N. V. Proskurin, On exponential sums and flowers,
Zap. Nauchn. Sem. POMI, 2021, Volume 502, 133–138

Записки научных
семинаров ПОМИ
Том 502, 2021 г.

Н. В. Проскурин

ОБ ЭКСПОНЕНЦИАЛЬНЫХ СУММАХ И ЦВЕТАХ

§1. Введение

Рассмотрим поле $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ простого порядка p и нетривиальный характер ψ его мультипликативной группы, продолженный на всё поле $\mathbb{F}_p$ посредством $\psi(0) = 0$. Обозначим через e_p аддитивный характер

$$x \mapsto \exp(2\pi i x/p)$$

поля $\mathbb{F}_p$. Каждой паре f, g полиномов (от одной переменной) над $\mathbb{F}_p$ сопоставим сумму

$$\sum_{x \in \mathbb{F}_p} \psi\bigl(f(x)\bigr)\, e_p\bigl(g(x)\bigr). \tag{1}$$

В терминологии принятой в [1], это экспоненциальная сумма смешанного типа. При весьма общих предположениях относительно f, g и ψ, имеет место оценка Вейля

$$\Bigl| \sum_{x \in \mathbb{F}_p} \psi\bigl(f(x)\bigr)\, e_p\bigl(g(x)\bigr) \Bigr| \leqslant (m + n - 1)\sqrt{p} \tag{2}$$

в которой n и m обозначают, соответственно, степень полинома g и степень радикала полинома f. В частности, оценка имеет место, если степень f равна 1 и степень g равна 2. Обзор общей теории см. в [1]. Детальное освещение арифметики алгебраических кривых см. в [2].

§2. Согласованные семейства характеров

Если $l \in \mathbb{Z}$ и $w \in \mathbb{C}$ – примитивный корень из 1 степени h, обозначим $\Omega_{l,w}$ множество всех простых чисел $p \equiv 1 \pmod h$ под условием: существует единственный мультипликативный характер χ_p порядка h с $\chi_p(l) = w$. Здесь сравнением $p \equiv 1 \pmod h$ обеспечивается существование характеров χ_p порядка h. Требование единственности можно переформулировать следующим образом: h взамно просто

Ключевые слова: конечные поля, кубические характеры, экспоненциальные суммы.

с индексом числа l относительно какой-либо образующей поля $\mathbb{F}_p^\star$. Для простого h, это означает, что l не является h-ой степенью в $\mathbb{F}_p^\star$. Множества $\Omega_{l,w}$ были определены в [3, 4].

Пусть $n \in \mathbb{Z}$ и $\gcd(n,h) = 1$. Имеем $\chi_p(l) = w$ в том и только в том случае если $\chi_p(l^n) = w^n$. Следовательно, $\Omega_{l,w} = \Omega_{l^n,w^n}$. С некоторым n, имеем $w^n = \exp(2\pi i/h)$. Следовательно, каждое из этих множеств равно некоторому множеству

$$\Theta_{l,h} = \Omega_{l,w} \quad \text{с } \; l \in \mathbb{Z} \; \text{ и } \; w = \exp(2\pi i/h). \tag{3}$$

Назовём согласованным семейством характеров семейство $\{\chi_p\}_{p\in\Theta_{l,h}}$ с характерами χ_p однозначно определяемыми условиями $\chi_p(l) = w$ с w из (3). Более детально, $\{\chi_p\}_{p\in\Theta_{l,h}}$ есть согласованное семейство характеров порядка h и аргумента l.

§3. Постановка вопроса

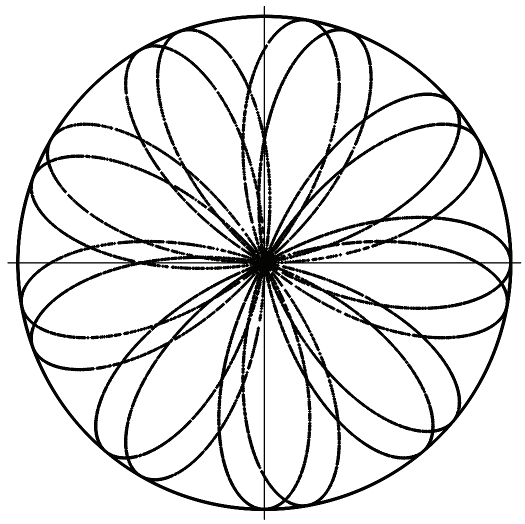
Наша общая цель – посредством численных экспериментов, составить представление о возможном распределении сумм (1) в круге, определённом неравенством (2). Конкретно, в настоящей публикации, мы рассмотрим суммы (1) с кубическими характерами ψ поля $\mathbb{F}_p$ и с $f(x) = x$, $g(x) = x^2$. При этом $m = 1$, $n = 2$ и нормированные суммы

$$E_p(\psi) = \frac{1}{2\sqrt{p}} \sum_{x\in\mathbb{F}_p} \psi(x)\, e_p(x^2) \tag{4}$$

лежат в круге $D = \bigl\{ z \in \mathbb{C} \bigm| |z| \leqslant 1 \bigr\}$.

§4. Полная картина

Мы вычислили $E_p(\psi)$ для всех кубических характеров ψ и всех простых чисел $p \equiv 1 \bmod 3$ под условием $p \leqslant X$ с $X = 360000$. Для каждого такого p имеется в точности два кубических характера поля $\mathbb{F}_p$ и если $\psi = \chi_p$ есть один из них, то второй есть $\psi = \bar{\chi}_p$. Результат вычислений представим следующим рисунком на комплексной плоскости.

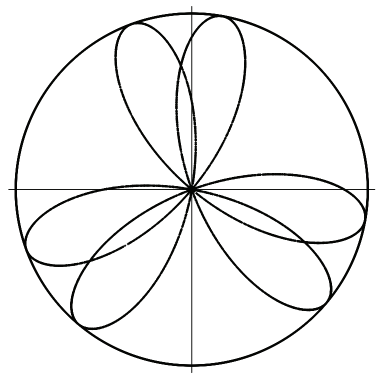


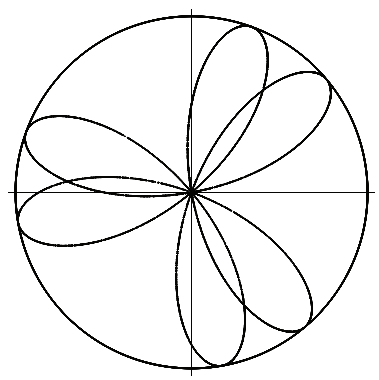
На этом рисунке мы видим цветок с 18-тью лепестками, границы которых составлены из точек $E_p(\chi_p)$ и $E_p(\bar{\chi}_p)$ с простыми числами $p \equiv 1 \bmod 3$ под условием $p \leqslant X$. Две прямые на этом рисунке суть вещественная и мнимая оси координат. Окружность, внутри которой находится цветок, суть граница единичного круга D. Ниже мы рассмотрим наш цветок более детально, а пока отметим, что его появление весьма неожиданно. Мы ожидали, скорее, увидеть некое "облако из точек" и находили такие "облака" вычисляя некоторые другие экспоненциальные суммы. (К примеру, так обстоит дело с суммами, получаемыми заменой $\psi(x)$ на $\psi(1-x)$ в (4).)

§5. Применение согласованных семейств

Рассмотрим согласованное семейство $\{\chi_p\}_{p\in\Theta_{l,3}}$ характеров порядка 3 и некоторого аргумента l. По нашему определению, простое число p принадлежит $\Theta_{l,3}$ в том и только в том случае, когда $p \equiv 1 \bmod 3$ и l не является кубом в группе $\mathbb{F}_p^\star$. Для каждого такого p, имеется единственный кубический характер χ_p под условием $\chi_p(l) = w$ с w из (3). Эти характеры и составляют семейство $\{\chi_p\}_{p\in\Theta_{l,3}}$. Рассмотрим теперь суммы (4) с $p \in \Theta_{l,3}$ и с $\psi = \chi_p$. Если l есть степень числа 2, то точки

$E_p(\chi_p)$ составляют одну из следующих двух фигур.



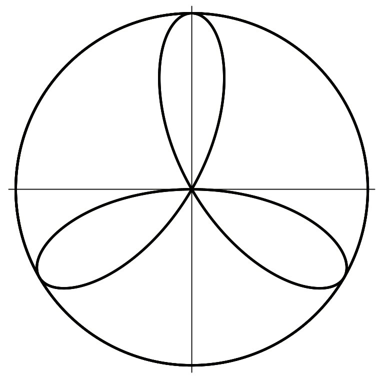


Точнее, первая фигура соответствует $l = 2^m$ с $m \equiv 1 \bmod 3$, а вторая – с $m \equiv 2 \bmod 3$. Эти два 6-тилепестковых цветка являются фрагментами 18-тилепесткового цветка, изображённого на первом рисунке. Ещё 6 лепестков на первом рисунке ограничены точками $E_p(\psi)$ с кубическими характерами ψ поля $\mathbb{F}_p$ для тех $p \equiv 1 \bmod 3$, для которых число 2 является кубом в $\mathbb{F}_p^\star$.

Иначе обстоит дело, если аргумент l согласованного семейства не является степенью числа 2. Рассмотрев несколько десятков таких аргументов l, мы обнаружили, что точки $E_p(\chi_p)$ разбросаны по всем 18-ти лепесткам.

§6. Трёхлистный клевер или трёхлепестковая роза

В декартовых координатах $x = \operatorname{Re} z$, $y = \operatorname{Im} z$, $z \in \mathbb{C}$, на комплексной плоскости, изобразим границу единичного круга D и кривую, определяемую уравнением $(x^2 + y^2)^2 + 3x^2y - y^3 = 0$. Так получаем следующий рисунок.



Кривая известна как трёхлистный клевер и как трёхлепестковая роза. Иоганн Кеплер в XVII веке и Гвидо Гранди в XVIII веке изучали некоторые классы кривых, содержащие эту розу. Возможно параметрическое задание кривой уравнениями $x = \cos(3t)\sin(t)$, $y = \cos(3t)\sin(t)$, $t \in [0, \pi)$. Мы обнаруживаем, что все цветы, рассмотренные в §4 и §5, получаются из одной такой розы поворотами вокруг точки 0 на углы кратные $\pi/18$. Это утверждение является приблизительным (хотя и весьма точным). Напомним, что цветы (или кривые) на рисунках в §4 и §5 составлены из точек $E_p(\psi)$ с теми или иными p и ψ. Эти точки найдены нами приближённо, посредством вычислений, и только в конечных пределах $p \leqslant X$. В типографском смысле, эти точки имеют конечные размеры и сливаются в кривые изображённые на рисунках. Без дополнительного исследования невозможно сказать, лежат ли все точки $E_p(\psi)$ в точности на кривых получаемых указанными поворотами розы, или они только сконцентрированы вблизи этих кривых.

§7. Радиальное распределение

Рассмотрим согласованное семейство $\{\chi_p\}_{p\in\Theta_{l,3}}$ характеров порядка 3 и некоторого аргумента l. Пусть $\pi_{l,3}(X)$ обозначает число простых чисел $p \in \Theta_{l,3}$ под условием $p \leqslant X$ и пусть $\Omega \subset [0, 1]$. Вычислениями (со многими отрезками Ω и с большими X) мы обнаруживаем, что числа

$$\frac{1}{\pi_{l,3}(X)}\,\sharp\left\{p\leqslant X\;\middle|\;|E_p(\chi_p)|\in\Omega\right\}$$

очень хорошо аппроксимируются интегралами

$$\frac{4}{\pi}\int\limits_{\Omega}\sqrt{1-x^2}\,dx\,,$$

известными в связи с гипотезой Сато-Тейта о суммах Клостермана. На этом основании, мы ожидаем, что имеет место равенство

$$\lim_{x\to\infty}\frac{1}{\pi_{l,3}(x)}\,\sharp\left\{p\in\Theta_{l,3}\;\middle|\;|E_p(\chi_p)|\in\Omega,\;\;p\leqslant x\right\}=\frac{4}{\pi}\int\limits_{\Omega}\sqrt{1-x^2}\,dx$$

для всех интервалов $\Omega\subset[0,1]$.

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. N. V. Proskurin, *Some problems on character sums in finite fields*, International Conference on Polynomial Computer Algebra, VVM Publishing, Saint Petersburg, 2020.
4. Н. В. Проскурин, *О суммах характеров в конечных полях* — Зап. научн. семин. ПОМИ, **490**, 104–108, 2020.

Proskurin N. V. On exponential sums and flowers.

By numerical experiments with some exponential sums in finite fields, it is discovered relation with flat curves known as roses and threeleaves clover.

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 27 сентября 2021 г.