Записки научных
семинаров ПОМИ
Том 468, 2018 г.

Н. В. Проскурин

О НЕКОТОРЫХ СПЕЦИАЛЬНЫХ ФУНКЦИЯХ НА КОНЕЧНЫХ ПОЛЯХ

§1. Введение

Известна аналогия между суммами Гаусса и суммами Якоби с одной стороны и гамма- и бета- функциями Эйлера с другой стороны. Также, скажем, суммы Клостермана аналогичны функциям Бесселя. Чтобы эту аналогию обнаружить, удобно трактовать арифметические суммы как комплексные функции определённые на конечных полях или на группах характеров конечных полей. В этом контексте были определены гипергеометрические функции [1] и ортогональные полиномы [2], было определено дифференцирование [2]. В работах многих авторов развита теория гипергеометрических функций на конечных полях и обнаружены связи этих функций с различными арифметическими объектами. Классические гипергеометрические функции определяют либо посредством представления степенными рядами либо как решения некоторых линейных дифференциальных уравнений, см. [3, 4]. Для этих рядов и уравнений нет необходимых аналогов в конечном контексте, то есть в рамках теории комплексных функций на конечных полях. Напротив, аналог находится для представляющего гипергеометрическую функцию интеграла Эйлера. Именно это представление является основным в [1]. Так же и в [2], для построения аналогов классических ортогональных полиномов использованы интегральные представления, но не реккурентные соотношения и не дифференциальные уравнения. Некоторые классические специальные функции удовлетворяют дифференциальным уравнениям, которые можно интерпретировать в конечном контексте. Это можно использовать для построения их аналогов без апелляции к каким-либо иным представлениям. Мы применим такой подход к построению конечных аналогов функции ошибок и неполной гамма-функции.

Ключевые слова: конечные поля, суммы характеров, функция ошибок, неполная гамма функция.

§2. Основные обозначения

Наши обозначения, в основном, совершенно стандартны. Фиксируем простое число p и конечное поле $\mathbb{F}_q$ из $q = p^l$ элементов с простым подполем $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Пусть $\mathbb{F}_q^\star$ – мультипликативная группа поля $\mathbb{F}_q$. Через $\widehat{\mathbb{F}}_q^\star$ обозначим группу мультипликативных характеров поля $\mathbb{F}_q$, то есть группу гомоморфизмов $\chi\colon \mathbb{F}_q^\star \to \mathbb{C}^\star$. Пусть ϵ – тривиальный характер, $\epsilon(x) = 1$ для всех $x \in \mathbb{F}_q^\star$. Продолжим каждый мультипликативный характер χ на $\mathbb{F}_q$ полагая $\chi(0) = 0$. В частности, $\epsilon(0) = 0$. Пусть $e_q\colon \mathbb{F}_q \to \mathbb{C}^\star$ – нетривиальный аддитивный характер. С некоторым $h \in \mathbb{F}_q^\star$, имеем $e_q(x) = \exp\bigl(2\pi i \operatorname{tr}(hx)/p\bigr)$ для всех $x \in \mathbb{F}_q$. Здесь tr обозначает след $\mathbb{F}_q \to \mathbb{F}_p$. Функцию $\delta\colon \mathbb{F}_q \to \mathbb{C}$ определим условиями $\delta(0) = 1$ и $\delta(x) = 0$ для всех $x \in \mathbb{F}_q^\star$.

Для мультипликативного характера χ, обозначим через $G(\chi)$ соответствующую сумму Гаусса, так что

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

При этом имеем

$$G(\epsilon) = -1 \quad \text{и} \quad G(\chi)\, G(\overline{\chi}) = \chi(-1)\, q \quad \text{для всех} \quad \chi \neq \epsilon. \tag{1}$$

О конечных полях и суммах Гаусса см. [5].

§3. Дифференцирование

Множество Ω_q всех комплексных функций на $\mathbb{F}_q$ снабдим, естественным образом, структурой комплексного векторного пространства и скалярным произведением

$$\langle F, E \rangle = \sum_{x \in \mathbb{F}_q} F(x) \overline{E(x)} \quad \text{for all} \quad F, E \in \Omega_q.$$

Каждому мультипликативному характеру η поля $\mathbb{F}_q$ сопоставим, следуя [2], линейный оператор D^η, который переводит функцию $F \in \Omega_q$ в функцию $D^\eta F \in \Omega_q$, определённую равенством

$$D^\eta F(x) = \frac{1}{G(\overline{\eta})} \sum_{t \in \mathbb{F}_q} F(t)\, \overline{\eta}(x - t) \quad \text{для всех} \quad x \in \mathbb{F}_q. \tag{2}$$

По формулам (1) это можно переписать также как

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

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

с F и x как и выше и с $\eta \neq \epsilon$. Согласно [2], $D^{\eta}F$ есть производная порядка η функции F. Это определение мотивировано аналогией с классической интегральной формулой Коши

$$\frac{1}{n!}\, f^{(n)}(z) = \frac{1}{2\pi i} \int \frac{f(t)\, dt}{(t-z)^{n+1}}$$

для производной $f^{(n)}$ порядка n функции f аналитической в окрестности точки z, с интегрированием вдоль пути обходящего z. Оператор $D^{\eta}F$ с $\eta \neq \epsilon$ переводит постоянные функции в нуль. Имеем

$$D^{\overline{\eta}} D^{\eta} F(x) = F(x) - \frac{1}{q} \sum_{t \in \mathbb{F}_q} F(t) \quad \text{для всех} \quad F \in \Omega_q, \quad x \in \mathbb{F}_q, \tag{3}$$

если только $\eta \neq \epsilon$. Для пары характеров α и β, если $\alpha\beta \neq \epsilon$, то $D^{\alpha} D^{\beta} = D^{\alpha\beta}$. Для пары функций $E, F \in \Omega_q$, $x \in \mathbb{F}_q$ и любого характера η имеем

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

(аналог формулы интегрирования по частям) и

$$D^{\eta} EF(x) = \frac{1}{q-1} \sum_{\theta \in \widehat{\mathbb{F}}_q^{\star}} \frac{G(\overline{\theta}) G(\theta\overline{\eta})}{G(\overline{\eta})}\, D^{\theta} E(x)\, D^{\eta\overline{\theta}} F(x).$$

(аналог правила Лейбница). Всё это имеется в [2].

§4. Функция ошибок

Функция ошибок erfc есть целая функция определяемая интегральным представлением

$$\operatorname{erfc}(z) = \frac{2}{\sqrt{\pi}} \int_z^{\infty} \exp(-t^2)\, dt \quad \text{для} \quad z \in \mathbb{C}. \tag{4}$$

Мы можем трактовать erfc как единственное решение дифференциального уравнения

$$w'(z) = -\frac{2}{\sqrt{\pi}} \exp(-z^2) \quad \text{с} \quad w(0) = 1. \tag{5}$$

Мы намерены построить комплексную функцию на $\mathbb{F}_q$, аналогичную erfc. Для этого, фиксируем некоторый мультипликативный характер $\nu \neq \epsilon$ и некоторую константу $c \in \mathbb{F}_q$, положим $f(t) = c\, e_q(t^2)$ для всех $t \in \mathbb{F}_q$ и рассмотрим дифференциальное уравнение

$$D^\nu w = f \tag{6}$$

относительно функции w, – аналог уравнения (5). Применим оператор $D^{\bar\nu}$ к обеим частям уравнения (6) и воспользуемся равенством (3). Так получаем

$$w = D^{\bar\nu} f + d$$

с некоторой константой $d \in \mathbb{F}_q$. Из определения (2) выводим

$$\begin{aligned} w(x) = D^{\bar\nu} f(x) + d &= \frac{c}{G(\nu)} \sum_{t\in\mathbb{F}_q} e_q(t^2)\, \nu(x-t) + d \\ &= \frac{c}{G(\nu)} \sum_{t\in\mathbb{F}_q} \nu(t)\, e_q\big((x-t)^2\big) + d. \end{aligned}$$

В выборе констант c и d мы свободны. Возьмем $c = G(\nu)$, $d = 0$. Соответствующую функцию w обозначим erfc_ν и назовём *функцией ошибок на конечном поле* $\mathbb{F}_q$,

$$\mathrm{erfc}_\nu(x) = \sum_{t\in\mathbb{F}_q} \nu(t)\, e_q\big((x-t)^2\big) \quad \textit{для всех } x \in \mathbb{F}_q. \tag{7}$$

Так определённая функция erfc_ν зависит от характера ν, выбранного произвольно и использованного в определении оператора дифференцирования D^ν.

§5. Неполная гамма-функция

Для неполной гамма-функции имеется интегральное представление

$$\Gamma(s+1, z) = \int_z^\infty e^{-x} x^s\, dx \quad \text{для } s \in \mathbb{C} \text{ и } z \in \mathbb{C} \setminus (-\infty, 0]. \tag{8}$$

С фиксированным $s \in \mathbb{C}$, функция $w = \Gamma(s+1, \cdot)$ является единственным решением дифференциального уравнения

$$w'(z) = -e^{-z} z^s \quad \text{с } w(0) = \Gamma(s+1). \tag{9}$$

Имея целью построить комплексную функцию на $\widehat{\mathbb{F}}_q^\star \times \mathbb{F}_q$, аналогичную неполной гамма-функции, мы можем действовать также, как и

выше при построении функции ошибок. Именно, фиксируем некоторый мультипликативный характер $\nu \neq \epsilon$. Оператор D^ν послужит нам дифференцированием, соответствующим дифференцированию первого порядка в (9). Наши построения зависят от выбора ν, так что фактически мы определим не одну функцию, а семейство функций

$$\Gamma_\nu \colon \widehat{\mathbb{F}}_q^\star \times \mathbb{F}_q \to \mathbb{C}. \tag{10}$$

Неполной гамма-функцией на конечном поле $\mathbb{F}_q$, *соответствующей мультипликативному характеру* ν, *назовём функцию* Γ_ν *определяемую равенством*

$$\Gamma_\nu(\mu, x) = \sum_{t \in \mathbb{F}_q} \mu(t)\,\nu(t-x)\,e_q(t) \quad \textit{для всех } \mu \in \widehat{\mathbb{F}}_q^\star \textit{ и } x \in \mathbb{F}_q. \tag{11}$$

Поясним основания для такого определения. Для мультипликативного характера μ и константы $c \in \mathbb{F}_q$, положим $f(t) = c\,e_q(t)\,\mu(t)$ для всех $t \in \mathbb{F}_q$ и рассмотрим дифференциальное уравнение

$$D^\nu w = f \tag{12}$$

относительно функции w, – аналог уравнения (9). Применим оператор $D^{\bar\nu}$ к обеим частям уравнения (12) и воспользуемся (3). Так получаем

$$w = D^{\bar\nu} f + d$$

с некоторой константой $d \in \mathbb{F}_q$. Из определения (2) выводим

$$w(x) = D^{\bar\nu} f(x) + d = \frac{c}{G(\nu)} \sum_{t \in \mathbb{F}_q} \mu(t)\,\nu(x-t)\,e_q(t) + d. \tag{13}$$

В выборе констант c и d мы свободны. С $c = G(\nu)\,\nu(-1)$ и $d = 0$ правая часть (13) есть в точности $\Gamma_\nu(\mu, x)$. Непосредственно из определения (11) видно, что

$$\Gamma_\nu(\mu, 0) = G(\mu\nu). \tag{14}$$

Это соответствует второму условию в (9). Для $x \neq 0$, заменой $t = xu$ в определении (11) выводим

$$\Gamma_\nu(\mu, x) = \mu(x)\,\nu(-x)\,G(\mu, \nu; x), \tag{15}$$

где положено

$$G(\mu, \nu; x) = \sum_{u \in \mathbb{F}_q} \mu(u)\,\nu(1-u)\,e_q(xu).$$

Из (14), (15) получаем *альтернативное представление нашей функции*: *для всех* $x \in \mathbb{F}_q$ *и* $\mu, \nu \in \widehat{\mathbb{F}_q^\star}$, $\nu \neq \epsilon$, *имеем*

$$\Gamma_\nu(\mu, x) = \mu(x)\,\nu(-x)\,G(\mu, \nu; x) + \delta(x)\,G(\mu\nu).$$

Список литературы

1. J. Greene, *Hypergeometric functions over finite fields*. — Transactions of the American Math. Soc. **301**, No. 1 (1987), 77–101.
2. R. J. Evans, *Hermite character sums*. — Pacific Journal of Mathematics **122**, No. 2 (1986), 357–390.
3. W. N. Bailey, *Generalized hypergeometric series*. Strechert–Hafner, New York, 1964.
4. F. W. J. Olver, *Introduction to asymptotics and special functions*. Academic Press, 1974.
5. K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*. Graduate Texts in Mathematics 87, Springer.

Proskurin N. V. On some special functions over finite fields.

A finite fields analogues of the classical error function and incomplete gamma function are defined as complex functions over finite fields.

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 14 августа 2018 г.