УДК 511.6

Обобщенные суммы для характеров и их применения к законам взаимности

И. В. Решетуха

1. Обобщенные суммы для характеров и их связь с гауссовыми суммами. Пусть p — простое нечетное число, $\zeta = e^{\frac{2\pi i}{p}}$ — аналитически нормированный p-й корень из единицы, $\chi, \sigma, \ldots, \varphi, \psi$ — совокупность n характеров по $\bmod p$, порядки которых являются делителями числа $p-1$. Пусть имеем сравнение

$$F(x, y, \ldots, z, t) = ax + by + \ldots + cz + dt \equiv q \pmod p, \tag{1}$$

где $a, b, \ldots, c, d$ и q — рациональные числа, не сравнимые с 0 по $\bmod p$. Для характеров $\chi, \sigma, \ldots, \varphi, \psi$ определим сумму

$$S = S(\chi, \sigma, \ldots, \varphi, \psi; F; q) = \sum\nolimits_1 \chi(x)\sigma(y)\ldots\varphi(z)\psi(t), \tag{2}$$

распространенную на все различные решения $(x, y, \ldots, z, t)$ сравнения (1).

Покажем, что существует связь суммы (2) с гауссовыми суммами, принадлежащими характерам χ, σ, $\ldots$, φ, ψ и $\chi\sigma\ldots\varphi\psi$.

Пусть ε — главный характер по $\bmod p$. Для гауссовой суммы

$$\tau(\chi; \zeta^m) = \sum_{x(\bmod p)} \chi(x)\zeta^{mx}, \quad \chi \neq \varepsilon, \quad m \not\equiv 0 \pmod p$$

известны соотношения

$$\tau(\chi; \zeta^m) = \overline{\chi}(m)\tau(\chi; \zeta), \tag{3}$$

$$\tau(\chi; \zeta)\tau(\overline{\chi}; \zeta) = \chi(-1)p. \tag{4}$$

Лемма. *Для n характеров $\chi \neq \varepsilon$, $\sigma \neq \varepsilon, \ldots, \varphi \neq \varepsilon$, $\psi \neq \varepsilon$ имеем*

$$S = \frac{\tau(x; \zeta^a)\tau(\sigma; \zeta^b)\ldots\tau(\varphi; \zeta^c)\tau(\psi; \zeta^d)}{\tau(\chi\sigma\ldots\varphi\psi; \zeta^q)}, \text{ если } \chi\sigma\ldots\varphi\psi \neq \varepsilon, \tag{5}$$

и

$$S = -\frac{1}{p}\tau(\chi; \zeta^a)\tau(\sigma; \zeta^b)\ldots\tau(\varphi; \zeta^c)\tau(\psi; \zeta^d), \text{ если } \chi\sigma\ldots\varphi\psi = \varepsilon. \tag{6}$$

Доказательство. Принимая во внимание (3), представим значения характеров в формуле (2) в виде отношений

$$\chi(x) = \frac{\overline{\tau}(\overline{\chi}; \zeta^x)}{\tau(\overline{\chi}; \zeta)}, \quad \sigma(y) = \frac{\tau(\overline{\sigma}; \zeta^y)}{\tau(\overline{\sigma}; \zeta)}, \ldots, \varphi(z) = \frac{\tau(\overline{\varphi}; \zeta^z)}{\tau(\overline{\varphi}; \zeta)},$$

$$\psi(t) = \frac{\tau(\overline{\psi}; \zeta^t)}{\tau(\overline{\psi}; \zeta)}.$$

Тогда имеем

$$S = \frac{1}{M}\sum\nolimits_1 \tau(\overline{\chi}; \zeta^x)\tau(\overline{\sigma}; \zeta^y)\ldots\tau(\overline{\varphi}; \zeta^z)\tau(\overline{\psi}; \zeta^t) = \frac{1}{M}\sum\nolimits_1 \sum_{u,v,\ldots,w,\gamma} \overline{\chi}(u)\overline{\sigma}(v)\ldots$$

$$\ldots\overline{\varphi}(w)\overline{\psi}(\gamma)\zeta^{ux+vy+\ldots+wz+\gamma t} = \frac{1}{M}\sum_{u,v,\ldots,w,\gamma} \overline{\chi}(u)\overline{\sigma}(v)\ldots$$

$$\ldots \overline{\varphi}(w)\,\overline{\psi}(\gamma)\sum_{1}\zeta^{ux+vy+\ldots+wz+\gamma r},$$

где

$$M=\tau(\overline{\chi};\zeta)\,\tau(\overline{\sigma};\zeta)\ldots\tau(\overline{\varphi};\zeta)\,\tau(\overline{\psi};\zeta).$$

Все различные решения сравнения (1) мы можем получить таким образом: придавая $x, y, \ldots, z$ различные произвольные значения по $\bmod p$, t будем находить из сравнения

$$t\equiv\frac{q}{d}-\frac{a}{d}x-\frac{b}{d}y-\ldots-\frac{c}{d}z\pmod p.$$

Следовательно,

$$S=\frac{1}{M}\sum_{u,v,\ldots,w,\gamma,}\overline{\chi}(u)\,\overline{\sigma}(v)\ldots\overline{\varphi}(w)\,\overline{\psi}(\gamma)\zeta^{\frac{q}{d}\gamma}\times$$

$$\times\sum_{x,y,\ldots,z}\zeta^{\left(u-\frac{a}{d}\gamma\right)x+\left(v-\frac{b}{d}\gamma\right)y+\ldots+\left(w-\frac{c}{d}\gamma\right)z}. \tag{7}$$

При фиксированных $y, \ldots, z$ сумма

$$\sum_{x}\zeta^{\left(u-\frac{a}{d}\gamma\right)x+\left(v-\frac{b}{d}\gamma\right)y+\ldots+\left(w-\frac{c}{d}\gamma\right)z}$$

отлична от 0 только при $u\equiv\frac{a}{d}\gamma\pmod p$ и равняется в этом случае

$$p\zeta^{\left(v-\frac{a}{d}\gamma\right)y+\ldots+\left(w-\frac{c}{d}\gamma\right)z}.$$

Благодаря этому, равенство (7) принимает вид

$$S=\frac{p}{M}\sum_{v,\ldots,w,\gamma}\overline{\chi}\left(\frac{a}{d}\gamma\right)\overline{\sigma}(v)\ldots\overline{\varphi}(w)\,\overline{\psi}(\gamma)\,\zeta^{\frac{q}{d}\gamma}\times$$

$$\sum_{y,\ldots,z}\zeta^{\left(v-\frac{b}{d}\gamma\right)y+\ldots+\left(w-\frac{c}{d}\gamma\right)z}.$$

Поступая аналогично с переменными $y, \ldots, z$, получим

$$S=\frac{p^{n-1}}{M}\sum_{\gamma}\overline{\chi}\left(\frac{a}{d}\gamma\right)\overline{\sigma}\left(\frac{b}{d}\gamma\right)\ldots\overline{\varphi}\left(\frac{c}{d}\gamma\right)\overline{\psi}(\gamma)\,\zeta^{\frac{q}{d}\gamma}=$$

$$=\frac{p^{n-1}\overline{\chi}(a)\,\overline{\sigma}(b)\ldots\overline{\varphi}(c)}{M\overline{\chi}\,\overline{\sigma}\ldots\overline{\varphi}(d)}\sum_{\gamma}\overline{\chi}\,\overline{\sigma}\ldots\overline{\varphi}\,\overline{\psi}(\gamma)\,\zeta^{\frac{q}{d}\gamma}.$$

Отсюда имеем

$$S=\frac{p^{n-1}\tau(\overline{\chi}\,\overline{\sigma}\ldots\overline{\varphi}\,\overline{\psi};\zeta^{q})}{\tau(\overline{\chi};\zeta^{a})\,\tau(\overline{\sigma};\zeta^{b})\ldots\tau(\overline{\varphi};\zeta^{c})\,\tau(\overline{\psi};\zeta^{d})},\quad\text{если }\chi\sigma\ldots\varphi\psi\neq\varepsilon, \tag{8}$$

и

$$S=-\frac{p^{n-1}}{\tau(\overline{\chi};\zeta^{a})\,\tau(\overline{\sigma};\zeta^{b})\ldots\tau(\overline{\varphi};\zeta^{c})\,\tau(\overline{\psi};\zeta^{d})},\quad\text{если }\chi\sigma\ldots\varphi\psi=\varepsilon. \tag{9}$$

Принимая во внимание соотношения (3) и (4), имеем

$$\tau(\bar{\chi};\zeta^a)=\frac{\chi(-1)p}{\tau(\chi;\zeta^a)},\ \ldots,\ \tau(\bar{\psi};\zeta^d)=\frac{\psi(-1)p}{\tau(\psi;\zeta^d)},$$

$$\tau(\bar{\chi}\bar{\sigma}\ldots\bar{\varphi}\bar{\psi};\zeta^q)=\frac{\chi\sigma\ldots\varphi\psi(-1)p}{\tau(\chi\sigma\ldots\varphi\psi;\zeta^q)}.$$

Следовательно, делая в равенствах (8) и (9) соответствующую замену, получаем равенства (5) и (6).

Установленную связь между суммами для характеров и гауссовыми суммами можно применять при рассмотрении законов взаимности. Это мы покажем далее на примерах квадратичного и кубического законов взаимности.

Пусть сравнение (1) имеет вид

$$x+y+\ldots+z+t\equiv q\pmod p, \tag{10}$$

где q — целое рациональное число с $q>1$, $(p,q)=1$, и число переменных $x, y, \ldots, z, t$ равняется q. Для характера $\chi\neq\varepsilon$ определим сумму

$$S(\chi;q)=\sum\nolimits_1\chi(xy\ldots zt), \tag{11}$$

распространенную на все различные решения сравнения (10). В силу леммы имеем

$$S(\chi;q)=\begin{cases}\dfrac{\tau(\chi;\zeta)^q}{\tau(\chi^q;\zeta^q)} & \text{при } \chi^q\neq\varepsilon,\\ -\dfrac{1}{p}\tau(\chi;\zeta)^q & \text{при } \chi^q=\varepsilon.\end{cases} \tag{12}$$

Рассмотрим теперь сумму (11), предполагая, что q — простое рациональное число, отличное от p. Пусть $(x_0, y_0, \ldots, z_0, t_0)$ — некоторое решение сравнения (10). Переставляя не сравнимые по mod p элементы местами, мы будем получать различные решения сравнения (10). Число таких решений будет вычисляться по формуле

$$k=\frac{q!}{n_1!\,n_2!\ldots n_f!},$$

где $n_1, n_2, \ldots, n_f$ — количества сравнимых по mod p элементов среди $x_0, y_0, \ldots, z_0, t_0 (n_1+n_2+\ldots+n_f=q)$. Если среди элементов $x_0, y_0, \ldots, z_0, t_0$ есть хотя бы два не сравнимых по mod p, то в силу предыдущего равенства число k кратно q. Если же все элементы сравнимы, то

$$x_0\equiv y_0\equiv\ldots\equiv z_0\equiv t_0\equiv 1\pmod p,\quad k=1,\quad \chi(x_0y_0\ldots z_0t_0)=1.$$

Учитывая все это, имеем

$$S(\chi;q)=1+q\eta, \tag{13}$$

где η — целое число поля $Q(\xi)$, $\xi^l=1$ (l — порядок характера χ).

Аналогичным путем убеждаемся, что и

$$S(\chi;q^m)=1+q\eta', \tag{13'}$$

где m — целое положительное число, η' — целое число поля $Q(\xi)$.

2. Квадратичный закон взаимности. Для квадратичной гауссовой суммы

$$\tau(\zeta^q)=\sum_{x(\bmod p)}\left(\frac{x}{p}\right)\zeta^{qx}$$

имеем соотношения

$$\tau(\zeta^q) = \left(\frac{q}{p}\right)\tau(\zeta), \quad \tau(\zeta)^2 = (-1)^{\frac{p-1}{2}} p.$$

Применяя соотношения (12) и (13), получим

$$1 + q\eta = \frac{\tau(\zeta)^q}{\left(\frac{q}{p}\right)\tau(\zeta)} = \frac{\tau(\zeta)^{q-1}}{\left(\frac{q}{p}\right)},$$

$$\left(\frac{q}{p}\right)(1 + q\eta) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}},$$

где η — целое рациональное число.

Рассматривая последнее равенство по mod q, получим квадратичный закон взаимности

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

3. Кубический закон взаимности. Для полного овладения кубическим законом взаимности мы должны рассматривать целые числа поля $Q(\varrho)$, где $\varrho = \frac{-1+\sqrt{-3}}{2}$ — кубический корень из единицы. Целые числа α этого поля имеют вид $\alpha = a + b\varrho$, где a и b — целые рациональные. Норма α вычисляется по формуле

$$N(\alpha) = \alpha\bar{\alpha} = a^2 - ab + b^2.$$

Единицами поля являются числа ± 1, $\pm\varrho$, $\pm\varrho^2$. Для целых чисел поля $Q(\varrho)$ справедлива теорема об однозначном разложении на простые множители. Имеет место следующий закон разложения:

а) простое рациональное число $p \equiv 1 \pmod 3$ разлагается на два простых ω и $\bar{\omega}$ поля $Q(\varrho)$ с $N(\omega) = N(\bar{\omega}) = p$;

б) простое рациональное число $q \equiv -1 \pmod 3$ является простым числом поля $Q(\varrho)$ с $N(q) = q^2$;

в) число три ассоциированно с квадратом простого числа $1 - \varrho$ и $N(1 - \varrho) = 3$.

Пусть λ — простой, отличный от $1 - \varrho$ модуль. Для всякого целого числа α поля $Q(\varrho)$, не делящегося на λ, имеем сравнение

$$\alpha^{\frac{N(\lambda)-1}{3}} \equiv \varrho^j \pmod\lambda \quad (j = 0, 1, 2).$$

Число α, для которых $j = 0$ (и только они), являются кубическими вычетами по mod λ. Пользуясь предыдущим сравнением, определяем кубический символ числа α по λ, полагая

$$c(\alpha, \lambda) = \varrho^j.$$

Из определения кубического символа следуют такие его свойства:

1) $c(\alpha, \lambda) = c(\alpha_1, \lambda)$, если $\alpha \equiv \alpha_1 \pmod\lambda$;

2) $c(\alpha, \lambda) = c(\alpha, \lambda')$, если λ ассоциированно с λ';

3) кубический символ является мультипликативной функцией от первой переменной, т. е. $c(\alpha\beta, \lambda) = c(\alpha, \lambda)\, c(\beta, \lambda)$;

4) $c(-1, \lambda) = c(1, \lambda) = 1$;

5) $c(\bar{\alpha}, \bar{\lambda}) = \bar{c}(\alpha, \lambda) = c(\alpha, \lambda)^2 = c(\alpha, \lambda)^{-1}$.

Рассмотрим также обобщенный кубический символ. Пусть Λ — произвольное целое число поля $Q(\rho)$, не делящееся на $1 - \rho$, и $\Lambda = \lambda_1, \lambda_2 \ldots \lambda_m$ — разложение его на простые множители (среди них могут быть

одинаковые или ассоциированные). Тогда обобщенный кубический символ числа α по Λ определяется равенством

$$c(\alpha, \Lambda) = c(\alpha, \lambda_1)\, c(\alpha, \lambda_2) \ldots c(\alpha, \lambda_m).$$

Нетрудно убедиться, что свойства 1) — 5) имеют место и для обобщенного кубического символа.

Кубический символ рационального числа x по простому модулю ω ($\omega\bar{\omega} = p \equiv 1 \pmod 3$) совпадает со значением $\chi(x)$ кубического характера χ по $\bmod p$, для которого имеет место обобщенный критерий Эйлера

$$\chi(x) \equiv x^{\frac{p-1}{3}} \pmod{\omega}.$$

Для кубической гауссовой суммы $\tau(\chi, \zeta)$ известно соотношение

$$\tau(\chi, \zeta)^3 = p\omega, \quad \omega\bar{\omega} = p. \tag{14}$$

Рассмотрим сумму $S(\chi; 3)$. Применяя соотношения (12), (13) и (14), получим

$$1 + 3\eta = -\frac{1}{p}\tau(\chi, \zeta)^3 = -\omega,$$

где η — целое число поля $Q(\rho)$. Отсюда имеем сравнение

$$\omega \equiv -1 \pmod 3.$$

Из шести чисел $\pm\alpha$, $\pm\rho\alpha$, $\pm\rho^2\alpha$, ассоциированных с данным целым числом α, не делящимся на $1 - \rho$, существует одно и только одно сравнимое с -1 по $\bmod 3$. Такое число назовем первичным. Простое рациональное число $q \equiv -1 \pmod 3$ является вещественным первичным простым числом поля $Q(\rho)$, а число ω, входящее в равенство (14), является мнимым первичным простым числом поля $Q(\rho)$.

Т е о р е м а (кубический закон взаимности). *Для двух первичных простых чисел λ и λ_1 ($\lambda \neq \lambda_1$) всегда имеем*

$$c(\lambda, \lambda_1) = c(\lambda_1, \lambda).$$

Д о к а з а т е л ь с т в о. Рассмотрим все возможные случаи.

Пусть $\lambda = q$, $\lambda_1 = q_1$, где q и q_1 — простые рациональные числа с $q \equiv q_1 \equiv -1 \pmod 3$. В этом случае имеем

$$q^{\frac{q_1^2-1}{3}} = (q^{\frac{q_1+1}{3}})^{q_1-1} \equiv 1 \pmod{q_1},$$

и, следовательно, $c(q, q_1) = 1$. Поменяв местами числа q и q_1, убеждаемся, что и $c(q_1, q) = 1$.

Пусть снова $\lambda = q$, а $\lambda_1 = \omega$ с $N(\omega) = p \equiv 1 \pmod 3$. Рассмотрим сумму $S(\chi; q^2)$, где χ — кубический характер по $\bmod p$, соответствующий числу ω. Применяя соотношения (12), (13′) и (14), получим

$$1 + q\eta = \frac{\tau(\chi, \zeta)^{q^2}}{\tau(\chi^{q^2}, \zeta^{q^2})} = \frac{\tau(\chi, \zeta)^{q^2-1}}{\chi(q)},$$

$$\chi(q)(1 + q\eta) = (p^{\frac{q+1}{3}})^{q-1}\omega^{\frac{q^2-1}{3}},$$

где η — целое число поля $Q(\rho)$. Рассмотрим последнее равенство по $\bmod q$. Учитывая, что $\chi(q) = c(q, \omega)$ и $\omega^{\frac{q^2-1}{3}} \equiv c(\omega, q) \pmod q$, мы имеем

$$c(q, \omega) \equiv c(\omega, q) \pmod q, \quad c(q, \omega) = c(\omega, q).$$

Пусть теперь $\lambda = \omega$ с $N(\omega) = p$, $\lambda_1 = \omega_1$ с $N(\omega_1) = p_1$, где p и p_1 — различные простые рациональные числа, сравнимые с единицей по mod 3. Рассмотрим сумму $S(\chi, p)$, где χ — кубический характер по mod p, соответствующий числу ω. Применяя соотношения (12) — (14), в этом случае получим

$$1 + p_1\eta = \frac{\tau(\chi;\zeta)^{p_1}}{\tau(\chi^{p_1}, \zeta^{p_1})} = \frac{\tau(\chi;\zeta)^{p_1-1}}{\overline{\chi}(p_1)},$$

$$\overline{\chi}(p_1)(1 + p_1\eta) = p^{\frac{p_1-1}{3}}\omega^{p_1-1} = (\omega^{\frac{p_1-1}{3}})^2\omega^{\frac{p_1-1}{3}},$$

где η — целое число поля $Q(\varrho)$. Рассмотрим последнее равенство по mod ω_1. Учитывая, что

$$\overline{\chi}(p_1) = c(p_1, \overline{\omega}), \quad \omega^{\frac{p_1-1}{3}} \equiv c(\omega, \omega_1) \quad \text{и} \quad \overline{\omega}^{\frac{p_1-1}{3}} \equiv c(\overline{\omega}, \omega_1) \pmod{\omega_1},$$

имеем

$$c(p_1, \overline{\omega}) \equiv c(\omega, \omega_1)^2 c(\overline{\omega}, \omega_1) \pmod{\omega_1},$$

$$c(\omega_1, \overline{\omega})\, c(\overline{\omega}, \overline{\omega}) = c(\overline{\omega}, \overline{\omega}_1)\, c(\overline{\omega}, \omega_1).$$

Воспользуемся еще равенством

$$c(\omega, \overline{\omega}_1)\, c(\overline{\omega}, \overline{\omega}_1) = c(\overline{\omega}_1, \overline{\omega})\, c(\overline{\omega}_1, \omega),$$

которое получаем, поменяв в предыдущем равенстве числа ω и ω_1 местами. Из этих двух последних равенств получаем

$$c(\overline{\omega}_1, \overline{\omega})^2 = c(\overline{\omega}, \overline{\omega}_1)^2, \quad c(\omega_1, \omega) = c(\omega, \omega_1).$$

Таким образом, мы показали, что теорема справедлива для любых первичных λ и λ_1 с $N(\lambda) \neq N(\lambda_1)$.

Заметим теперь, что если числа Λ и Λ_1 поля $Q(\rho)$ можно представить в виде произведения первичных простых чисел и при этом $N(\Lambda)$ и $N(\Lambda_1)$ не имеют общих целых рациональных делителей, отличных от ± 1, то

$$c(\Lambda, \Lambda_1) = c(\Lambda_1, \Lambda).$$

Если же числа Λ и Λ_1 еще и рациональные, то

$$c(\Lambda, \Lambda_1) = c(\Lambda_1, \Lambda) = 1.$$

Воспользуемся этим замечанием при доказательстве теоремы в случае $\lambda = \omega$, $\lambda_1 = \overline{\omega}$, $\omega\overline{\omega} = p$. Пусть $\omega = a + b\varrho$ с целыми рациональными a и b. Тогда имеем

$$\overline{\omega} = a + b\varrho^2 \equiv 2a - b \pmod{\omega},$$

$$c(\overline{\omega}, \omega) = c(2a - b, \omega), \quad c(2a - b, \omega)^2 = c(2a - b, \omega^2) = c(\omega^2, 2a - b).$$

Но $\omega^2 \equiv a^2 - b^2 \pmod{(2a - b)}$, следовательно,

$$c(2a - b, \omega)^2 = c(a^2 - b^2, 2a - b) = 1, \quad c(\overline{\omega}, \omega) = c(\omega, \overline{\omega}) = 1.$$

Теперь теорема полностью доказана.

Применение сумм для характеров к законам взаимности дает значительные упрощения. Так, например, при доказательстве квадратичного закона взаимности с помощью гауссовой суммы [1] приходится рассматривать теорию сравнений поля $Q(\zeta)$, $\zeta^p = 1$. Применяя суммы для характеров, мы обходимся теорией сравнений рационального поля Q.

При доказательстве кубического закона взаимности мы обходимся теорией сравнений поля $Q(\rho)$.

ЛИТЕРАТУРА

1. Г. Хассе, Лекции по теории чисел, ИЛ, М., 1953.
2. G. Eisenstein, Beweis des Reziprozitätssatzes für die kubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten komplexen Zahlen, J. math., 27, 1844, 289—310.

Поступила 11.VI 1969 г.
Институт кибернетики АН УССР