Записки научных
семинаров ПОМИ
Том 547, 2025 г.

Н. В. Проскурин

О СУММАХ ЗНАЧЕНИЙ МУЛЬТИПЛИКАТИВНЫХ ХАРАКТЕРОВ ОТ КУБИЧЕСКИХ ПОЛИНОМОВ

Суммы над простыми конечными полями. Для поля $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ простого порядка p, пусть $\mathbb{F}_p^\star$ – его мультипликативная группа, e_p – его канонический аддитивный характер, $i = \sqrt{-1}$,

$$e_p(t \bmod p) = \exp(2\pi i t/p) \quad \text{для всех} \quad t \in \mathbb{Z}. \tag{1}$$

Полиномам f, g над $\mathbb{Z}$ и характерам ψ_p группы $\mathbb{F}_p^\star$ сопоставляем полиномиальные экспоненциальные суммы

$$S_p(f, g; \psi_p) = \sum_{t \in \mathbb{F}_p} \psi_p\big(f(t)\big)\, e_p\big(g(t)\big), \tag{2}$$

называемые также суммами характеров над полем $\mathbb{F}_p$. Здесь мы принимаем соглашение $\psi_p(0) = 1$ для тривиального ψ_p и $\psi_p(0) = 0$ для всех других ψ_p. Также, $e_p(t)$ и $\psi_p(t)$ с $t \in \mathbb{Z}$ понимаются как $e_p(t \bmod p)$ и $\psi_p(t \bmod p)$. Среди сумм (2) выделяют мультипликативные ($g = 0$), аддитивные (с тривиальным ψ_p) и смешанные (все другие) суммы.
При весьма общих предположениях[1] относительно полиномов и характеров, сумма (2) может быть выражена через нули соответствующей ей L-функции Артина и имеет место неравенство

$$|S_p(f, g; \psi_p)| \leqslant C_p \sqrt{p}\,, \tag{3}$$

где $C_p = m_p + n_p - 1$, $n_p = \deg(g \bmod p)$, $m_p = \deg(\mathrm{radical}(f \bmod p))$. Коэффициент C_p есть не что иное, как число нулей L-функции Артина. Пусть $n = \deg(g)$ и $m = \deg(\mathrm{radical} f)$. Тогда $n_p \leqslant n$, $m_p \leqslant m$ и точки

$$E_p(f, g; \psi_p) = \frac{1}{(m + n - 1)\sqrt{p}}\, S_p(f, g; \psi_p) \tag{4}$$

лежат в единичном круге $D = \big\{ z \in \mathbb{C} \;\big|\; |z| \leqslant 1 \big\}$. См. [1] и [2].

Ключевые слова: конечные поля, мультипликативные экспоненциальные суммы, распределение экспоненциальных сумм над конечными полями.

[1] Если $p \nmid n_p$, h – порядок характера ψ_p и $\gcd\big(\deg(f \bmod p), h\big) = 1$, то имеет место (3). Также, имеем (3) для мультипликативных сумм с характерами ψ_p порядка $h > 1$, если $f = g_1^{s_1} \dots g_r^{s_r}$, где полиномы g_j различны, неприводимы и $\gcd(h, s_1, \dots, s_r) = 1$.

Нас интересует распределение точек (4) в круге D. Более определённо, полиномы f, g и число $h \geqslant 1$, $h \in \mathbb{Z}$, фиксируем. Рассмотрим точки (4) соответствующие всевозможным характерам ψ_p порядка h и простым числам $p \equiv 1 \pmod h$ под условием $p \leqslant c$. Какую фигуру мы увидим при больших c или в пределе $c \to \infty$? Например, можем взять $h = 1$ и тривиальный характер ψ_p для каждого p. В случае $h = 2$ можно рассмотреть точки (4) с единственным квадратичным характером ψ_p для каждого нечётного простого числа p. В случае $h \geqslant 3$ и $p \equiv 1 \pmod h$ имеется более одного характера ψ_p порядка h. Мы можем рассмотреть точки (4) соответствующие всевозможным таким ψ_p или одному ψ_p, определённому каким-то принципом выбора.

Допустимые семейства характеров. Пусть $h, l \in \mathbb{Z}$ и $l \neq 0$, $h \geqslant 1$. Пусть w – примитивный корень из 1 степени h, $w \in \mathbb{C}$. Обозначим через $P_{h,l}$ множество всех тех простых чисел p, для которых поле $\mathbb{F}_p$ имеет один и только один мультипликативный характер χ_p под условиями $\operatorname{ord}(\chi_p) = h$ и $\chi_p(l) = w$. Легко видеть, что $P_{h,l}$ не зависит от произвола в выборе примитивного корня w и что $P_{h,l}$ есть подмножество множества P_h всех простых чисел $p \equiv 1 \pmod h$. Эквивалентно, для простого числа p имеем $p \in P_{h,l}$ если и только если $p \equiv 1 \pmod h$, $p \nmid l$ и h взаимно просто с индексом числа l относительно какой-либо образующей группы $\mathbb{F}_p^\star$. В частности, для простого числа h, последнее условие, касательно h, можно заменить на условие l не является h-той степенью в $\mathbb{F}_p^\star$.

Допустимым назовём семейство $\{\chi_p\}_{p \in P_{l,h}}$ характеров χ_p с общим значением $\chi_p(l) = w$ в точке l. Степенью, аргументом и значением такого семейства назовём параметры h, l и w. Для каждого такого семейства имеем последовательность точек $E_p(f, g; \chi_p)$, занумерованную простыми числами из $P_{l,h}$.

При фиксированных f, g и h, мы можем варьировать свободный параметр l и получать различные последовательности точек $E_p(f, g; \chi_p)$ с тем или иным распределением в единичном круге D. Поучительный пример допустимых семейств кубических характеров рассмотрен в [3] связи с суммами

$$\frac{1}{2\sqrt{p}} \sum_{t \in \mathbb{F}_p} \psi_p(t)\, e_p(t^2).$$

В этом примере, распределение точек существенно зависит от того, является ли l степенью числа 2.

Чтобы пояснить наше определение, сравним его с определением комплексного логарифма. Экспонента отображает $\mathbb{C}$ на область $\mathbb{C} \setminus \{0\}$, которая не является односвязной. Нет (неперерывной) ветви логарифна определённой на $\mathbb{C} \setminus \{0\}$. Пусть $\Delta \subset \mathbb{C}$ и $0 \in \Delta$. Если дополнение $\mathbb{C} \setminus \Delta$ оказывается односвязной областью, то существуют ветви логарифма определённые на этой области. Для любой точки $z \in \mathbb{C} \setminus \Delta$, ветвь логарифма на $\mathbb{C} \setminus \Delta$ определяется однозначно своим значением в z. Мы берём множество P_h всех простых чисел $p \equiv 1 \pmod h$ вместо комплексной плоскости $\mathbb{C}$. Множества $P_{l,h}$ играют роль односвязных областей. Имеем $P_{l,h} = P_h \setminus D_{l,h}$, если определить $D_{l,h}$ как множество всех простых чисел p под условиями $p \equiv 1 \pmod h$ и

$$p \mid l \quad \text{или} \quad \gcd(h, \text{индекс } l \text{ в } \mathbb{F}_p^\star) \neq 1.$$

Требование $\chi_p(l) = w$ играет роль условия непрерывности в определении ветвей.

Мультипликативные суммы с кубическими полиномами. Напомним, мультипликативными называют суммы (2) с нулевым g. Опустим нуль в обозначениях (2) и (4). Имеем представление

$$S_p(f; \psi_p) = \sum_{t \in \mathbb{F}_p} \psi_p\big(f(t)\big), \tag{5}$$

для мультипликативных сумм. Мы вычислили суммы (5) для многих случайно выбранных полиномов f степени 3 и для характеров ψ_p и простых чисел p в пределах $h = \operatorname{ord}(\psi_p) \leqslant 8$, $p \leqslant 800000$. Для соответствующих им точек (4) имеем представление

$$E_p(f; \psi_p) = \frac{1}{2\sqrt{p}}\, S_p(f; \psi_p) \tag{6}$$

с коэффициентом 2, исключая только вырожденные случаи с полиномами f, имеющими кратные корни.

Наши наблюдения можно суммировать следующим образом.

$\underline{h = 1.}$ В этом случае, характеры в (5) тривиальны и суммы равны числу слагаемых, т. е. $S_p(f; \psi_p) = p$.

$\underline{h = 2.}$ Значения квадратичных характеров в (5) суть 1, -1, 0. Суммы (5) принадлежат $\mathbb{Z}$, а соответствующие им точки (6) лежат на отрезке $[-1, 1]$ вещественной прямой $\mathbb{R}$.

$\underline{h = 3.}$ В этом случае, характеры в (5) – кубические. Их значения – 1, ω, ω^2, 0 с $\omega = \exp(2\pi i/3) = (-1 + \sqrt{-3})/2$. Суммы (5) оказываются

целыми числами поля $\mathbb{Q}(\sqrt{-3})$, а соответствующие им точки (6) выстраиваются в круге D вдоль окружности C радиуса $1/2$ с центром в нуле. Более определённо, мы увидим (11), что для полиномов f с ненулевым дискриминантом расстояние от точек $E_p(f;\psi_p)$ до окружности C убывает как $1/\sqrt{p}$ при $p\to\infty$.

$\underline{h=4.}$ В этом случае, характеры в (5) – биквадратичные, со значениями ±1, $\pm\sqrt{-1}$, 0. Суммы (5) оказываются целыми числами поля $\mathbb{Q}(\sqrt{-1})$ и, в частности, могут быть равны нулю. Соответствующие им точки (6), те из них, что отличны от нуля, обнаруживаются в круге D на окружностях радиусов $1/2$, $1/\sqrt{2}$ и 1 с общим центром в нуле.

$\underline{h=6.}$ Суммы (5) – целые числа поля $\mathbb{Q}(\sqrt{-3})$. Отличные от нуля точки (6) обнаруживаются в круге D на окружностях радиусов $1/2$ и 1 с общим центром в нуле.

Точные формулы. В некоторых частных случаях, мультипликативные суммы могут быть выражены через суммы Якоби $J(\mu,\nu)$ посредством достаточно простых формул. Напомним,

$$J(\mu,\nu)=\sum_{t\in\mathbb{F}_p}\mu(t)\nu(1-t) \tag{7}$$

для каждой пары мультипликативных характеров μ, ν поля $\mathbb{F}_p$. Вместе с тем, имеем:

$$|J(\mu,\nu)|=\sqrt{p}\quad\text{и}\quad J(\bar\nu,\nu)=-\nu(-1), \tag{8}$$

если характеры μ, ν, $\mu\nu$ нетривиальны; см. [5].

В рассматриваемом нами контексте (простых конечных полей и кубических полиномов) имеют место следующие две формулы. Первая из них может быть найдена в [5]. Вторая – была выведена Райтом в [4].

Пусть $f(x)=ax^3+d$ с $a,d\in\mathbb{Z}$ и пусть ψ_p – нетривиальный мультипликативный характер поля $\mathbb{F}_p$, $p\nmid ad$. Если $p\equiv1\,(\mathrm{mod}\ 3)$, то

$$S_p(f;\psi_p)=\psi_p(d)\big\{\bar\lambda(a/d)J(\lambda,\psi_p)+\lambda(a/d)J(\bar\lambda,\psi_p)\big\}, \tag{9}$$

где λ – какой-либо из двух кубических характеров $\mathbb{F}_p$. Если же $p\not\equiv1\,(\mathrm{mod}\ 3)$, то поле $\mathbb{F}_p$ не имеет кубических характеров, f – перестановочный полином над $\mathbb{F}_p$ и $S_p(f;\psi_p)=0$, см. [5].

Пусть ψ_p – кубический характер поля $\mathbb{F}_p$, $p\equiv1\,(\mathrm{mod}\ 3)$. Для кубического полинома $f(x)=ax^3+bx^2+cx+d$ над $\mathbb{Z}$, пусть

$$\Delta=b^2c^2+18abcd-4ac^3-4b^3d-27a^2d^2$$

– его дискриминант. Согласно Райту [4], если $p \nmid \Delta$, то

$$S_p(f;\psi_p) = -\psi_p(a) + \eta_p(\Delta)\psi_p(\Delta)J(\psi_p,\psi_p). \tag{10}$$

Здесь η_p – квадратичный характер поля $\mathbb{F}_p$. Отсюда следует

$$\Big| E_p(f;\psi_p) + \frac{\psi_p(a)}{2\sqrt{p}} \Big| = \frac{1}{2}\,, \tag{11}$$

см. (8) и (6). Таким образом, точки $E_p(f;\psi_p)$ расположены вблизи окружности C радиуса $1/2$ с центром в точке 0.

Иллюстрации. По данным h и f, проставим на комплексной плоскости $\mathbb{C}$ точки $E_p(f;\psi_p)$ со всевозможными характерами ψ_p порядка h и со всевозможными простыми $p \equiv 1 (\mathrm{mod}\, h)$ в пределах $p \leqslant X$ с каким-то большим X. Так мы сможем составить представление о распределении точек $E_p(f;\psi_p)$ в пределе с $X \to \infty$. Добавим к рисункам ещё вещественную и мнимую оси координат. Ниже мы приводим несколько типичных картинок и, затем, пояснения к каждой из них. Во всех случаях, $X = 800000$, а f – кубический полином общего вида без кратных корней.

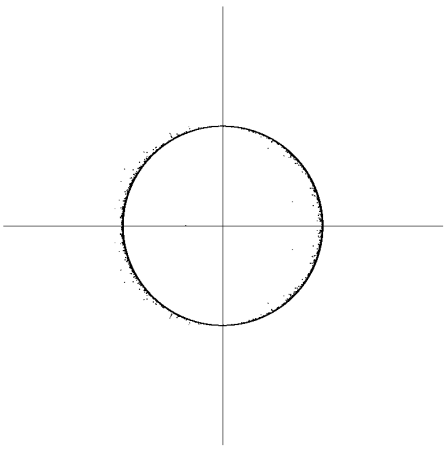

Рис. 1

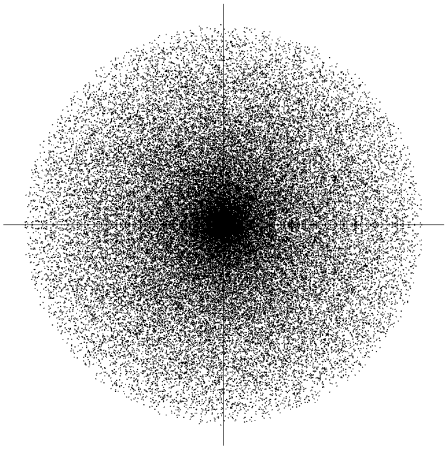

Рис. 2

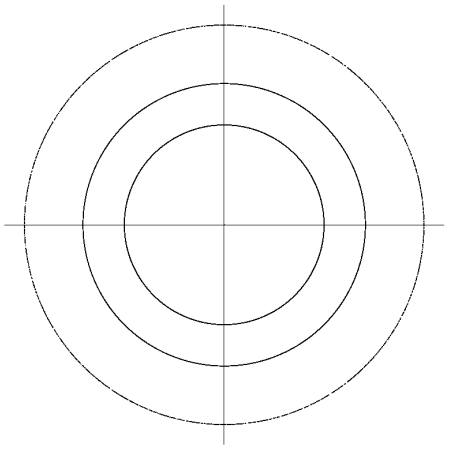

Рис. 3

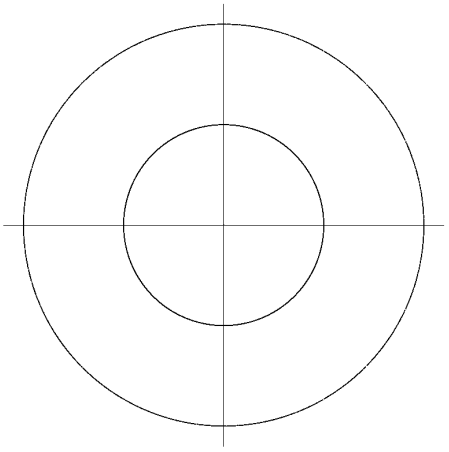

Рис. 4

Пояснения к рисункам.

Рис. 1. Здесь $h = 3$, все ψ_p – кубические характеры. Мы находимся в условиях [4] и имеем явные формулы (10) для сумм $S_p(f;\psi_p)$ и (11) для точек $E_p(f;\psi_p)$, которые сконцентрированы вдоль окружности $C = \{z \in \mathbb{C} \mid |z| = 1/2\}$. Это общее свойство присущее точкам $E_p(f;\psi_p)$ с кубическими полиномами f без кратных корней. Конкретно, рисунок построен по $f(x) = x^3 + 7x^2 + x - 5$.

Рис. 2. В случае $h > 3$, исключая $h = 4, 6, 10$, не обнаруживается какой-то ярко выраженной структуры в распределении точек $E_p(f;\psi_p)$. На рисунке представлен один типичный пример. Он построен по $h = 7$ и по полиному $f(x) = 5x^3 + 7x^2 - 13x + 1$.

Рис. 3. Здесь $h = 4$, все ψ_p – биквадратичные характеры. Рисунок построен по $f(x) = x^3 + x^2 - 7x + 1$. Каждая из точек $E_p(f;\psi_p)$, если отлична от нуля, то лежит на одной из трёх окружностей радиусов 1, $1/\sqrt{2}$ и $1/2$ с центрами в нуле. То же обнаруживается и для других полиномов f.

Рис. 4. Для $h = 6$, отличные от нуля точки $E_p(f;\psi_p)$ лежат на двух окружностях радиусов 1 и $1/2$ с центрами в нуле. Для многих полиномов f находятся также точки $E_p(f;\psi_p)$ равные 0. Конкретно, рисунок построен по $h = 6$ и $f(x) = -4x^3 + x^2 + 13x - 7$. Аналогичные рисунки имеем и в случае $h = 10$, но с четырьмя окружностями вместо двух.

Список литературы

1. J.-P. Serre, *Majorations de sommes exponentielles*. — Société Mathématique de France, Asterisque **41**–**42** (1977), 111–126.
2. С. А. Степанов, *Арифметика алгебраических кривых*, Москва, Наука, 1991.
3. Н. В. Проскурин, *Об экспоненциальных суммах и цветах*. — Зап. научн. семин. ПОМИ, **502** (2021), 133–138.
4. D. J. Wright, *Cubic character sums of cubic polynomials*. — Proc. of the AMS, **100**, No. 3 (1987).
5. R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, sec. ed., 1997.

Proskurin N. V. On multiplicative characters sums of cubic polynomials.

Exponential sums involving multiplicative characters of prime finite fields and cubic polynomials are considered and studied by means of numerical experiments. Some observations on distribution of the sums in the complex plane are given. A concept of admissible family of characters is introduced in this context.

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

Поступило 20 ноября 2025 г.