1 l} \sum_{k=0}^{h-1} \varepsilon^k \left(\frac{a^k}{d}\right) = 0 \quad \text{при} \quad |D|/4 \equiv 1 \,(\mathrm{mod} 4)\,.$$

Здесь учитывалось, что $a \equiv \pm 1 \pmod 4$.

Аналогично, если $|D|/4 \equiv \pm 1 \pmod 4$, то

$$\sum_{A\in Cl_F} \psi(A)\, G_A(q;l) = \gamma_d(q,l,D) \sum_{k=0}^{h-1} \varepsilon^k \left(\frac{a}{d}\right)^k = \frac{\varepsilon^h \left(\frac{a^h}{d}\right) - 1}{\varepsilon \left(\frac{a}{d}\right) - 1} = 0\,,$$

т.к. $\left(a^h, *, *\right)$ — форма, эквивалентная главной форме.

Наконец, в оставшемся случае $|D|/8 \equiv \pm 1 \pmod 4$ также устанавливается, что

$$\sum_{A\in Cl_F} \psi(A)\, G_A(q;l) = 0$$

в случае цикличности Cl_F. Но тогда, аналогично случаю нечетного q, получаем, что для абелевой группы Cl_F

$$\sum_{A\in Cl_F} \psi(A)\, G_A(q;l) = 0\,.$$

Таким образом, в случае $(q, D) \geq 1$ и произвольной группы классов Cl_F, справедлива

Теорема 3. *Для группы классов идеалов Cl_F любого мнимого квадратичного поля $F = Q\left(\sqrt{d}\right)$, где $d < 0$ справедливо соотношение*

$$\sum_{A \in Cl_F} \psi(A)\, G_A(q; l) = 0\,,$$

где ψ — мультипликативный характер группы Cl_F.

Замечание. Если НОД $(\delta_F, q) = 1$, то указанный результат сводится к известному свойству для суммы значений характера па всех элементах группы Cl_F, поскольку в этом случае двойная сумма Гаусса $G_A(q,l)$ не зависит от класса идеала и пет необходимости в использовании композиции бипарых квадратичных форм.

Литература

1. Боревич З.И., Шафаревич И.Р. Теории чисел / М., 1985.
2. Гекке Э. Лекции по теории алгебраических чисел / М.-Л., 1940.
3. Лидл Р. Нидеррайтер Г. Конечные ноля. Т.1 / М.: Мир, 1988.
4. Касселс Дж. Рациональные квадратичные формы / М.: Мир, 1982.
5. Венков Б.А. Элементарная теория чисел / М.-Л.: ОНТИ, 1937.
6. Пачев У.М., Дохов Р.А. О двойных суммах Гаусса, соответствующих классом идеалов мнимого квадратичного ноля // Научные ведомости БелГУ. Математика. Физика. – 2013. – №19(162); Вып.32. – С.108-119.
7. Эдвардс Г. Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел / М.: «Мир», 1980.

ABOUT NULLIFICATION OF THE SUM ON IDEAL CLASSES GROUP CONNECTED WITH IMAGINARY QUADRATIC FIELD

R.A. Dohov

Kabardino-Balkar state University,
Chernishevsky St., 173, Nalchik, 360004, Russia, e-mail: urusbi@rambler.ru

Abstract. It is proved, using the classes co$\left(\sqrt{d}\right)$tion theory of binary quadratic forms, that the sum $\sum\limits_{A \in Cl} \Psi(A) G_A(q,l)$ of compositions of mu…cative character ψ of the ideal classes group connected with any imaginary quadratic field $F = Q\left(\sqrt{d}\right)$, $d < 0$ on double Gauss sums $G_A(q,l)$ is equal to zero.

Key words: group of characters, class of ideals, double Gauss sum, composition of classes, binary quadratic form, imaginary quadratic field.