Записки научных
семинаров ПОМИ
Том 479, 2019 г.

Н. В. Проскурин

О НЕКОТОРЫХ ТРИГОНОМЕТРИЧЕСКИХ СУММАХ В СВЯЗИ С ФУНКЦИЕЙ ЭЙРИ

§1. Введение

Мы рассмотрим комплексные функции на конечных полях и аналог дифференцирования из [1]. В этом контексте мы рассмотрим аналог уравнения Эйри, известного также как линеаризованное уравнение Кортевега–де Фриза. Для решений находится явное представление содержащее кубическую тригонометрическую сумму.

§2. Обозначения и основные функции

Для простого числа p, рассмотрим поле $\mathbb{F}_q$ – конечное расширение простого поля $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Здесь $q = p^l$ с некоторым целым $l \geqslant 1$.
Гомоморфизмы $\chi\colon \mathbb{F}_q^\star \to \mathbb{C}^\star$ мультипликативной группы $\mathbb{F}_q^\star$ поля $\mathbb{F}_q$ в мультипликативную группу $\mathbb{C}^\star$ поля комплексных чисел $\mathbb{C}$ продолжим на $\mathbb{F}_q$, положив $\chi(0) = 0$, и будем называть мультипликативными характерами поля $\mathbb{F}_q$. Пусть ϵ – тривиальный характер, $\epsilon(x) = 1$ для всех $x \in \mathbb{F}_q^\star$ и $\epsilon(0) = 0$.
Пусть $e_q\colon \mathbb{F}_q \to \mathbb{C}^\star$ – нетривиальный аддитивный характер поля $\mathbb{F}_q$.
Обозначим через Ω_q комплексное векторное пространство состоящее из функций $\mathbb{F}_q \to \mathbb{C}$ и снабжённое скалярным произведением

$$\langle f, g\rangle = \sum_{x\in\mathbb{F}_q} f(x)\overline{g(x)} \quad \text{для всех} \quad f, g \in \Omega_q.$$

Для всех $a, b \in \mathbb{F}_q$ и всех мультипликативных характеров α, β имеем

$$\sum_{z\in\mathbb{F}_q} e_q(az)\overline{e_q(bz)} = \begin{cases} q, & \text{если} \;\; a = b,\\ 0, & \text{в противном случае,}\end{cases}$$

$$\sum_{z\in\mathbb{F}_q^\star} \alpha(z)\overline{\beta(z)} = \begin{cases} q-1, & \text{если} \;\; \alpha = \beta,\\ 0, & \text{в противном случае.}\end{cases}$$

О конечных полях см. [2–4].

Ключевые слова: конечные поля, кубические тригонометрические суммы.

§3. Преобразования Фурье

Аддитивное преобразование Фурье функции $F\colon \mathbb{F}_q \to \mathbb{C}$ есть функция $\widehat{F}\colon \mathbb{F}_q \to \mathbb{C}$ определяемая равенством

$$\widehat{F}(x) = \sum_{y \in \mathbb{F}_q} F(y) e_q(yx) \quad \text{для всех } x \in \mathbb{F}_q. \tag{1}$$

Имеет место формула обращения

$$F(z) = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \widehat{F}(x) e_q(-xz) \quad \text{для всех } z \in \mathbb{F}_q. \tag{2}$$

§4. Суммы характеров

Мультипликативному характеру χ поля $\mathbb{F}_q$ сопоставим сумму Гаусса

$$G(\chi) = \sum_{x \in \mathbb{F}_q^*} e_q(x)\, \chi(x).$$

Хорошо известно (см. [3] и [4]), что $G(\epsilon) = -1$ и $G(\chi)\, G(\bar{\chi}) = \chi(-1)q$, $|G(\chi)|^2 = q$, если $\chi \neq \epsilon$. Для $a, b \in \mathbb{F}_q$ положим

$$B_q(a,b) = \sum_{y \in \mathbb{F}_q} e_q(-ay^3 - by). \tag{3}$$

Суммы такого вида были рассмотрены многими авторами. В частности, в [5] была обнаружена их связь с кубическими суммами Клостермана.

§5. Дифференцирование

Сопоставим каждому мультипликативному характеру χ поля $\mathbb{F}_q$ линейный оператор D^χ, который переводит функцию $F \in \Omega_q$ в функцию $D^\chi F \in \Omega_q$, определённую равенством

$$D^\chi F(x) = \frac{1}{G(\bar{\chi})} \sum_{t \in \mathbb{F}_q} \bar{\chi}(t)\, F(x-t) \quad \text{для всех} \quad x \in \mathbb{F}_q. \tag{4}$$

Это определение предложено в [1] как аналог дифференцирования. Согласно [1], $D^\chi F$ трактуется как производная порядка χ функции F.

Оператор D^χ с $\chi \neq \epsilon$ переводит постоянные функции в нулевую функцию. Легко выводятся формулы

$$D^\epsilon F(x) = F(x) - \sum_{t\in\mathbb{F}_q} F(t),$$

$$D^\chi D^{\bar\chi} F(x) = F(x) - \frac{1}{q}\sum_{t\in\mathbb{F}_q} F(t),$$

$$D^\alpha D^\beta = D^{\alpha\beta}$$

для всех $F \in \Omega_q$, $x \in \mathbb{F}_q$ и мультипликативных характеров α, β, χ под условиями $\chi \neq \epsilon$, $\alpha\beta \neq \epsilon$. Имеется также аналог формулы интегрирования по частям

$$\sum_{z\in\mathbb{F}_q} E(z)\, D^\nu F(z) = \nu(-1) \sum_{z\in\mathbb{F}_q} F(z)\, D^\nu E(z)$$

для всех мультипликативных характеров ν и всех $E, F \in \Omega_q$, $x \in \mathbb{F}_q$. Эти формулы можно найти в [1].

§6. Три леммы

Лемма 1. *Пусть $c \in \mathbb{F}_q^\star$, $d \in \mathbb{F}_q$. Рассмотрим композицию E функции $F\colon \mathbb{F}_q \to \mathbb{C}$ с функцией $x \mapsto cx + d$. Другими словами, пусть $E(x) = F(cx + d)$ для всех $x \in \mathbb{F}_q$. Тогда, для любого мультипликативного характера χ и любого $x \in \mathbb{F}_q$, имеем*

$$D^\chi E(x) = \chi(c) D^\chi F(cx + d). \tag{5}$$

В частности, если $E(x) = e_q(-cx)$ для всех $x \in \mathbb{F}_q$, то

$$D^\chi E(x) = \chi(c)\, E(x). \tag{6}$$

Доказательство. Формула (5) является простейшим аналогом классической формулы для производной сложной функции и следует непосредственно из определения (4). Её частный случай (6) соответствует $d = 0$ и $F(z) = e_q(-z)$. □

Лемма 2. *Пусть χ – нетривиальный мультипликативный характер поля $\mathbb{F}_q$. Рассмотрим дифференциальное уравнение $D^\chi E = RE$ с некоторым $R \in \mathbb{C}$. Его решения $E\colon \mathbb{F}_q \to \mathbb{C}$ суть всевозможные линейные комбинации функций $x \mapsto e_q(-cx)$ со всевозможными $c \in \mathbb{F}_q$ под условием $\chi(c) = R$. В частности, для примитивного характера*

χ имеется не более одного такого c. Если R не является значением характера χ, то уравнение имеет только нулевое решение.

Доказательство. Для функции $E\colon \mathbb{F}_q \to \mathbb{C}$, возьмём разложение по аддитивным характерам

$$E(x) = \sum_{c \in \mathbb{F}_q} r(c)\, e_q(-cx).$$

По линейности дифференцирования и лемме 1, выводим отсюда

$$D^\chi E(x) - RE(x) = \sum_{c \in \mathbb{F}_q} r(c)\{\chi(c) - R\}\, e_q(-cx).$$

Сумма справа равна 0 тождественно по $x \in \mathbb{F}_q$ в том и только в том случае если для каждого $c \in \mathbb{F}_q$ имеем либо $r(c) = 0$ либо $\chi(c) = R$, что и требовалось. □

Ещё одна лемма связывает аддитивное преобразование Фурье $\widehat{F}$ функции F с аддитивным преобразованием Фурье её производной.

Лемма 3. *Пусть χ – нетривиальный мультипликативный характер поля $\mathbb{F}_q$. Для каждой функции $F\colon \mathbb{F}_q \to \mathbb{C}$ и каждого $x \in \mathbb{F}_q$ имеем*

$$\sum_{y \in \mathbb{F}_q} D^\chi F(y) e_q(yx) = \chi(x) \widehat{F}(x). \tag{7}$$

Вместе с тем, имеем

$$\sum_{y \in \mathbb{F}_q} \underbrace{D^\chi \ldots D^\chi}_{m} F(y) e_q(yx) = \chi(x)^m\, \widehat{F}(x) \tag{8}$$

для каждого целого положительного числа m.

Доказательство. Для вычисления левой части (7) воспользуемся определением (4). Мы находим

$$\begin{aligned}
G(\bar\chi)\sum_{y\in\mathbb{F}_q} D^{\chi}F(y)e_q(yx) &= \sum_{y,t\in\mathbb{F}_q}\bar\chi(t)\,F(y-t)e_q(yx)\\
&= \sum_{t\in\mathbb{F}_q}\bar\chi(t)\sum_{y\in\mathbb{F}_q}F(y-t)e_q(yx)\\
&= \sum_{t\in\mathbb{F}_q}\bar\chi(t)e_q(tx)\sum_{y\in\mathbb{F}_q}F(y-t)e_q((y-t)x)\\
&= \Big\{\sum_{t\in\mathbb{F}_q}\bar\chi(t)e_q(tx)\Big\}\Big\{\sum_{y\in\mathbb{F}_q}F(y)e_q(yx)\Big\}.
\end{aligned}$$

В последней строке сумма по y равна значению $\widehat{F}(x)$ в точке x преобразования Фурье $\widehat{F}$ функции F, а сумма по t равна $\chi(x)G(\bar\chi)$. Это доставляет нам равенство (7). Равенство (8) следует из (7) индукцией по m. □

§7. Уравнение Эйри

Функция Эйри есть целая функция, определённая интегралом

$$Ai(z) = \frac{1}{2\pi}\int\limits_{\mathbb{R}} \exp\bigl(it^3/3 + izt\bigr)\,dt \quad \text{для всех } x\in\mathbb{R}$$

и удовлетворяющая уравнению $Ai''(z) = zAi(z)$ для всех $z\in\mathbb{C}$. Известная формула

$$w(x,t) = \frac{1}{(3t)^{1/3}}\int\limits_{\mathbb{R}} Ai\Bigl(\frac{x-y}{(3t)^{1/3}}\Bigr)v(y)\,dy, \quad x,t\in\mathbb{R},\ \ t>0,$$

представляет единственное решение уравнения Эйри

$$\frac{\partial w}{\partial t} + \frac{\partial^3 w}{\partial^3 x} = 0$$

с начальным условием

$$w(x,0) = v(x) \ \text{ для всех } \ x\in\mathbb{R}.$$

В качестве $v\colon\mathbb{R}\to\mathbb{R}$ здесь можно взять любую бесконечно дифференцируемую функцию с компактным носителем. Решение можно представить также преобразованием Фурье

$$w(x,t) = \frac{1}{2\pi}\int\limits_{\mathbb{R}}\Bigl\{\int\limits_{\mathbb{R}}\exp(-iky)\,v(y)\,dy\Bigr\}\exp(ikx+ik^3t)\,dk, \quad x,t\in\mathbb{R}.$$

§8. Смена контекста

Среди нетривиальных мультипликативных характеров χ поля $\mathbb{F}_q$ выберем какой-либо один и условимся обозначать через D соответствующий ему оператор дифференцирования D^χ. Для целого числа $m \geqslant 1$, определим D^m как композицию m операторов D. В частности, имеем $D^3F = DDDF = D^\chi D^\chi D^\chi F$ для всех $F\colon \mathbb{F}_q \to \mathbb{C}$. Для функции $F\colon \mathbb{F}_q \times \mathbb{F}_q \to \mathbb{C}$, обозначим через $D_k^m F$ результат применения D^m к F по k-ой переменной, $k = 1, 2$. В том же смысле мы используем обозначения типа $D_x^m F$ и $D_t^m F$, если переменные, вместо номеров, имеют обозначения x, t.

Теорема 1. *Для поля $\mathbb{F}_q$ и оператора дифференцирования D, соответствующего* (4) *примитивному мультипликативному характеру χ, рассмотрим задачу отыскания функции*

$$\begin{aligned} \mathbb{F}_q \times \mathbb{F}_q &\to \mathbb{C} \\ (x,t) &\mapsto w(x,t) \end{aligned} \tag{9}$$

удовлетворяющей дифференциальному уравнению

$$D_t w = C D_x^3 w \tag{10}$$

с константой $C \in \mathbb{C}$ и условию

$$w\big|_{t=0} = v \tag{11}$$

с некоторой функцией $v\colon \mathbb{F}_q \to \mathbb{C}$.
Если $C = \chi(c)$ с некоторым $c \in \mathbb{F}_q$, то функция

$$w(x,t) = \frac{1}{q} \sum_{n \in \mathbb{F}_q} B_q(ct, x-n)\, v(n) \qquad \text{для всех } x, t \in \mathbb{F}_q \tag{12}$$

является единственным решением задачи (10), (11). (*$B_q(\ldots)$ – кубическая сумма из* (3)). *Если константа C не является значением характера χ, то уравнение* (10) *не имеет решений помимо нулевого.*

Доказательство. Обозначим через $\tilde{w}$ функцию, получаемую из искомой функции (9) аддитивным преобразованием Фурье по первой переменной. Согласно определению (1), имеем

$$\tilde{w}(y,t) = \sum_{x \in \mathbb{F}_q} w(x,t) e_q(xy) \qquad \text{для всех} \;\; y, t \in \mathbb{F}_q. \tag{13}$$

Функция w восстанавливается по $\tilde{w}$ обратным преобразованием Фурье, а $\tilde{w}$ удовлетворяет обыкновенному дифференциальному уравнению

$$D_t\tilde{w}(y,t) = C\chi(y)^3\tilde{w}(y,t) \quad \text{для всех} \quad y,t \in \mathbb{F}_q. \tag{14}$$

Это легко пояснить. Дифференцируя почленно (13) находим, что производные по второй переменной функций $\tilde{w}$ и w связаны равенством

$$D_t\tilde{w}(y,t) = \sum_{x\in\mathbb{F}_q} D_t w(x,t)e_q(xy) \quad \text{для всех} \quad y,t \in \mathbb{F}_q. \tag{15}$$

По лемме 3, применённой к функции $x \mapsto w(x,t)$ (с фиксированным t и с $m=3$), находим

$$\chi(y)^3\tilde{w}(y,t) = \sum_{x\in\mathbb{F}_q} D_x^3 w(x,t)e_q(xy) \quad \text{для всех} \quad y,t \in \mathbb{F}_q. \tag{16}$$

Коэффициенты при $e_q(xy)$ в (15) и (16) связаны уравнением (10). Отсюда получаем равенство (14) для левых частей (15) и (16).
К уравнению (14) применим лемму 2 (с $R = C\chi(y)^3$). Если C не является значением характера χ, то, при любом $y \in \mathbb{F}_q$, уравнение (14) имеет только нулевое решение. Таким образом, $\tilde{w}$ – нулевая функция. Отсюда следует, что и функция w – нулевая. Пусть теперь $C = \chi(c)$ с некоторым $c \in \mathbb{F}_q$. Поскольку характер χ примитивен, c определяется по C однозначно. Общее решение уравнения (14) даётся формулой

$$\tilde{w}(y,t) = P(y)e_q(-tcy^3) \quad \text{для всех} \quad t,y \in \mathbb{F}_q \tag{17}$$

с произвольной функцией $P\colon \mathbb{F}_q \to \mathbb{C}$, не зависящей от t. Обратным преобразованием Фурье (2), из (17) выводим

$$\begin{aligned} w(x,t) &= \frac{1}{q}\sum_{y\in\mathbb{F}_q}\tilde{w}(y,t)e_q(-yx) \\ &= \frac{1}{q}\sum_{y\in\mathbb{F}_q} P(y)e_q(-tcy^3 - yx) \quad \text{для всех} \ t,x \in \mathbb{F}_q. \end{aligned} \tag{18}$$

В частности, взяв $t=0$ получаем

$$\frac{1}{q}\sum_{y\in\mathbb{F}_q} P(y)e_q(-yx) = u(x,0) = v(x) \quad \text{для всех} \ x \in \mathbb{F}_q.$$

Это означает, что P есть преобразование Фурье функции v, то есть

$$P(y) = \sum_{n\in\mathbb{F}_q} v(n)e_q(ny) \quad \text{для всех} \ y \in \mathbb{F}_q.$$

Подставив это в (18) получаем

$$
\begin{aligned}
w(x,t) &= \frac{1}{q}\sum_{y\in\mathbb{F}_q}\Big\{\sum_{n\in\mathbb{F}_q} v(n)e_q(ny)\Big\}\, e_q(-tcy^3-yx) \\
&= \frac{1}{q}\sum_{n\in\mathbb{F}_q}\Big\{\sum_{y\in\mathbb{F}_q} e_q(-tcy^3-(x-n)y)\Big\}\, v(n) \\
&= \frac{1}{q}\sum_{n\in\mathbb{F}_q} B_q(ct,x-n)\,v(n) \quad \text{для всех } t,x\in\mathbb{F}_q,
\end{aligned}
$$

что и требовалось. □

§9. Об L_2-норме решений

Возвращаясь к §7 напомним, что для решения w уравнения Эйри имеет место равенство

$$
\int\limits_{\mathbb{R}} w(x,t)^2\,dx = \int\limits_{\mathbb{R}} v(x)^2\,dx \quad \text{для всех} \quad t\in\mathbb{R}. \tag{19}
$$

Другими словами, норма функции w по пространственной переменной не зависит от времени. В конечном контексте, естественным аналогом (19) должно быть равенство

$$
\sum_{x\in\mathbb{F}_q} w(x,t)^2 = \sum_{x\in\mathbb{F}_q} v(x)^2 \quad \text{для всех} \quad t\in\mathbb{F}_q \tag{20}
$$

с w и v из (12) и (11). Мы обнаруживаем, что равенство (20) действительно имеет место. Без апелляции к дифференциальному уравнению, этот результат можно сформулировать и доказать следующим образом.

Теорема 2. *С любыми $c_n\in\mathbb{C}$ и $m\in\mathbb{F}_q$ имеем*

$$
\sum_{x\in\mathbb{F}_q}\Big|\sum_{n\in\mathbb{F}_q} c_n B_q(m,x-n)\Big|^2 = q^2\sum_{n\in\mathbb{F}_q}|c_n|^2.
$$

Доказательство. Для любых $n_1, n_2, m \in \mathbb{F}_q$ имеем

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_q} B_q(m, x-n_1)\,\overline{B_q(m, x-n_2)} \\
&= \sum_{x\in\mathbb{F}_q}\Big\{\sum_{y_1\in\mathbb{F}_q} e_q\big(-my_1^3-(x-n_1)y_1\big)\Big\}\overline{\Big\{\sum_{y_2\in\mathbb{F}_q} e_q\big(-my_2^3-(x-n_2)y_2\big)\Big\}} \\
&= \sum_{y_1,\,y_2\in\mathbb{F}_q} e_q(-my_1^3+my_2^3+n_1y_1-n_2y_2)\sum_{x\in\mathbb{F}_q} e_q(-xy_1+xy_2) \\
&= q\sum_{y\in\mathbb{F}_q} e_q((n_1-n_2)y) = \begin{cases} q^2 & \text{если } n_1 = n_2, \\ 0 & \text{в противном случае.}\end{cases}
\end{aligned}$$

Остаётся умножить на $c_{n_1}\bar{c}_{n_2}$ и просуммировать по $n_1, n_2 \in \mathbb{F}_q$. □

Список литературы

1. R. J. Evans, *Hermite character sums.* — Pacific J. Math. **122**, No. 2 (1986), 357–390.
2. Jean-Pierre Serre, *A Course d'arithmétique*, Presses Universitaires de France, Paris, 1970.
3. K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Grad. Texts in Math., 84. Springer-Verlag (1990).
4. R. Lidl, H. Niederreiter, *Finite fields*, Cambridge University Press, Second edition, 1997.
5. W. Duke, H. Iwaniec, *A relation between cubic exponential and Kloosterman sums.* — Contemporary Math. **143** (1993), 255–258.

Proskurin N. V. On some trigonometric sums related to the Airy function.

Complex functions over finite fields and analog to the Airy differential equation are considered. Solution is given in terms of some cubic trigonometric sums.

С.-Петербургское отделение
Математического института
им. В. А. Стеклова РАН,
набережная реки Фонтанки 27,
191023, С.-Петербург, Россия
E-mail: np@pdmi.ras.ru

Поступило 27 июня 2019 г.