Записки научных
семинаров ПОМИ
Том 490, 2020 г.

Н. В. Проскурин

О СУММАХ ХАРАКТЕРОВ В КОНЕЧНЫХ ПОЛЯХ

§1. Суммы Клостермана и мера Сато–Тейта

Для простого числа p, рассмотрим $\mathbb{Z}/p\mathbb{Z}$ – конечное простое поле из p элементов и $e_p\colon \mathbb{F}_p \to \mathbb{C}^\star$ – нетривиальный аддитивный характер поля, то есть нетривиальный гомоморфизм аддитивной группы поля $\mathbb{Z}/p\mathbb{Z}$ в мультипликативную группу $\mathbb{C}^\star$ комплексного поля $\mathbb{C}$. Сумма

$$Kl_p(c) = \sum_{t\in\mathbb{Z}/p\mathbb{Z}\setminus\{0\}} e_p(t^{-1}+ct) \quad \text{с} \quad c\in\mathbb{Z} \tag{1}$$

есть известная сумма Клостермана. Согласно Вейлю, $|Kl_p(c)| \leqslant 2\sqrt{p}$. Мы имеем

$$\frac{Kl_p(c)}{2\sqrt{p}} \in [-1,1] \tag{2}$$

и можем рассмотреть вопрос о распределении точек (2) по отрезку вещественной оси $[-1,1]$.

На этом отрезке имеется вероятностная мера

$$[u,v] \;\mapsto\; \varrho_{st}(u,v) = \frac{2}{\pi}\int\limits_u^v \sqrt{1-t^2}\,dt \quad \text{для всех} \quad [u,v]\subset[-1,1],$$

известная как мера Сато-Тейта.

Если p пробегает простые числа $\leqslant x$ и $\pi(x)$ есть число всех таких p, то число дробей (2) в отрезке $[u,v]$ близко к $\varrho_{st}(u,v)\,\pi(x)$. Более точно, ожидается, что

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\sharp\Big\{p\leqslant x \;\Big|\; \frac{Kl_p(c)}{2\sqrt{p}}\in[u,v]\Big\} = \frac{2}{\pi}\int\limits_u^v\sqrt{1-t^2}\,dt \tag{3}$$

для всех $[u,v]\subset[-1,1]$, $c\in\mathbb{Z}$. Определив $\vartheta(p,c)$ как единственное число на отрезке $[0,\pi]$ под условием

$$Kl_p(c) = 2\sqrt{p}\,\cos\vartheta(p,c),$$

Ключевые слова: конечные поля, суммы характеров.

получаем тригонометрическую переформулировку гипотезы (3)

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\sharp\Big\{p\leqslant x\;\Big|\;\theta(p,c)\in[u,v]\Big\}=\frac{2}{\pi}\int\limits_u^v\sin^2 t\,dt \tag{4}$$

для всех $[u,v]\subset[0,\pi]$, $c\in\mathbb{Z}$.

§2. Полиномиальные суммы

Мультипликативному характеру χ_p поля $\mathbb{Z}/p\mathbb{Z}$ и паре многочленов a и b от одной переменной над $\mathbb{Z}$, сопоставим сумму[1]

$$S_p=\sum_{t\in\mathbb{Z}/p\mathbb{Z}}\chi_p(a(t))\,e_p(b(t)). \tag{5}$$

Мы намерены здесь рассмотреть возможные аналоги гипотезы (3), (4) применительно к полиномиальным суммам (5).

Напомним, что сумма Клостермана (1) относится к классу полиномиальных сумм (5), поскольку для неё имеется представление

$$Kl_p(c)=\sum_{t\in\mathbb{Z}/p\mathbb{Z}}\kappa_p(t^2-4c)\,e_q(t)$$

с квадратичным характером κ_p поля $\mathbb{Z}/p\mathbb{Z}$, $p\neq 2$.

При весьма общих предположениях относительно a, b и χ_p, соответствующая L-функция Артина оказывается многочленом, который можно записать как произведение

$$L(z;a,b)=\prod_{j=1}^{k}(1-\omega_j z)\quad\text{с}\quad\omega_1,\dots,\omega_k\in\mathbb{C}, \tag{6}$$

а для сумм (5) имеется представление

$$S_p=-\sum_{j=1}^{k}\omega_j\quad\text{с}\;\;k=n+m-1, \tag{7}$$

где n – степень редукции $b \bmod p$ многочлена b и m – степень радикала многочлена $a \bmod p$. Поясним, $m=\deg(a_1\dots a_r)$, если $a \bmod p$ есть

[1]Здесь и далее мы считаем все нетривиальные характеры χ_p продолженными с мультипликативной группы поля $\mathbb{Z}/p\mathbb{Z}$ на всё поле равенством $\chi_p(0)=0$. Тривиальный характер продолжаем равенством $\chi_p(0)=1$.

произведение $a_1^{s_1} \dots a_r^{s_r}$ степеней неприводимых над $\mathbb{Z}/p\mathbb{Z}$ многочленов $a_1, \dots, a_r$. Далее, по аналогии с гипотезой Римана для ζ-функции, имеем

$$|\omega_j| = \sqrt{p} \quad \text{для всех} \ \ j = 1, \dots, k, \tag{8}$$

что было доказано в широкой общности Вейлем и было известно до того в некоторых частных случаях. Следствием (7) и (8) является фундаментальная оценка

$$|S_p| \leqslant (n + m - 1)\sqrt{p}, \tag{9}$$

Достаточно предположить $p \nmid n$, чтобы имели место равенства (6) и (7). Если $n = 0$ и χ_p – характер порядка $h \geqslant 2$, достаточным условием для (6) и (7) является $\gcd(h, s_1, \dots, s_r) = 1$. Если $p \nmid n$ и степень многочлена $a \bmod p$ взаимно проста с порядком h характера χ_p, то имеем (6), (7) и (8).

Общая теория представлена в обзоре Ж.-П. Серра [1]. Изложение теории имеется также в монографии С. А. Степанова [2].

§3. Общие формулировки

Чтобы исследовать поведение сумм типа (5) в зависимости от p и сформулировать что-то аналогичное (3), необходимо определиться с выбором характеров χ_p. Скажем, можно рассмотреть суммы с тривиальными характерами χ_p или, для каждого $p \neq 2$, взять в качестве χ_p единственный квадратичный характер поля $\mathbb{Z}/p\mathbb{Z}$. С суммами (5), отвечающими характерам χ_p более высоких порядков, возникает “проблема выбора”. Скажем, при рассмотрении сумм (5) с кубическими характерами χ_p, каковые существуют при условии $p \equiv 1 \pmod 3$, необходимо, для каждого такого p, выбрать в качестве χ_p один из двух кубических характеров.

Наше намерение – сформулировать возможный аналог гипотезы (3) применительно к суммам (5) с χ_p порядка $h \geqslant 2$.

Введём в рассмотрение некоторое “вспомогательное” число $l \in \mathbb{Z}$ и число $w \in \mathbb{C}$ – некоторый примитивный степени h корень из единицы.

Определим Ω_l как множество всех простых чисел $p \equiv 1 \pmod h$ под условием: существует единственный характер χ_p порядка h поля $\mathbb{Z}/p\mathbb{Z}$ с $\chi_p(l) = w$.

Здесь $p \equiv 1 \bmod h$ – необходимое и достаточное условие существование характеров χ_p порядка h (количеством $\varphi(h)$, если φ – функция

Эйлера). Условие единственности можно переформулировать так: h взаимно просто с индексом числа l относительно какой-то (и, значит, любой) образующей мультипликативной группы поля $\mathbb{Z}/p\mathbb{Z}$. В частности, для простого h это означает в точности, что l не является h-ой степенью в $\mathbb{Z}/p\mathbb{Z}$.

Рассмотрим теперь суммы (5) с $p \in \Omega_l$ и с характерами χ_p из определения множества Ω_l. Предположим, для них имеется оценка (9). *Пусть* $\pi_l(x)$ – *число всех* $p \in \Omega_l$ *под условием* $p \leqslant x$ *и пусть* $D \subset \mathbb{C}$ – *круг радиуса* $R = n + m - 1$ *с центром в* 0. Мы предлагаем следующую формулировку.

Для каждого (*достаточно хорошего*) *измеримого множества* $V \subset D$ *имеет место равенство*

$$\lim_{x\to\infty} \frac{1}{\pi_l(x)} \sharp \left\{ p \in \Omega_l \;\middle|\; p \leqslant x,\ S_p/\sqrt{p} \in V \right\} = \int\limits_V C(z)\, dz,$$

в котором $C\colon D \to \mathbb{R}$ *вещественная положительная измеримая функция, зависящая только от параметров задачи* a, b, w, l *и подлежащая определению. В случае, когда* $S_p \in \mathbb{R}$ *для всех* $p \in \Omega_l$, *естественно заменить круг* D *на отрезок* $D \cap \mathbb{R}$ *и считать, что* V – *отрезки, содержащиеся в* $D \cap \mathbb{R}$. *Вместе с тем, можно рассмотреть аналогичные проблемы относительно пределов*

$$\lim_{x\to\infty} \frac{1}{\pi_l(x)} \sharp \left\{ p \in \Omega_l \;\middle|\; p \leqslant x,\ |S_p|^2/p \in V \right\} \quad c\ V \subset [\,0, R^2\,],$$

$$\lim_{x\to\infty} \frac{1}{\pi_l(x)} \sharp \left\{ p \in \Omega_l \;\middle|\; p \leqslant x,\ \theta_p \in V \right\} \quad c\ V \subset [\,0, 2\pi\,]$$

и с θ_p *под условиями* $S_p = |S_p| \exp(i\theta_p)$, $\theta_p \in [\,0, 2\pi\,]$.

Мы считаем, что предложенные формулировки являются естественными аналогами для проблемы (3).

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.

Proskurin N. V. On character sums in finite fields.

For polynomial character sums in finite fields, it is constructed some analogue to the known conjecture on distribution of the Kloosterman sums values.

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

Поступило 21 сентября 2020 г.