Записки научных
семинаров ПОМИ
Том 458, 2017 г.

**Н. В. Проскурин**

# О КУБИЧЕСКИХ ЭКСПОНЕНЦИАЛЬНЫХ СУММАХ И СУММАХ ГАУССА

Для конечного поля $\mathbb{F}_q$ порядка $q$, пусть $e_q\colon \mathbb{F}_q \to \mathbb{C}^\star$ – нетривиальный аддитивный характер, $\chi\colon \mathbb{F}_q^\star \to \mathbb{C}^\star$ – характер мультипликативной группы $\mathbb{F}_q^\star$ поля $\mathbb{F}_q$. Соответствующие суммы Гаусса суть

$$G(c;\chi) = \sum_{z\in\mathbb{F}_q^\star} e_q(cz)\,\chi(z) \quad \text{с} \quad c\in\mathbb{F}_q \tag{1}$$

и, в частности,

$$G(\chi) = G(1;\chi) = \sum_{z\in\mathbb{F}_q^\star} e_q(z)\,\chi(z). \tag{2}$$

Если $q \equiv 1\,(\mathrm{mod}\ 3)$, то среди характеров $\chi$ группы $\mathbb{F}_q^\star$ есть два кубических (т.е. порядка 3) характера. Кубическими называют и соответствующие им суммы Гаусса. Следуя стандартной практике, продолжим характеры группы $\mathbb{F}_q^\star$ до функций на $\mathbb{F}_q$, полагая $\chi(0) = 1$ для единичного характера $\chi$ и полагая $\chi(0) = 0$ для всех других $\chi$. Положим

$$C(w) = \sum_{z\in\mathbb{F}_q} e_q\Big(\frac{z^3}{w} - 3z\Big) \quad \text{с} \quad w\in\mathbb{F}_q,\ \ w\neq 0. \tag{3}$$

В этой статье мы выводим соотношение связывающее кубические экспоненциальные суммы (3) с кубическими суммами Гаусса (1), (2).

**Теорема.** *Пусть $\psi$ – кубический характер поля $\mathbb{F}_q$, $q \equiv 1\,(\mathrm{mod}\ 3)$. Для любых $a$, $b\in\mathbb{F}_q^\star$ имеет место равенство*

$$\frac{1}{q}\sum_{n\in\mathbb{F}_q^\star} C(an)\,C(bn)\,\psi(n) + \frac{1}{q}\,\psi(ab)\,G(\psi)^2 = \overline{\psi}(ab)\,\psi(a-b)\,\overline{G(\psi)} \tag{4}$$

*и, в частности,*

$$G(\psi)^2 = -\sum_{n\in\mathbb{F}_q^\star} C(n)^2\,\psi(n). \tag{5}$$

*Ключевые слова*: сумма Гаусса, конечное поле, кубическая экспоненциальная сумма.

Если $a = b$, то правая часть (4) равна 0, так как $\psi(0) = 0$. Формула (5) есть не что иное, как (4) с $a = b = 1$.

Введём в рассмотрение суммы Клостермана

$$Kl(w;\chi) = \sum_{x\in\mathbb{F}_q^\star} e_q(x^{-1} + wx)\,\chi(x)$$

с параметром $w \in \mathbb{F}_q$ и с характером $\chi$ группы $\mathbb{F}_q^\star$. Следующее общее утверждение доказано в работе автора [1].

*Пусть $\mu$ и $\nu$ – характеры группы $\mathbb{F}_q^\star$, $\rho = \mu\bar{\nu}$. Тогда*

$$\frac{1}{q}\sum_{n\in\mathbb{F}_q^\star} Kl(an;\mu)\,\overline{Kl(bn;\nu)}\,\rho(n) + \frac{1}{q}\,G(a;\mu)\,\overline{G(b;\nu)} = G(c;\rho) \qquad (6)$$

*для всех $a, b \in \mathbb{F}_q$ с $ab \neq 0$, $c = a - b$.*

Для доказательства (4) мы воспользуемся этой формулой с кубическими характерами $\mu$ и $\nu$. При этом суммы Клостермана могут быть выражены через кубические экспоненциальные суммы следующей формулой, принадлежащей Иванцу и Дюку [2].

*Пусть $\psi$ – кубический характер поля $\mathbb{F}_q$, $q \equiv 1 \pmod 3$. Тогда*

$$Kl(w;\psi) = \psi(w)\,C(w) \quad \textit{с любым} \quad w \in \mathbb{F}_q,\ w \neq 0. \qquad (7)$$

В доказательстве этой формулы, данном в [2], существенную роль играет соотношение Дэвенпорта–Хассе.

Пусть $\psi$ и $\overline{\psi}$ – кубические характеры группы $\mathbb{F}_q^\star$, $q \equiv 1 \pmod 3$. Рассмотрим (6) с $\mu = \psi$, $\nu = \overline{\psi}$, $\rho = \psi^2 = \overline{\psi}$. Для сумм Гаусса в (6) имеем

$$G(c;\rho) = \psi(a-b)\,G(\overline{\psi}),$$
$$G(a;\mu)\,\overline{G(b;\nu)} = \overline{\psi}(ab)\,G(\psi)\,\overline{G(\overline{\psi})},$$

так как $G(c,\chi) = \overline{\chi}(c)\,G(\chi)$ для всех $c \in \mathbb{F}_q$ и всех характеров $\chi$, исключая единичный. Также, см. [4], если характер $\chi$ не единичный, имеем

$$G(\overline{\chi}) = \chi(-1)\,\overline{G(\chi)} \qquad \text{и} \qquad |G(\chi)|^2 = q.$$

В частности, $G(\overline{\psi}) = \overline{G(\psi)}$, так как $\psi(-1) = 1$. Приняв это во внимание, мы можем переписать (6) как[1]

$$\frac{1}{q}\sum_{n\in\mathbb{F}_q^\star} Kl(an;\psi)\,\overline{Kl(bn;\overline{\psi})}\,\overline{\psi}(n) + \frac{1}{q}\,\overline{\psi}(ab)\,G(\psi)^2 = \psi(a-b)\,\overline{G(\psi)}. \quad (8)$$

Применением формулы (7) с $\psi$ и с $\overline{\psi}$, мы находим, что сумма по $n$ в левой части (8) равна

$$\sum_{n\in\mathbb{F}_q^\star} C(an)\,\overline{C(bn)}\,\psi(abn). \quad (9)$$

Подставив (9) в формулу (8) и умножив все компоненты формулы на $\overline{\psi}(ab)$, получаем

$$\frac{1}{q}\sum_{n\in\mathbb{F}_q^\star} C(an)\,\overline{C(bn)}\,\psi(n) + \frac{1}{q}\,\psi(ab)\,G(\psi)^2 = \overline{\psi}(ab)\psi(a-b)\,\overline{G(\psi)} \quad (10)$$

и, в частности, при $a = b = 1$,

$$\sum_{n\in\mathbb{F}_q^\star} |C(n)|^2\,\psi(n) = -G(\psi)^2. \quad (11)$$

Очевидно, все суммы (3) вещественные. Для доказательства (4) и (5) остаётся заменить $\overline{C(bn)}$ и $|C(n)|^2$ на $C(bn)$ и $C(n)^2$ в (10) и в (11).

Нашим формулам можно дать иное доказательство, не использующее суммы Клостермана. Вычислим, например, левую часть в (11). Вместо сумм Клостермана и формул (6) и (7) нам будут нужны суммы Якоби и формулы (12) и (13).

*Если $\psi$ – кубический характер группы $\mathbb{F}_q^\star$, $q \equiv 1 \pmod 3$, то*

$$\frac{1}{q}\,G(\psi)^3 = J(\psi,\psi) \quad (12)$$

*с суммой Якоби в правой части.*

Напомним, что сумма Якоби $J(\mu,\nu)$, для пары характеров $\mu$ и $\nu$ группы $\mathbb{F}_q^\star$, определяется равенством

$$J(\mu,\nu) = \sum_{z\in\mathbb{F}_q} \mu(z)\,\nu(1-z).$$

[1] В [3] (лемма 6) доказана формула, которая, с точностью до обозначений, является частным случаем (8) соответствующим простому $q$ и $a = b = 1$.

Свойства сумм Якоби, включая формулу (12), см. в [4]. Ещё одна нужная нам формула доказана в [5].

*Пусть $\psi$ – кубический характер группы $\mathbb{F}_q^\star$, $q \equiv 1 \pmod 3$. С любыми $a, d, c, d \in \mathbb{F}_q$ имеем*

$$\sum_{z\in\mathbb{F}_q} \psi\big(az^3 + bz^2 + cz + d\big) = -\psi(a) + h\,\psi(\Delta)\,J(\psi,\psi), \tag{13}$$

*где $\Delta = b^2c^2 + 18abcd - 4ac^3 - 4b^3d - 27a^2d^4$ есть дискриминант бинарной кубической формы $au^3 + bu^2v + cuv^2 + dv^3$ и $h = 1$, если поле разложения этой формы есть $\mathbb{F}_q$ или $\mathbb{F}_{q^3}$, $h = -1$, если поле разложения этой формы есть $\mathbb{F}_{q^2}$.*

Обратимся к левой части формулы (11). Имеем

$$\begin{aligned}
\sum_{n\in\mathbb{F}_q^\star} |C(n)|^2\psi(n) &= \sum_{n\in\mathbb{F}_q^\star} \Big\{\sum_{y\in\mathbb{F}_q} e_q\Big(\frac{y^3}{n} - 3y\Big)\Big\}\overline{\Big\{\sum_{z\in\mathbb{F}_q} e_q\Big(\frac{z^3}{n} - 3z\Big)\Big\}}\,\psi(n)\\
&= \sum_{y,z\in\mathbb{F}_q} e_q(-3y+3z) \sum_{n\in\mathbb{F}_q^\star} e_q\Big(\frac{y^3}{n} - \frac{z^3}{n}\Big)\,\psi(n)\\
&= \sum_{y,z\in\mathbb{F}_q} e_q(-3y+3z) \sum_{m\in\mathbb{F}_q^\star} e_q\big(m(y^3 - z^3)\big)\,\overline{\psi}(m)\\
&= \sum_{y,z\in\mathbb{F}_q} e_q(-3y+3z)\,G(y^3 - z^3; \overline{\psi}) = G(\overline{\psi})\,R(\psi), \qquad (14)
\end{aligned}$$

где положено

$$R(\psi) = \sum_{y,z\in\mathbb{F}_q} e_q(-3y+3z)\,\psi(y^3 - z^3).$$

В последней сумме выделим слагаемые с $z = 0$ и сделаем замену $y = zu$ в слагаемых с $z \neq 0$. Так находим

$$\begin{aligned}
R(\psi) &= \sum_{y\in\mathbb{F}_q} e_q(-3y)\,\psi(y^3) + \sum_{\substack{u,z\in\mathbb{F}_q\\ z\neq 0}} e_q(-3zu+3z)\,\psi(z^3u^3 - z^3)\\
&= \sum_{\substack{y\in\mathbb{F}_q\\ y\neq 0}} e_q(-3y) + \sum_{\substack{u,z\in\mathbb{F}_q\\ z\neq 0}} e_q(-3zu+3z)\,\psi(u^3 - 1)\\
&= -1 + \sum_{u\in\mathbb{F}_q} \psi(u^3-1) \sum_{\substack{z\in\mathbb{F}_q\\ z\neq 0}} e_q\big(3z(1-u)\big)
\end{aligned}$$

$$= -1 - \sum_{u\in\mathbb{F}_q} \psi(u^3-1) = -J(\psi,\psi), \tag{15}$$

где последнее равенство получено применением формулы Райта (13). Из (14) и (15) следует, что левая часть в (11) равна

$$G(\overline{\psi})\, J(\psi,\psi). \tag{16}$$

Так как $G(\overline{\psi}) = \overline{G(\psi)}$ и $|G(\psi)|^2 = q$, из формулы (12) следует, что (16) равно $G(\psi)^2$, как и утверждается в (11).

## Литература


1. Н. В. Проскурин, *О суммах Клостермана с характерами.* — Зап. научн. семин. ПОМИ **302** (2003), 96–106. (English translation: *Convolutions of twisted Kloosterman sums*, Journal of Mathematical Sciences, **129**, No. 3, 2005)
2. W. Duke, H. Iwaniec, *A relation between cubic exponential and Kloosterman sums.* — Contemporary Mathematics **143** (1993), 255–258.
3. J. Booher, A. Etropolski, and A. Hittson, *Evaluations of cubic twisted Kloosterman sheaves.* — International J. Number Theory **6** (2010), 1349–1365.
4. K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Second eq. Grad. Texts in Math., 84. Springer-Verlag, 1990.
5. D. J. Wright, *Cubic character sums of cubic polynomials.* — Proc. Amer. Math. Soc. **100**, No. 3 (1987), 409–413.


Proskurin N. V. On cubic exponential sums and Gauss sums.

Let $e_q$ be a nontrivial additive character of a finite field $\mathbb{F}_q$ of order $q \equiv 1 \pmod 3$, and let $\psi$ be a cubic multiplicative character of $\mathbb{F}_q$, $\psi(0) = 0$. Consider the cubic Gauss sum and the cubic exponential sum

$$G(\psi) = \sum_{z\in\mathbb{F}_q} e_q(z)\,\psi(z), \quad C(w) = \sum_{z\in\mathbb{F}_q} e_q\Big(\frac{z^3}{w} - 3z\Big), \quad w \in \mathbb{F}_q,\ \ w \neq 0.$$

For all nonzero $a, b \in \mathbb{F}_q$, it is proved that

$$\frac{1}{q}\sum_n C(an)\,C(bn)\,\psi(n) + \frac{1}{q}\,\psi(ab)\,G(\psi)^2 = \overline{\psi}(ab)\,\psi(a-b)\,\overline{G(\psi)},$$

where summation runs over all nonzero $n \in \mathbb{F}_q$.


С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН
*E-mail*: np@pdmi.ras.ru


Поступило 13 сентября 2017 г.