Записки научных
семинаров ПОМИ
Том 511, 2021 г.

Н. В. Проскурин

РАСПРЕДЕЛЕНИЕ КУБИЧЕСКИХ ЭКСПОНЕНЦИАЛЬНЫХ СУММ

§1. Введение

Для простого числа p, рассмотрим поле $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, 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 экспоненциальную сумму

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

Имеет место (см. [1] и [2]) фундаментальное неравенство

$$\big|\, S_p(f) \,\big| \leqslant (\deg f - 1)\sqrt{p} \quad \text{при условии} \quad p \nmid \deg f. \tag{2}$$

Пусть f полином от одной переменной над кольцом $\mathbb{Z}$. Имея ввиду редукцию $\bmod p$, рассматрим f как полином над $\mathbb{F}_p$ и положим

$$E_p(f) = \frac{1}{(\deg f - 1)\sqrt{p}}\, S_p(f)\,. \tag{3}$$

С фиксированным f, рассмотрим точки (3) для всех $p \nmid \deg f$. Согласно (2), эти точки расположены в единичном круге

$$D = \big\{ z \in \mathbb{C} \;\big|\; |z| \leqslant 1 \big\}.$$

Пусть $\pi(x)$ обозначает число простых чисел $p \leqslant x$. Множеству $\Omega \subset D$ сопоставим число

$$\lim_{x \to \infty} \frac{1}{\pi(x)} \sharp \Big\{ p \leqslant x \;\Big|\; E_p(f) \in \Omega \Big\}. \tag{4}$$

Ключевые слова: конечные поля, кубические экспоненциальные суммы.

Так мы можем получить меру на круге D, характеризующую распределение точек $E_p(f)$ в D, если только пределы существуют для достаточно широкого класса множеств $\Omega \subset D$. Более общо, можно рассмотреть пределы

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sharp \Big\{ p \leqslant x \;\Big|\; \Phi(E_p(f)) \in \Omega \Big\} \tag{5}$$

с различными функциями Φ на D. Например, с $\Phi(z) = |z|,\ \Omega \subset [0,1]$.

Для данного полинома f и большого числа X, точки $E_p(f)$ с простыми $p \leqslant X$ составляют некоторую фигуру

$$E(f,X) = \big\{\, E_p(f) \;\big|\; p \leqslant X \big\} \subset \mathbb{C},$$

которая может служить визуализацией к проблеме распределения. Такого рода фигуры $E(f,X)$ с кубическими полиномами f изображены на нескольких рисунках в §4 и, в бóльшем числе, в [3]. Эмпирическим наблюдениям, основанным на вычислениях и рисунках, мы дадим теоретическое объяснение в §5 и §6. Основываясь на вычислениях, мы предложили в [3] гипотезу о распределении точек $|E_p(f)|$ с кубическими полиномами f. В настоящей публикации в §2 мы сформулируем эту гипотезу с поправкой, несколько ограничивающей общность. Для полиномов, исключённых этой поправкой, вопрос о распределении точек $|E_p(f)|$ оказывается связанным с проблемой Куммера и рассмотрен в §3.

§2. Радиальное распределение

Для полинома f над $\mathbb{Z}$, рассмотрим распределение точек $|E_p(f)|$ на отрезке $[0,1]$ вещественной прямой $\mathbb{R}$. Предел (5) аппроксимируется посредством

$$\frac{1}{\pi(X)} \sharp \Big\{ p \leqslant X \;\Big|\; |E_p(f)| \in \Omega \Big\} \tag{6}$$

с большим X. Мы можем взять $\Omega = [0,z]$ с $z \in [0,1]$ и трактовать (6) как функцию z. Вычислениями со многими кубическими полиномами f и с большими X (вплоть до 2000000) мы обнаруживаем очень хорошее согласование (6) с функцией

$$z \;\mapsto\; \frac{4}{\pi} \int_0^z \sqrt{1-t^2}\, dt. \tag{7}$$

Обнаруживаются однако и некоторые исключения, которые не были отмечены нами в [3].

Наша гипотеза состоит в том, что равенство

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\sharp\Big\{p\leqslant x\;\Big|\;|E_p(f)|\in\Omega\Big\}=\frac{4}{\pi}\int\limits_{\Omega}\sqrt{1-t^2}\,dt \tag{8}$$

имеет место для всех интервалов $\Omega\subset[0,1]$ *и для всех кубических полиномов* f, *исключая полиномы, редукция которых* $\bmod p$ *оказывается перестановочным полиномом для бесконечно многих* p.

Напомним, что функция (7) известна в связи с гипотезами Сато–Тейта о распределении точек на эллиптических кривых и о суммах Клостермана.

§3. Исключительные полиномы

Напомним, полином f над $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ называют перестановочным, если функция $z\mapsto f(z)$ отображает биективно $\mathbb{F}_p$ на $\mathbb{F}_p$. Для таких полиномов имеем $S_p(f)=0$. Говорят, что полином над $\mathbb{Z}$ является перестановочным $\bmod p$, если его редукция $\bmod p$ является перестановочным полиномом.

Если полином ax^3+bx^2+cx+d над $\mathbb{Z}$ является перестановочным $\bmod p$ для бесконечно многих простых чисел p, то он представим в виде $k(ux+v)^3+w$ с $u,v\in\mathbb{Z}$, $w,k\in\mathbb{Q}$ и является перестановочным $\bmod p$ для всех простых $p\equiv 2 \bmod 3$, исключая $p\mid a$. Это известно из исследований, связанных с гипотезой Шура, см. [5, 6]. Вот пара примеров: $f(x)=12x^3+30x^2+25x$ и $f(x)=16x^3+36x^2+27x$.
Простейший кубический полином $f(x)=x^3$, рассматриваемый как полином над $\mathbb{F}_p$ с $p\equiv 2 \bmod 3$, является перестановочным и, следовательно, $S_p(f)=0$. Для $p\equiv 1 \bmod 3$, существует кубический характер χ мультипликативной группы $\mathbb{F}_p^\star$ поля $\mathbb{F}_p$, можно положить

$$G(\chi)=\sum_{m\in\mathbb{F}_p^\star}\chi(m)\exp(2\pi im/p)$$

и найти, что $S_p(f)=G(\chi)+\overline{G(\chi)}$ и $|G(\chi)|^2=p$. Суммы $S_p(f)$ с $f(x)=x^3$ и $G(\chi)$ известны как кубические суммы Гаусса и также как суммы Куммера. Основываясь на вычислениях с простыми числами $p<500$, Куммер высказал некоторое предположение о распределении точек $E_p(f)=\operatorname{Re}G(\chi)/\sqrt{p}$, которое, как мы теперь знаем, не было

правильным. Вопрос был разрешён Хис-Брауном и Паттерсоном [4] доказавшими, что точки $G(\chi)/\sqrt{p}$ распределены по единичной окружности равномерно.

Этот фундаментальный результат можно переформулировать как равенство

$$\lim_{x\to\infty} \frac{1}{\pi'(x)} \sharp \Big\{ p \leqslant x \;\Big|\; p \equiv 1(3),\ |E_p(f)| \in [0,z] \Big\} = \frac{2}{\pi} \arcsin z. \qquad (9)$$

Здесь $f(x) = x^3$, $z \in [0,1]$ *и* $\pi'(x)$ *есть число простых чисел* $p \leqslant x$ *под условием* $p \equiv 1 \bmod 3$.

По теореме о простых числах в арифметических прогрессиях, имеем $\pi'(x) = (1/2 + o(1))\,\pi(x)$ при $x \to \infty$. Вернём к рассмотрению простые числа $p \equiv 2 \bmod 3$ и заметим, что производная функции arcsin в точке t равна $1/\sqrt{1-t^2}$.

Из (9) *немедленно следует равенство*

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sharp \Big\{ p \leqslant x \;\Big|\; |E_p(f)| \in \Omega \Big\} = \frac{1}{2}\,\delta(Q) + \frac{1}{\pi} \int\limits_{\Omega} \frac{dt}{\sqrt{1-t^2}} \qquad (10)$$

для $f(x) = x^3$ *и для всех интервалов* $\Omega \subset [0,1]$. *Здесь* $\delta(\Omega)$ *есть* 1 *или* 0 *смотря по тому* $0 \in \Omega$ *или* $0 \notin \Omega$.

Равенства (9) и (10) имеют место также с $f(x) = (ux+v)^3$ с целым $u \neq 0$ и любым целым v. Действительно, если $p \nmid u$, то полином $ux+v$ перестановочен $\bmod p$ и сумма $S_p(f)$ не изменится, если заменить в ней полином $f(x) = x^3$ на полином $f(x) = (ux+v)^3$. Измениться могут только суммы $S_p(f)$ с $p \mid u$, но это не изменит пределов в (9) и (10).

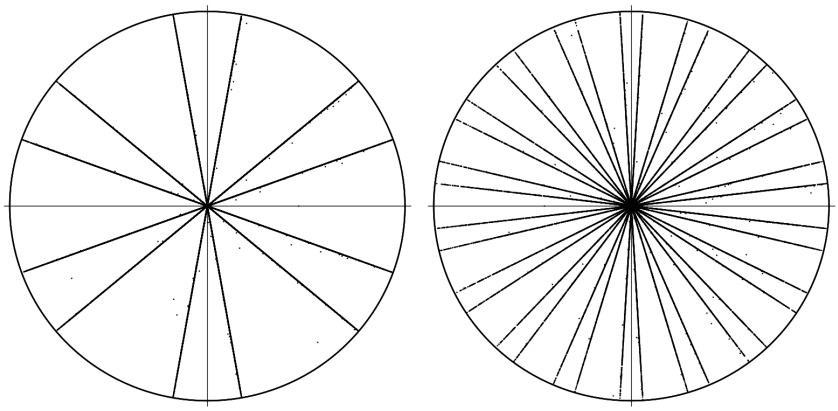
Мы ожидаем, что равенства (9) *и* (10) *имеют место для каждого кубического полинома* f *над* $\mathbb{Z}$, *редукция которого* $\bmod p$ *является перестановочным полиномом для бесконечно многих* p.

§4. Примеры

Возьмём некоторый кубический полином f над $\mathbb{Z}$ и изобразим на комплексной плоскости множество $E(f,X)$, то есть семейство точек $E_p(f)$ с простыми $p \leqslant X$. Если верхняя граница X достаточно велика, мы увидим на рисунке несколько отрезков, каждый из которых есть пересечение или содержится в пересечении круга D с некоторой

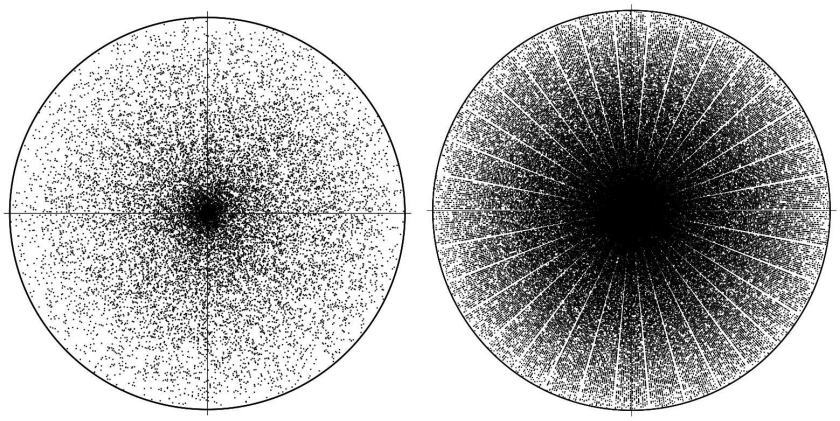
прямой, проходящей через 0, и увидим ещё несколько точек, расположенных вне этих отрезков. Разумеется, множества $E(f, X)$ конечны, содержатся в не более чем счётном множестве всех точек $E_p(f)$ и не могут составлять отрезок прямой. Однако реально, на рисунке, каждая точка изображается маленьким кругом и изображения точек сливаются в отрезки прямых. Это было замечено в численных экспериментах [3].

Ниже, на рисунках изображены вещественная и мнимая координатные оси, единичный круг D и типичные множества $E(f, X)$ с $X = 400000$.



На левом рисунке изображено множество $E(f, X)$ с $f(x) = 6x^3 + 3x^2 + 4x$, которое выглядит как цветок сформированный 6-тью отрезками. На правом рисунке изображено множество $E(f, X)$ с $f(x) = 2x^3 + 2x^2 + 3x$, которое выглядит как цветок сформированный 18-тью отрезками. Неправильно было бы думать, что точки $E_p(f)$ лежат на отрезках, которые мы видим на рисунках. Точки $E_p(f)$ только сконцентрированы вблизи этих отрезков и, за редкими исключениями, не лежат на них. Обнаруживается, что точки $E_p(f)$ концентрируются вблизи того или иного отрезка в зависимости только от класса $p \bmod m$ с некоторым модулем m, зависящим только от f. В наших примерах модуль m равен 18 и 27. Эти вопросы будут рассмотрены в §5 и §6.

Ниже на левом рисунке изображено множество $E(f, X)$ с полиномом $f(x) = 17x^3 + 9x^2 + x$ и с $X = 200000$.



Подобные рисунки, на которых не обнаруживается какой-либо структуры, мы назвали в [3] кластерами. Мы теперь знаем и покажем в §6, что структура проявится и что каждый кластер превратится в сформированный отрезками цветок, если продолжить вычисления. В частности, с тем же полиномом f и с $X = 2000000$, множество $E(f, X)$ выглядит как 272 прямые сгруппированные в 17 пучков по 16 прямых. Это множество изображено на правом рисунке.

Чтобы пояснить причины, по которым мы во всех примерах рассматриваем полиномы f без свободного члена, положим $g(x) = f(x) + d$ с каким-то $d \in \mathbb{Z}$ и заметим, что $S_p(g) = e_p(d)\, S_p(f)$ с $e_p(d) = \exp(2\pi i d/p) = 1 + O(d/p)$ при $p \to \infty$. Отсюда видно, что интересующие нас предельные распределения не зависят от свободного члена полинома f.

§5. Об аргументах кубических сумм

Для простого числа p и полинома $f(x) = ax^3 + bx^2 + cx + d$ над $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ под единственным условием $6a \neq 0$, рассмотрим сумму (1) и заметим, что её можно записать как произведение

$$S_p(f) = e_p\big(f(v)\big)\, S_p(g), \tag{11}$$

в котором v есть единственный корень второй производной полинома f, а g есть нечётный кубический полином. Сказать точнее, здесь $g(x) = ax^3 + (c + bv)x$ и $3av + b = 0$. Для доказательства (11), достаточно в каждом слагаемом суммы (1) заменить x на $x + v$, отчего сумма не

изменится, и заметить, что $f(x+v) = f(v) + g(x)$. Поскольку полином g нечётный (то есть $g(-x) = -g(x)$ для всех $x \in \mathbb{F}_p$), имеем $S_p(g) \in \mathbb{R}$. С этим замечанием, (11) приводит к следующему утверждению.

Для кубического полинома f над полем $\mathbb{F}_p$ с $p \nmid 6$, сумма $S_p(f)$ либо равна 0 либо лежит на прямой пересекающей вещественную ось в точке 0 под углом $2\pi l/p$, где l есть наименьшее неотрицательное число в классе $f(v) \bmod p$ и v есть корень второй производной полинома f.

Рассмотрим более детально множитель $e_p\big(f(v)\big)$ в (11). Мы имеем $e_p\big(f(v)\big) \in \mathbb{R}$ в том и только в том случае, если $f(v) = 0$. Легко находим равенство

$$f(v) = \frac{2b^3 - 9abc}{27a^2} + d \tag{12}$$

и следующее утверждение.

Для полинома $f(x) = ax^3 + bx^2 + cx$ с $a \neq 0$ над полем $\mathbb{F}_p$ с $p \nmid 6$, если $b = 0$ или $2b^2 = 9ac$, то сумма $S_p(f)$ лежит на вещественной прямой. Обратно, если $S_p(f)$ лежит на вещественной прямой и $S_p(f) \neq 0$, то $b = 0$ или $2b^2 = 9ac$.

Пусть теперь $f(x) = ax^3 + bx^2 + cx + d$ будет кубическим полиномом над $\mathbb{Z}$. Рассмотрим прямую L на плоскости $\mathbb{C}$, пересекающую вещественную ось в точке 0 под каким-то углом $\theta \neq 0$. Если $S_p(f) \in L$, $S_p(f) \neq 0$ и $p \nmid 6a$, то $\theta = 2\pi l/p$ с каким-то целым $l = 1, \dots, p-1$. Это немедленно следует из доказанного выше утверждения. Заметим ещё, что если $\theta = 2\pi l/p$ с простым p и целым $l \neq 0$, то $\theta \neq 2\pi l'/p'$ для любого другого простого числа p' и любого целого числа l'. Так мы доказали утверждение, которое было сформулировано в §4, и даже более того.

На каждом отрезке на наших рисунках, исключая только отрезок вещественной оси $[-1, 1]$, имеется не более чем одна отличная от 0 точка $E_p(f)$ с $p \nmid 6a$.

§6. Предельные прямые

Рассмотрим кубический полином $f(x) = ax^3 + bx^2 + cx$ над $\mathbb{Z}$ и простое число p под условием $p \nmid 6a$. Для соответствующей суммы $S_p(f)$ мы имеем разложение

$$S_p(f) = e_p\big(f(v)\big)\, S_p(g), \tag{13}$$

в котором $g(x) = ax^3 + (c+bv)x$, $v = -bu$ и u есть целое число под условием $3au \equiv 1 \bmod p$. Это переформулировка (11) с целыми числами и сравнениями вместо конечного поля. В этом разложении, полином g нечётный, $S_p(g) \in \mathbb{R}$ и $f(v) = (2b^2 - 9ac)abu^3$. Пусть $w = u^3$ — число обратное к $27a^3 \bmod p$. Условимся использовать фигурные скобки $\{\cdot\}$ для обозначения дробных частей вещественных чисел. Из (13) получаем следующее утверждение.

Если $S_p(f) \neq 0$ и $p \nmid 6a$, то прямая, проходящая через 0 и $S_p(f)$, пересекает вещественную ось под углом

$$\theta_p = 2\pi\Big\{ab\,(2b^2 - 9ac)\,\frac{w}{p}\Big\}. \tag{14}$$

Пусть l — целое число под условием $\gcd(l, 3a) = 1$. Рассмотрим простые числа p под условием $lp+1 \equiv 0 \bmod 27a^3$ и соответствующие им числа θ_p. Все такие числа p лежат в арифметической прогрессии с разностью $27a^3$ и начальным членом l' с $ll' \equiv -1 \bmod 27a^3$. Исключая простые делители числа $3a$, все простые числа лежат в этих прогрессиях. Целое число $(lp+1)/(27a^3)$ обратно к $27a^3 \bmod p$. Подставим это число в (14) вместо w. Так получаем следующее утверждение.

Пусть l — целое число под условием $\gcd(l, 3a) = 1$ и p — простое число под условиями $lp + 1 \equiv 0 \bmod 27a^3$ и $p \nmid 6a$. Если $S_p(f) \neq 0$, то прямая, проходящая через 0 и $S_p(f)$, пересекает вещественную ось под углом

$$\theta_p = 2\pi\left\{\frac{b\,(2b^2 - 9ac)}{27a^2}\Big(l + \frac{1}{p}\Big)\right\}. \tag{15}$$

Отсюда, наконец, получаем полную характеризацию отрезков, о которых шла речь в §4.

Прямые, вдоль которых сконцентрированы точки $E_p(f)$ на наших рисунках, пересекают вещественную ось в точке 0 под углами

$$\theta = 2\pi\left\{\frac{b\,(2b^2 - 9ac)}{27a^2}\,l\right\} \tag{16}$$

с целыми l под условием $\gcd(l, 3a) = 1$.

Обратим внимание на то, что в формулах (15) и (16) не исключены случаи $b = 0$ и $2b^2 - 9ac = 0$. Прямая, соответствующая этим случаям, – вещественная ось.

Рассмотрим вопрос о числе отрезков на рисунке соответствующем данному полиному f. Пусть φ обозначает функцию Эйлера, $\varphi(m)$ есть

число единиц кольца $\mathbb{Z}/m\mathbb{Z}$. Представим коэффициент при l в (16) несократимой дробью —

$$\frac{b\,(2b^2-9ac)}{27a^2}=\frac{P}{Q}\quad \text{с}\quad \gcd(P,Q)=1,\ \ Q>0.$$

Все возможные углы θ *в* (16) *получим перебрав* $l \bmod Q$ *с* $\gcd(l,Q)=1$. *Если* $4 \nmid Q$, *то все прямые, соответствующие этим* θ, *различны и число таких прямых равно* $\varphi(Q)$. *Если* $4 \mid Q$, *то вместе с углом* $\theta \in (0,\pi)$ *имеется и угол* $\theta+\pi \in (\pi,2\pi)$, *которому соответствует та же прямая, что и углу* θ. *В этом случае, число прямых, получаемых по формуле* (16), *равно* $\varphi(Q)/2$.

Таким образом, можно ожидать, что на рисунке изображающем множество $E(f,X)$ будет $\varphi(Q)$ или $\varphi(Q)/2$ отрезков. Именно это мы и обнаруживаем, но есть некоторые исключения. Чтобы это пояснить, рассмотрим какую-то прямую L из тех, что определены (16). Из доказательства формул (15) и (16) видно, что точки $S_p(f)$, которые могут быть сконцентрированы вблизи L, соответствуют простым числам из некоторого класса вычетов $\bmod 27a^3$. Однако может случиться, что $S_p(f)=0$ для таких p. В таком случае L не появится на рисунке изображающем множество $E(f,X)$ и число отрезков на рисунке будет меньше чем $\varphi(Q)$ или $\varphi(Q)/2$.

Список литературы

1. J.-P. Serre, *Majorations de sommes exponentielles*, Société Mathématique de France, Asterisque 41–42, 111–126, 1977.
2. S. A. Stepanov, *Arithmetic of algebraic curves*, Moscow, 1991 (in Russian). English transl., Springer–Verlag, 1995.
3. Н. В. Проскурин, *О некоторых кубических экспоненциальных суммах.* — Зап. научн. семин. ПОМИ, **502** (2021), 122–132.
4. D. R. Heath-Brown, S. J. Patterson, *The distribution of Kummer sums at prime arguments*, Journal für die reine und angew. Math. 310 (1979), 111–130.
5. I. Schur, *Über den Zusammenhang zwische einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen*, S.-B. Preuss. Akad. Wiss. Berlin (1923), 123–134.
6. G. Turnwald, *On Schur's conjecture*, Journal Austral. Math. Soc. (Series A) **58** (1995), 312–357.

Proskurin N. V. Distribution of cubic exponential sums.

Some results on distribution of cubic additive exponential sums in finite fields are discovered by numerical experiments and proved. It is stated a conjecture on distribution of their absolute values.

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 13 сентября 2022 г.