Записки научных
семинаров ПОМИ
Том 538, 2024 г.

Н. В. Проскурин

О РАСПРЕДЕЛЕНИИ НЕКОТОРЫХ ЭКСПОНЕНЦИАЛЬНЫХ СУММ

§1. Введение

Рассмотрим поле $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ простого порядка p, его аддитивный характер

$$x \mapsto e_p(x) = \exp(2\pi i x/p), \quad x \in \mathbb{F}_p,$$

полином f над $\mathbb{F}_p$ и аддитивную экспоненциальную сумму

$$S_p(f) = \sum_{x \in \mathbb{F}_p} e_p\big(f(x)\big). \tag{1}$$

Под условием $p \nmid \deg f$ имеет место неравенство Вейля $\big|\, S_p(f)\,\big| \leqslant C\sqrt{p}$ с $C = \deg f - 1$ и, значит,

$$S_p(f) = C\sqrt{p}\; E_p(f) \quad \text{с некоторыми} \quad E_p(f) \in D, \tag{2}$$

где $D = \big\{ z \in \mathbb{C} \,\big|\, |z| \leqslant 1 \big\}$ — единичный круг на комплексной плоскости. См. [1, 2].

Возьмём какой-либо полином f определёный над $\mathbb{Z}$. Посредством редукции его коэффициентов $\bmod p$, мы можем считать f полиномом над каждым из полей $\mathbb{F}_p$ и можем рассмотреть распределение точек $E_p(f)$. Для почти всех p, редукция $\operatorname{mod} p$ сохраняет степень $\deg f$ полинома f и $p \nmid \deg f$, так что точки $E_p(f)$ лежат в D.

Мы рассматривали в [3] и [4] суммы $S_p(f)$ и распределение точек $E_p(f)$ для кубических полиномов f над $\mathbb{Z}$. Было обнаружено экспериментально, а затем и доказано, что точки $E_p(f)$ концентрируются вдоль нескольких отрезков проходящих через 0. Мы сформулируем это более точно в §2.

В настоящей публикации, наша цель – предъявить ещё один класс экспоненциальных сумм с подобным распределением значений. Мы сообщаем в §3 о результатах численных экспериментов. Доказательства построены в частном случае, который будет рассмотрен в §4.

Ключевые слова: конечные поля, экспоненциальные суммы.

С принятыми выше обозначениями, исключим из рассмотрения $p = 2$, а для каждого нечётного простого числа p обозначим через κ_p единственный квадратичный характер мультипликативной группы $\mathbb{F}_p^\star$ поля $\mathbb{F}_p$ продолженный равенством $\kappa_p(0) = 0$ на всё поле $\mathbb{F}_p$. Пусть u и v – полиномы над $\mathbb{Z}$, $\deg u = 1$, $\deg v = 2$. Паре u, v сопоставим экспоненциальную сумму

$$S_p(u,v) = \sum_{x \in \mathbb{F}_p} \kappa_p\bigl(u(x)\bigr)\, e_p\bigl(v(x)\bigr). \tag{3}$$

В терминологии принятой в [1], такие суммы относятся к классу экспоненциальных сумм смешанного типа. Имеем $\bigl| S_p(u,v) \bigr| \leqslant C\sqrt{p}$ и, следовательно,

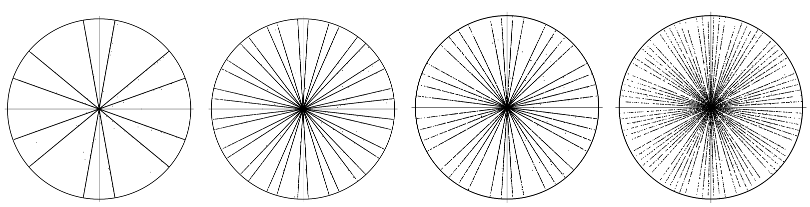
$$S_p(u,v) = C\sqrt{p}\, E_p(u,v) \quad \text{с некоторыми} \quad E_p(u,v) \in D \tag{4}$$

и с $C = \deg u + \deg v - 1 = 2$. Константы C в (4) и в (2) равны числу нулей L-функций Артина, соответствующих суммам (3) и (1), см. [1, 2].

§2. О кубических суммах

Для данного полинома f над $\mathbb{Z}$, пусть $E(f, X)$ – множество точек $E_p(f)$ с $p \leqslant X$ и пусть $E(f)$ – множество всех точек $E_p(f)$. Множества $E(f, X)$ с большим X могут служить аппроксимацией к предельному множеству $E(f)$ и могут служить визуализацией к проблеме распределения точек $E_p(f)$ в D.

Ниже, на рисунках, изображены вещественная и мнимая координатные оси, круг D и типичные множества $E(f, X)$ с $X = 400000$ для кубических полиномов f. Под каждым из рисунков выписан соответствующий ему полином.



$6x^3 + 3x^2 + 4x$ $\quad$ $2x^3 + 2x^2 + 3x$ $\quad$ $5x^3 + 3x^2 + 3x$ $\quad$ $7x^3 + 9x^2$

Точки $E_p(f)$, составляющие множество $E(f,X)$, расположены столь близко друг к другу, что их изображения сливаются, формируя некоторые фигуры – отрезки прямых, проходящих через 0. *В действительности, за редкими исключениями, точки $E_p(f)$ не лежат на этих отрезках, но только сконцентрированы вдоль них. Расстояние от точки $E_p(f)$ до ближайшего отрезка $\ll 1/p$. Обнаруживается также, что точки $E_p(f)$ концентрируются вдоль того или иного из этих отрезков в зависимости только от класса $p \bmod q$ с некоторым $q \mid 27\, l^3$, зависящем только от f. Здесь l – старший коэффициент полинома f.* Всё это было обнаружено экспериментально в [3] и было доказано в [4].

§3. О смешанных суммах

Пусть $a, b, c \in \mathbb{Z}$. Положим

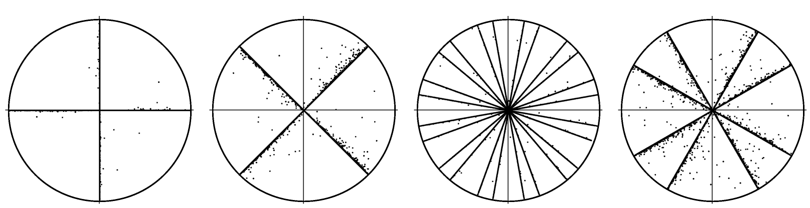
$$DQ_p(a,b,c) = \sum_{x\in\mathbb{F}_p} \kappa_p(ax+b)e_p(cx^2) \tag{5}$$

(D, Q – первые буквы слов *double* и *quadratic*). Сумма (5) есть не что иное, как $S_p(u,v)$ из (3) с $u(x) = ax+b$, $v(x) = cx^2$. При этом мы имеем

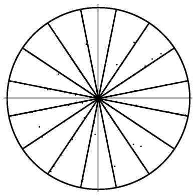
$$DQ_p(a,b,c) = 2\sqrt{p}\; E_p(a,b,c) \quad \text{с} \quad E_p(a,b,c) \in D \tag{6}$$

для всех простых p под условием $p \nmid 2\gcd(a,c)$.

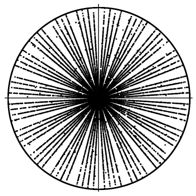
Рассмотрим распределение точек $E_p(a,b,c)$ в нескольких примерах, основанных на вычислительных экспериментах. Ниже, на рисунках, изображены вещественная и мнимая координатные оси, круг D и 20000 точек $E_p(a,b,c)$ с простыми нечётными $p \leqslant 224750$. Под каждым из рисунков выписаны соответствующие ему коэффициенты a, b, c.



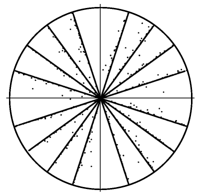
$a{=}b{=}c{=}1$ $\quad a=2,\ b{=}3,\ c{=}7$ $\quad a{=}3,\ b{=}2,\ c{=}4$ $\quad a{=}3,\ b{=}8,\ c{=}6$



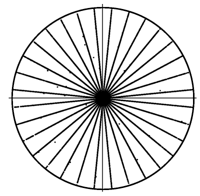
$a=4,\ b=3,\ c=1$



$a=5,\ b=4,\ c=6$



$a=5,\ b=6,\ c=5$



$a=8,\ b=3,\ c=2$

Во всех примерах мы встречаем распределение подобное распределению кубических сумм. Если задаться вопросом, что объединяет суммы (5) с кубическими суммами (1) и, возможно, отвечает за их распределение, то можно заметить, что L-функции Артина всех этих сумм имеют по 2 нуля. На первом рисунке, соответствующем коэффициентам $a = b = c = 1$, почти все точки лежат почти точно на осях координат. В следующем параграфе мы рассмотрим суммы $DQ_p(a, b, c)$ с $b = 0$ и увидим, что они все лежат в точности на осях координат. Общий случай, с $b \neq 0$, остаётся не исследованным.

§4. Несколько точных формул

Рассмотрим детально суммы (5) с $b = 0$. С точностью до множителя $\kappa_p(a) = \pm 1$, эти суммы зависят только от одного параметра c.

С любым $c \in \mathbb{Z}$ и с любым нечётным простым p, сумма

$$DQ_p(c) = \sum_{x \in \mathbb{F}_p} \kappa_p(x) e_p(cx^2) \tag{7}$$

лежит либо на вещественной оси $\mathbb{R}$ либо на мнимой оси $i\mathbb{R}$.

Мы докажем это утверждение и, по ходу дела, найдём два представления этих сумм через суммы Гаусса и докажем следующее неравенство.

С любым $c \in \mathbb{Z}$ и с любым нечётным простым p, имеет место неравенство

$$|DQ_p(c)| \leqslant 2\sqrt{p}. \tag{8}$$

Это неравенство в точности совпадает с тем, что доставляет, применительно к суммам (7), общая теория [1, 2].

Начнём с одного вспомогательного вычисления. Пусть g, h – полиномы над $\mathbb{Z}$ и $f = h \circ g$ – их композиция. Очевидно,

$$S_p(f) = \sum_{z \in \mathbb{F}_p} \sharp\big\{x \in \mathbb{F}_p \mid g(x) = z\big\}\, e_p\big(h(z)\big).$$

Если $g(x) = ux^2 + vx + w$ и $p \nmid u$, то

$$\sharp\big\{x \in \mathbb{F}_p \mid g(x) = z\big\} = 1 + \kappa_p\big(v^2 - 4u(w - z)\big)$$

и

$$S_p(f) = \sum_{z \in \mathbb{F}_p} e_p\big(h(z)\big) + \sum_{z \in \mathbb{F}_p} \kappa_p\big(v^2 - 4u(w - z)\big)\, e_p\big(h(z)\big). \tag{9}$$

С любым $c \in \mathbb{Z}$ и с любым нечётным простым p, имеем представление

$$DQ_p(c) = \sum_{z \in \mathbb{F}_p} e_p(cz^4) - \sum_{z \in \mathbb{F}_p} e_p(cz^2) \tag{10}$$

суммы (7) *разностью сумм Гаусса степеней* 2 *и* 4.

Это следует из формулы (9) с $g(x) = x^2$ и $h(z) = cz^2$.

С любым $c \in \mathbb{Z}$, если $p \equiv 3 \bmod 4$, то $DQ_p(c) = 0$.

Если x пробегает поле $\mathbb{F}_p$, то также и $-x$. С $p \equiv 3 \bmod 4$, имеем $\kappa_p(-x) = -\kappa_p(x)$,

$$DQ_p(c) = \sum_{x \in \mathbb{F}_p} \kappa_p(-x) e_p\big(c(-x)^2\big) = -DQ_p(c) \ \text{ и } \ DQ_p(c) = 0,$$

что и требовалось.

С любым простым нечётным p, если $c \equiv 0 \bmod p$, то $DQ_p(c) = 0$.

Для таких c, правая часть в (7) есть сумма значений характера κ_p распространённая на все элементы поля $\mathbb{F}_p$. Следовательно, $DQ_p(c) = 0$.

Рассмотрим теперь суммы Гаусса $G(\chi)$ с характерами χ группы $\mathbb{F}_p^\star$,

$$G(\chi) = \sum_{x \in \mathbb{F}_p^\star} \chi(x) e_p(x). \tag{11}$$

Нам будут нужны только две формулы

$$\overline{G(\chi)} = \chi(-1) G(\bar\chi) \quad \text{и} \quad |G(\chi)|^2 = p \tag{12}$$

для нетривиальных характеров χ, см. [2].

Пусть $p \equiv 1 \bmod 4$. *С любым* $c \in \mathbb{Z}$ *имеет место равенство*

$$DQ_p(c) = \bar{\eta}_p(c)\, G(\eta_p) + \eta_p(c)\, G(\bar{\eta}_p), \tag{13}$$

в котором η_p – *какой-либо из двух характеров порядка* 4 *группы* $\mathbb{F}_p^\star$ *дополненный соглашением* $\eta_p(0) = 0$.

Случай $c \equiv 0 \bmod p$ очевиден. Пусть $c \not\equiv 0 \bmod p$. Имеем $\eta_p^2 = \kappa_p$, $\eta_p^3 = \bar{\eta}_p$ и

$$\sum_{x \in \mathbb{F}_p^\star} e_p(cx^4) = \sum_{x \in \mathbb{F}_p^\star} \bigl\{1 + \eta_p(x) + \eta_p(x)^2 + \eta_p(x)^3\bigr\}\, e_p(cx),$$

$$\sum_{x \in \mathbb{F}_p^\star} e_p(cx^2) = \sum_{x \in \mathbb{F}_p^\star} \bigl\{1 + \eta_p(x)^2\bigr\}\, e_p(cx).$$

Вместе с формулой (10) это даёт

$$DQ_p(c) = \sum_{x \in \mathbb{F}_p^\star} \bigl\{\eta_p(x) + \bar{\eta}_p(x)\bigr\}\, e_p(cx).$$

Умножив обе части последнего равенства на $\eta_p(c)\, \bar{\eta}_p(c) = 1$ и заменив суммирование по x на суммирование по $z = cx$, получим

$$DQ_p(c) = \bar{\eta}_p(c) \sum_{z \in \mathbb{F}_p^\star} \eta_p(z)\, e_p(z) + \eta_p(c) \sum_{z \in \mathbb{F}_p^\star} \bar{\eta}_p(z)\, e_p(z),$$

а это и есть (13), см. (11).

Пусть $p \equiv 1 \bmod 4$. *С любым* $c \in \mathbb{Z}$, $c \not\equiv 0 \bmod p$, *имеет место равенство*

$$DQ_p(c)^2 = \kappa_p(c) \bigl\{G(\eta_p)^2 + \overline{G(\eta_p)}^2\bigr\} + 2(-1)^{(p-1)/4} p, \tag{14}$$

в котором, как и выше, η_p – *характер порядка* 4 *группы* $\mathbb{F}_p^\star$.

Для доказательства обратимся к равенству (13) и, возведением в квадрат, найдём

$$DQ_p(c)^2 = \kappa_p(c)\, G(\eta_p)^2 + \kappa_p(c)\, G(\bar{\eta}_p)^2 + 2G(\eta_p) G(\bar{\eta}_p).$$

По формулам (12), здесь $G(\bar{\eta}_p)^2 = \overline{G(\eta_p)}^2$ и $G(\eta_p) G(\bar{\eta}_p) = \eta_p(-1) p$. Остаётся заметить, что $\eta_p(-1)$ равно $(-1)^{(p-1)/4}$.

Утверждение относительно сумм $DQ_p(c)$, сформулированное в начале параграфа, эквивалентно $DQ_p(c)^2 \in \mathbb{R}$. Мы видели, что $DQ_p(c) = 0$ в случае $p \equiv 3 \bmod 4$ и в случае $c \equiv 0 \bmod p$. Во всех других случаях мы имеем равенство (14), в котором правая часть, очевидно, вещественна. Неравенство (8) следует немедленно из (13) и (12).

Пусть $p \equiv 1 \bmod 4$ *и* $c \in \mathbb{Z}$, $c \not\equiv 0 \bmod p$. *Если* $p \equiv 1 \bmod 8$, *то* $DQ_p(c) \in \mathbb{R}$. *Если* $p \equiv 5 \bmod 8$, *то* $DQ_p(c) \in i\mathbb{R}$.

Для доказательства, перепишем (14) как $DQ_p(c)^2 = 2(-1)^{(p-1)/4}p+X$, где $X \in \mathbb{R}$ и $|X| \leqslant 2p$, см. (12). Отсюда видно, что $DQ_p(c)^2 \geqslant 0$ для $p \equiv 1 \bmod 8$ и $DQ_p(c)^2 \leqslant 0$ для $p \equiv 5 \bmod 8$.

Список литературы

1. J.-P. Serre, *Majorations de sommes exponentielles*, Société Mathématique de France, Asterisque 41–42, p. 111–126, 1977.
2. С. А. Степанов, *Арифметика алгебраических кривых*, Москва, Наука, 1991.
3. Н. В. Проскурин, *О некоторых кубических экспоненциальных суммах.* — Записки научн. семин. ПОМИ **502** (2021), 122–132.
4. Н. В. Проскурин, *Распределение кубических экспоненциальных сумм.* — Записки научн. семин. ПОМИ **511** (2022), 161–170.

Proskurin N. V. On distribution of some exponential sums.

By numerical experiments, it is discovered some stricture in distribution of mixed exponential sums with quadratic characters in finite fields.

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

Поступило 15 ноября 2024 г.