Записки научных
семинаров ПОМИ
Том 517, 2022 г.

Н. В. Проскурин

О БИКВАДРАТИЧНЫХ ЭКСПОНЕНЦИАЛЬНЫХ СУММАХ

§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 соответствующую им [1], [2] экспоненциальную сумму аддитивного типа

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

Пусть $C = \deg f - 1$ и $D = \bigl\{z \in \mathbb{C} \bigm| |z| \leqslant 1\bigr\}$. Под условием $p \nmid \deg f$ имеет место неравенство Вейля

$$\bigl| S_p(f) \bigr| \leqslant C\sqrt{p}$$

и мы можем представить сумму (1) как

$$\sum_{x \in \mathbb{F}_p} e_p\bigl(f(x)\bigr) = C\sqrt{p}\, E_p(f)$$

с $E_p(f) \in D$. Нас интересует распределение точек $E_p(f)$ в единичном круге D. В настоящей публикации[1] мы сообщаем о результатах наших вычислений сумм (1) с многочленами f степени 4.

Пусть f полином от одной переменной над $\mathbb{Z}$, который (посредством редукции $\bmod p$) рассмотрим также как полином над каждым из полей $\mathbb{F}_p$. Рассмотрим точки $E_p(f)$ для всех простых чисел p. Пусть $\pi(x)$ обозначает число простых чисел $p \leqslant x$. Мы ожидаем, что существуют пределы

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sharp \Bigl\{ p \leqslant x \Bigm| E_p(f) \in \Omega \Bigr\},$$

Ключевые слова: конечные поля, биквадратичные экспоненциальные суммы.

[1]Некоторые другие суммы были рассмотрены ранее в [3] и [4].

по меньшей мере для “достаточно хороших” множеств $\Omega \subset D$, и также, что существуют пределы

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

с некоторыми функциями R, скажем с $R(z) = |z|,\ \Omega \subset [0,1]$.
Чтобы составить представление о распределении точек $E_p(f)$, мы провели вычисление для широкого класса биквадратичных полиномов, то есть полиномов f степени 4. Для данного полинома f и большого числа X, пусть $E(f)$ будет множеством всех точек $E_p(f)$ и пусть

$$E(f,X) = \Big\{ E_p(f) \;\Big|\; p \text{ – простое число } \leqslant X \Big\}. \tag{2}$$

Эти множества могут служить визуализацией к проблеме распределения. Если реально изобразить на листе бумаги точки $E_p(f)$, составляющие множество $E(f,X)$, мы обнаружим, что многие точки расположены столь близко друг к другу, что их изображения сливаются, формируя некоторые фигуры. То, что мы увидим на рисунке – отрезки и криволинейные треугольники, – будет скорее изображением замыкания, в топологическом смысле, предельного множества $E(f)$, что собственно нам и надо.
Мы относим каждый полином f к одному из трёх классов, в соответствии с тем, как выглядит на рисунке соответствующее ему множество $E(f,X)$ с большим X. Эти классы мы опишем в §4, §5 и §6.

§2. Биквадратичная сумма Гаусса

Сумма $S_p(f)$ с $f(x) = x^4$ есть биквадратичная сумма Гаусса. Если $p = 2$, то $S_p(f) = 0$. Если $p \equiv 3 \pmod 4$, то биквадратичная сумма равна квадратичной, для которой известна явная формула Гаусса и мы имеем $S_p(f) = i\sqrt{p}$ и $E_p(f) = i/3$. В случае $p \equiv 1 \pmod 4$ имеется почти явная формула

$$S_p(f) = \sqrt{p} \pm \sqrt{2u\,(p + v\sqrt{p}\,)}\,, \tag{3}$$

в которой v определяется из разложения числа p в сумму квадратов целых чисел $v^2 + w^2 = p$ и условия $v \equiv -u \pmod 8$, а u равно 1 или -1, смотря по тому $p \equiv 1 \pmod 8$ или $p \equiv 5 \pmod 8$. Формула приведена в [5] (теорема 4.2.1) со ссылкой на Гаусса [6]. В связи с проблемой выбора знака, которая долгое время оставалась открытой, также см. [5]. Из формулы (3) следует, что точки $E_p(f)$ принадлежат отрезку $[-1/3, 1]$

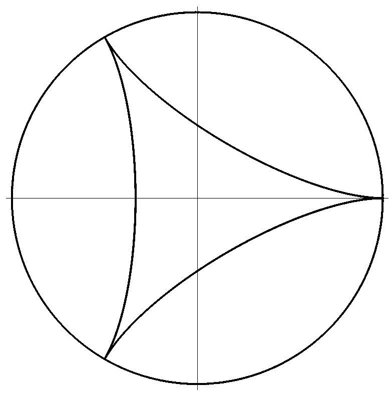
вещественной оси или отрезку $[1/3 - 2i/3, 1/3 + 2i/3]$, смотря по тому $p \equiv 1 \pmod 8$ или $p \equiv 5 \pmod 8$.

§3. Основной треугольник

На приведённом ниже рисунке изображены вещественная и мнимая координатные оси, круг $D \subset \mathbb{C}$ и дельтоида – правильный криволинейный треугольник, состоящий из точек $z = x + iy$ под условиями

$$3(x^2 + y^2)(x^2 + y^2 + 2) = 8x^3 - 24xy^2 + 1, \quad x, y \in \mathbb{R},$$

Этот треугольник, рассмотренный ещё Эйлером, можно трактовать как траекторию точки, которая лежит на окружности радиуса $1/3$ катящейся по границе круга D. Мы увидим в §6, что треугольник, очень похожий на дельтоиду, играет роль в описании множеств $E(f)$.



Вершины треугольника – кубические корни из 1, то есть точки 1, $\omega = (-1 + \sqrt{-3})/2$ и $\omega' = (-1 - \sqrt{-3})/2$. Углы равны 0. Стороны треугольника равны между собой и совмещаются друг с другом при повороте треугольника на угол $2\pi/3$ вокруг точки 0. Площадь треугольника равна $2\pi/9$.

§4. Конфигурации отрезков

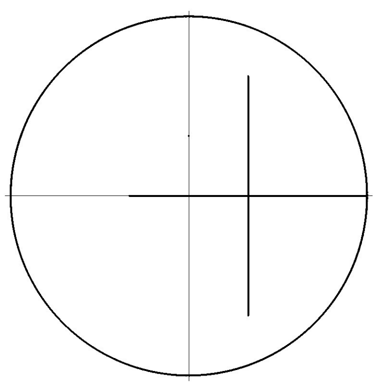
Для многих полиномов f, точки $E_p(f)$ лежат на нескольких отрезках или сконцентрированы, все или почти все, вблизи нескольких отрезков в круге D. Эти отрезки образуют весьма разнообразные конфигурации, что мы продемонстрируем примерами. Один пример мы уже обсуждали в §2.

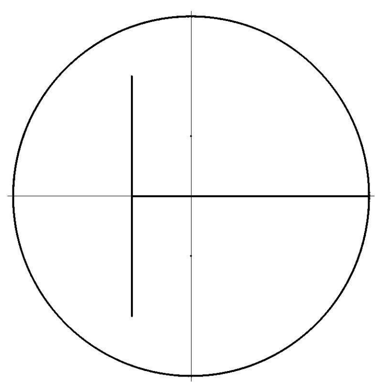
На приведённых ниже рисунках изображены вещественная и мнимая координатные оси, единичный круг $D \subset \mathbb{C}$ и конечное множество $E(f, X)$ точек $E_p(f) \in D$ для простых чисел $p \leqslant X$ с $X = 480000$, см. (2). Каждый рисунок соответствует тому или иному полиному f. На каждом рисунке мы видим несколько отрезков и изолированных точек. Обнаруживается, что точки $E_p(f)$ относятся к тому или иному отрезку смотря только по классу $p \bmod m$ с некоторым модулем m, зависящим только от f.

Приводимые нами утверждения относительно отдельных отрезков и точек считываются с рисунков. Мы не располагаем доказательствами.

По нашему мнению, полиномы f, которым соответствуют такого рода рисунки, следует трактовать как исключительные. Для сумм $S_p(f)$, соответствующих этим полиномам, можно надеяться найти явные формулы, подобные формулам Гаусса, рассмотренным в §2. К типичным, не исключительным, следует, наверное, относить полиномы, которым соответствуют рисунки, рассматриваемые в §6.

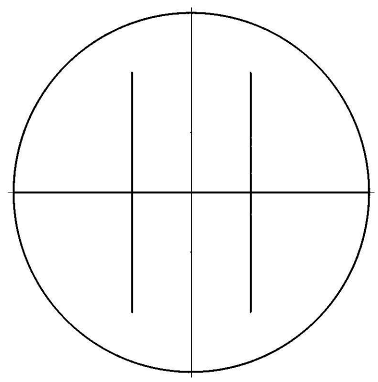
Простейшие конфигурации. Рисунок слева составлен из двух отрезков $[-1/3, 1]$, $[1/3 - 2i/3, 1/3 + 2i/3]$ и точки $i/3$. Так выглядит множество $E(f, X)$ для полинома $f(x) = x^4$ и так же выглядит множество $E(f, X)$ для полинома $f(x) = 4x^4$. При этом, горизонтальный отрезок сформирован точками $E_p(f)$ с $p \equiv 1 \pmod 8$, а вертикальный – точками $E_p(f)$ с $p \equiv 5 \pmod 8$. Все $E_p(f)$ с $p \equiv 3 \pmod 4$ равны $i/3$.





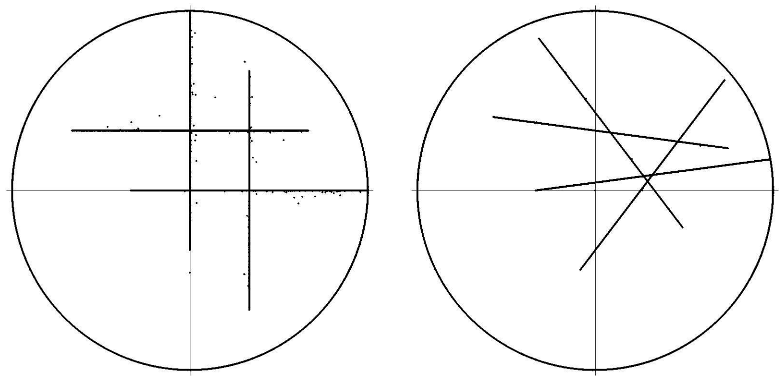
Правый рисунок составлен из отрезков $[-1/3, 1]$, $[-1/3 - 2i/3, -1/3 + 2i/3]$ и точек $\pm i/3$. Так выглядит множество $E(f, X)$ для полинома $f(x) = 2x^4$ и так же выглядит множество $E(f, X)$ для полинома $f(x) = 8x^4$. При этом, горизонтальный отрезок сформирован точками $E_p(f)$ с $p \equiv 1 \pmod 8$, а вертикальный – точками $E_p(f)$ с $p \equiv 5 \pmod 8$. Все $E_p(f)$ с $p \equiv 3 \pmod 8$ равны $-i/3$. Все $E_p(f)$ с $p \equiv 7 \pmod 8$ равны $i/3$.

Следующий рисунок составлен из отрезков $[-1, 1]$, $[-1/3-2i/3, -1/3+2i/3]$, $[1/3 - 2i/3, 1/3 + 2i/3]$ и точек $\pm i/3$. Так выглядят множества $E(f, X)$ для полиномов $f(x) = 3x^4$, $5x^4$, $6x^4$, $7x^4$. Случай $f(x) = 3x^4$ рассмотрим более детально. Мы обнаруживаем, что принадлежность точки $E_p(f)$ тому или иному отрезку определяется вычетом $p \pmod{24}$. Сказать точнее, $E_p(f)$ есть $-i/3$ или $i/3$ смотря по тому, $p \equiv 7 \pmod{12}$ или $p \equiv 11 \pmod{12}$.



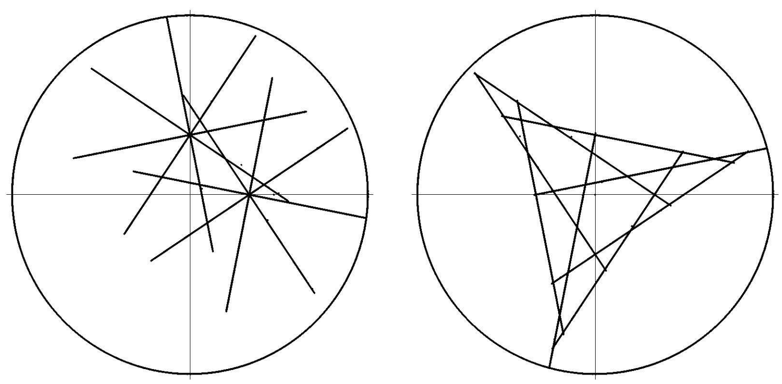
И далее: точки $E_p(f)$ с $p \equiv 1 \pmod{24}$ формируют отрезок $[-1/3, 1]$; точки $E_p(f)$ с $p \equiv 17 \pmod{24}$ формируют отрезок $[-1, 1/3]$; точки $E_p(f)$ с $p \equiv 5 \pmod{24}$ формируют отрезок $[-1/3 - 2i/3, -1/3 + 2i/3]$; точки $E_p(f)$ с $p \equiv 13 \pmod{24}$ формируют отрезок $[1/3 - 2i/3, 1/3 + 2i/3]$.

Вот ещё пара конфигураций. Ниже, на рисунке слева изображено множество $E(f, X)$ с $f(x) = x^4 + 2x^2$. Для каждого из четырёх классов $r \bmod 8$ взаимнопростых с модулем, на рисунке имеется отрезок сформированный точками $E_p(f)$ с $p \equiv r \pmod 8$. Сказать точнее, это отрезки $[-1/3, 1]$, $[-i/3, i]$, $[1/3 - 2i/3, 1/3 + 2i/3]$, $[-2/3 + i/3, 2/3 + i/3]$ соответствующие классам $r \equiv 1, 3, 5, 7 \pmod 8$.

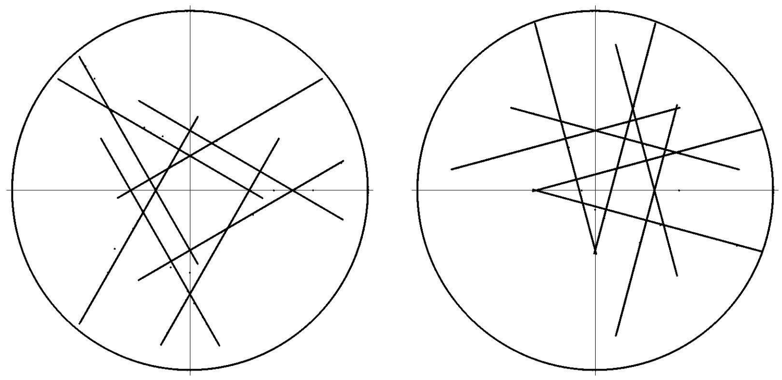


Правый рисунок соответствует полиному $f(x) = 6x^4 + x^2$. Для каждого из четырёх классов $r \mod 12$ взаимнопростых с модулем, на рисунке имеется отрезок сформированный точками $E_p(f)$ с $p \equiv r \pmod{12}$. Каждая из точек $\pm 1/3$, $\pm i/3$ принадлежит одному из отрезков.

Конфигурации 8-и отрезков. Левый рисунок соответствует полиному $f(x) = x^4 + 2x^3 + x^2$, а правый – полиному $f(x) = 4x^4 + x^2$. Для каждого из восьми классов $r \mod 16$ взаимнопростых с модулем, на каждом из рисунков имеется отрезок сформированный точками $E_p(f)$ с $p \equiv r \pmod{16}$. Каждый отрезок содержит одну из точек $\pm 1/3$ и $\pm i/3$.

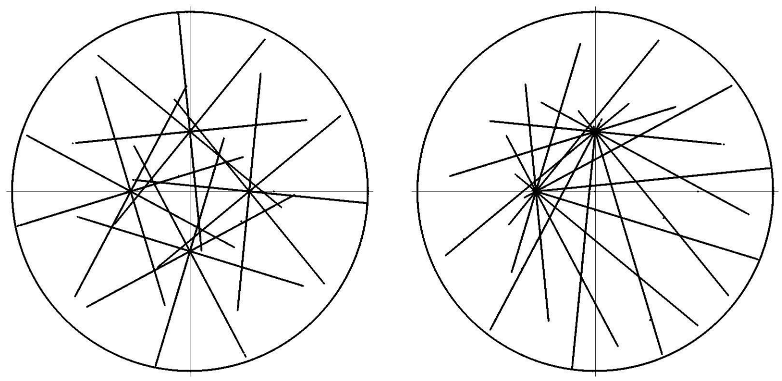


Ниже, левый рисунок соответствует полиному $f(x) = 6x^4 + 2x^2$, а правый – полиному $f(x) = 3x^4 + x^2$. Для каждого из шестнадцати классов $r \mod 24$ взаимнопростых с модулем, на каждом из рисунков имеется отрезок сформированный точками $E_p(f)$ с $p \equiv r \pmod{24}$.

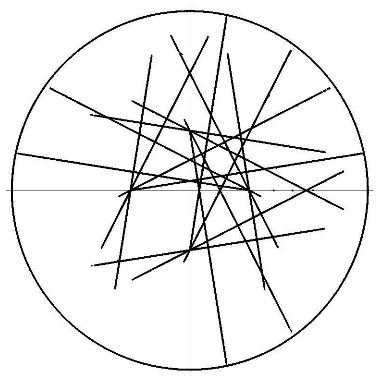


Каждая из точек $\pm 1/3$ и $\pm i/3$ принадлежит 2-м отрезкам.

Конфигурации 16-и отрезков. На левом рисунке, соответствующем полиному $f(x) = 8x^4 + 8x^3 + 2x^2$, по 4 отрезка проходят через каждую из точек $\pm 1/3$ и $\pm i/3$. На правом рисунке, соответствующем полиному $f(x) = 8x^4 + x^2$, по 8 отрезков проходят через точки $-1/3$ и $i/3$.

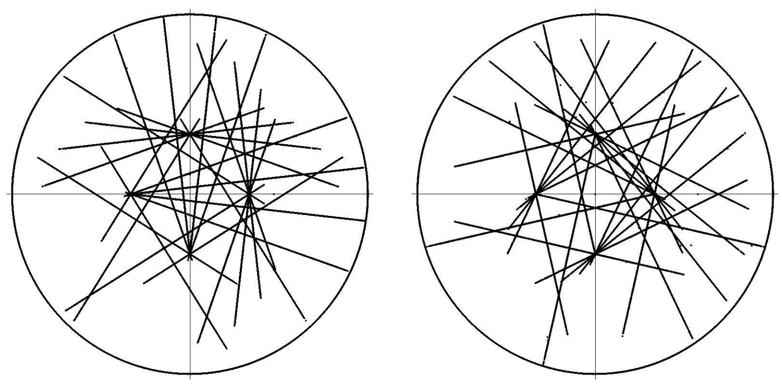


Для каждого из шестнадцати классов $r \mod 32$ взаимнопростых с модулем, на каждом из рисунков имеется отрезок сформированный точками $E_p(f)$ с $p \equiv r \pmod{32}$.
Ниже, левый рисунок соответствует полиному $f(x) = 5x^4 + x^2$, а правый – полиному $f(x) = 5x^4 + 2x^2$. Каждая из точек $\pm 1/3$ и $\pm i/3$ принадлежит 4-м отрезкам.



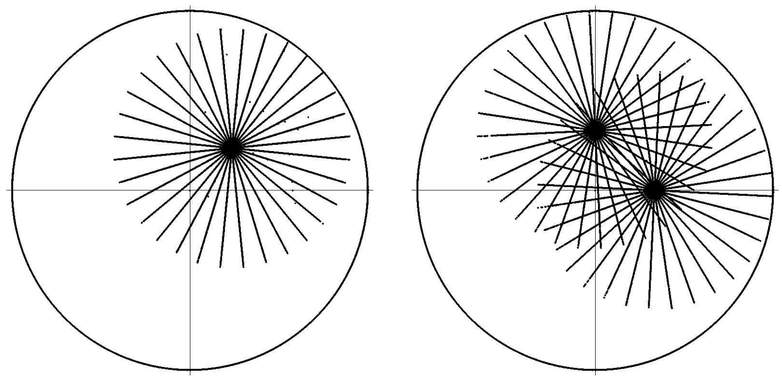
Для каждого из шестнадцати классов $r \mod 40$ взаимнопростых с модулем, на каждом из рисунков имеется отрезок сформированный точками $E_p(f)$ с $p \equiv r \pmod{40}$.

Конфигурации 24-х отрезков. Левый рисунок соответствует полиному $f(x) = 7x^4 + x^2$, а правый – полиному $f(x) = 7x^4 + 2x^2$. Каждая из точек $\pm 1/3$ и $\pm i/3$ принадлежит 6-и отрезкам.



Для каждого из двадцати четырёх классов $r \mod 56$ взаимнопростых с модулем, на каждом из рисунков имеется отрезок сформированный точками $E_p(f)$ с $p \equiv r \pmod{56}$.

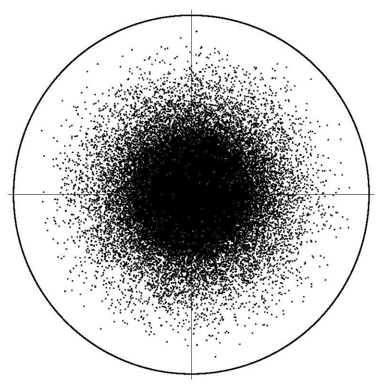
Конфигурации 16-и и 32-х отрезков. Левый рисунок соответствует полиному $f(x) = 8x^4 + 8x^3 + 4x^2 + x$. Каждому из шестнадцати классов $r \mod 32$ взаимнопростых с модулем соответствует отрезок сформированный точками $E_p(f)$ с $p \equiv r \pmod{32}$. Мы видим 16 отрезков длины $4/3$ с общим центром.



Правый рисунок соответствует полиному $f(x) = 4x^4 + 4x^3 + x^2$. На этом рисунке мы видим 16 отрезков с центрами в точке $1/3$ и 16 отрезков с центрами в точке $i/3$. Каждому из тридцати двух классов $r \bmod 64$ взаимнопростых с модулем соответствует отрезок сформированный точками $E_p(f)$ с $p \equiv r \pmod{64}$.

§5. Кластеры

На приведённом ниже рисунке изображены вещественная и мнимая координатные оси, единичный круг $D \subset \mathbb{C}$ и точки $E_p(f) \in D$ для полинома $f(x) = 5x^4 + x^3 + 3x^2 + 7x$ и всех простых чисел $p \leqslant X$ с $X = 480000$.

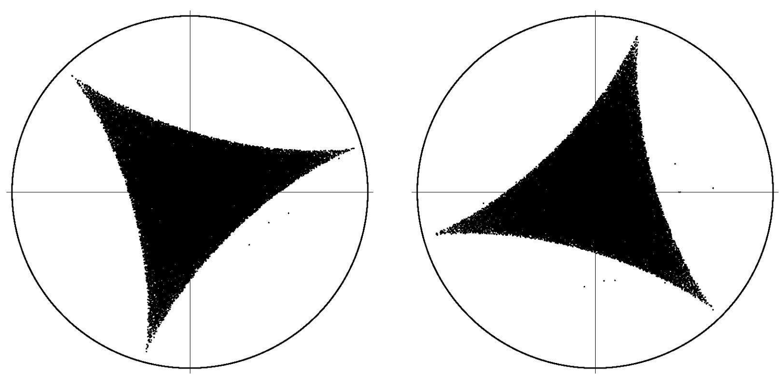


Множество $E(f, X)$ выглядит как шаровое звёздное скопление (globular cluster) без какой-либо структуры в распределениии точек. Такие кластеры $E(f, X)$ обнаруживаются для многих полиномов f. Однако мы не можем исключить того, что структуры проявятся при рассмотрении множеств $E(f, X)$ с бо́льшими X.

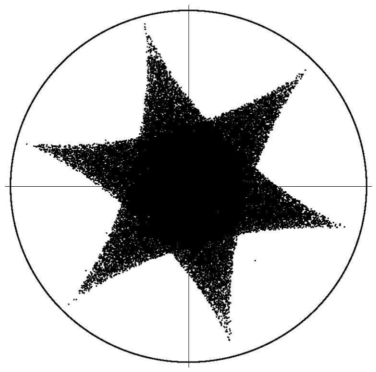
§6. Треугольники

Для некоторых полиномов f, точки $E_p(f)$ заполняют криволинейный треугольник, который по форме идентичен основному треугольнику из §3 и может быть совмещён с основным треугольником поворотом вокруг точки 0. Для многих полиномов f, точки $E_p(f)$ заполняют 2, 4 или 8 таких треугольников. Проиллюстрируем это примерами. Приводимые нами утверждения относительно распределения точек $E_p(f)$ основаны на вычислениях и считываются с рисунков. Доказательствами мы не располагаем.

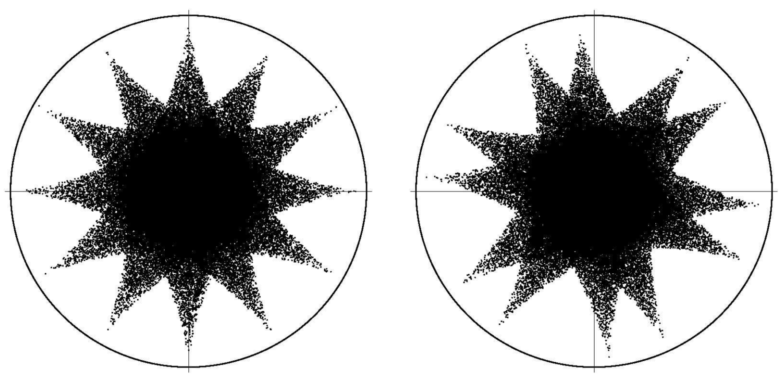
Простейшие конфигурации. Множества $E(f, X)$ с $X = 1000000$. Левый рисунок соответствует полиному $f(x) = 4x^4 + 8x^3 + 3x^2 + 6x$. Одна из вершин лежит на биссектрисе второго квадранта. Правый рисунок соответствует полиному $f(x) = 4x^4+8x^3+3x^2+7x$. Одна из вершин лежит на биссектрисе четвёртого квадранта. Есть несколько точек $E_p(f)$ лежащих вне треугольников.



Конфигурации 2-х треугольников. Множества $E(f, X)$ с $X = 1000000$. Левый рисунок соответствует полиному $f(x) = 2x^4 + 4x^3$. Из двух треугольников, один сформирован точками $E_p(f)$ с $p \equiv 1, 3 \pmod 8$, а другой – точками $E_p(f)$ с $p \equiv 5, 7 \pmod 8$. Правый рисунок соответствует полиному $f(x) = 8x^4 + 16x^3$. Из двух треугольников, один сформирован точками $E_p(f)$ с $p \equiv 1 \pmod 4$, а другой – точками $E_p(f)$ с $p \equiv 3 \pmod 4$.

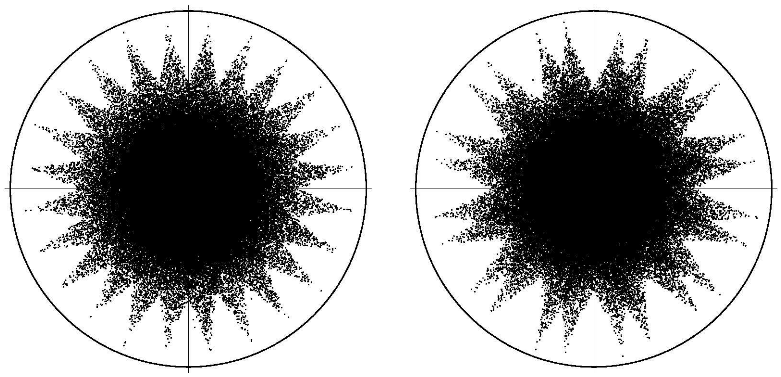


Конфигурации 4-х треугольников. Множества $E(f,X)$ с $X = 1300000$. Левый рисунок соответствует полиному $f(x) = 7x^4 + x$. Из четырёх треугольников, один сформирован точками $E_p(f)$ с $p \equiv 1, 5, 9, 13, 25, 45 \pmod{56}$, другой – точками $E_p(f)$ с $p \equiv 3, 15, 19, 23, 27, 39 \pmod{56}$, третий – точками $E_p(f)$ с $p \equiv 11, 31, 43, 47, 51, 55 \pmod{56}$, четвёртый – точками $E_p(f)$ с $p \equiv 17, 29, 33, 37, 41, 53 \pmod{56}$. Правый рисунок соответствует полиному $f(x) = 6x^4+4x^3+x^2+5x$. Из четырёх трегольников, один сформирован точками $E_p(f)$ с $p \equiv 1, 19 \pmod{24}$, другой – точками $E_p(f)$ с $p \equiv 5, 23 \pmod{24}$, третий – точками $E_p(f)$ с $p \equiv 7, 13 \pmod{24}$, четвёртый – точками $E_p(f)$ с $p \equiv 11, 17 \pmod{24}$.



Конфигурации 8-и треугольников. Множества $E(f,X)$ с $X = 2000000$. Левый рисунок соответствует полиному $f(x) = 8x^4 + 16x^3 + x^2 +$

$7x$. Каждому из восьми классов $r \mod 16$ взаимнопростых с модулем соответствует треугольник сформированный точками $E_p(f)$ с $p \equiv r \pmod{16}$. Правый рисунок соответствует полиному $f(x) = 3x^4 + 4x^3 + x^2 + 5x$. Каждому из восьми классов $r \mod 24$ взаимнопростых с модулем соответствует треугольник сформированный точками $E_p(f)$ с $p \equiv r \pmod{24}$.



§7. Радиальное распределение

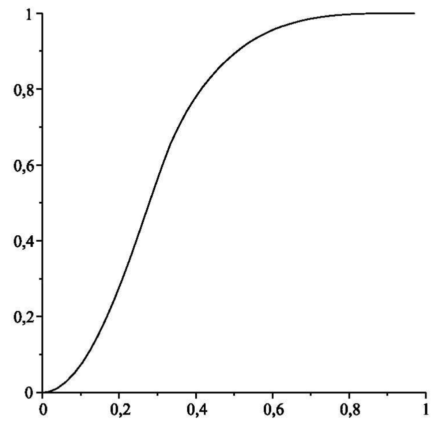
С фиксированным полиномом f, рассмотрим распределение точек $|E_p(f)|$ на отрезке $[0, 1]$. Для каждого отрезка $\Omega \subset [0, 1]$ положим

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

В предположении, что пределы в правой части существуют, значения $\mu(\Omega)$ меры μ аппроксимируются посредством

$$\frac{1}{\pi(X)} \sharp \Big\{ p \leqslant X \;\Big|\; |E_p(f)| \in \Omega \Big\} \tag{5}$$

с большим X. Возьмём $\Omega = [0, z]$ с $z \in [0, 1]$ и будем трактовать (5) как функцию z. Исключим из рассмотрения полиномы f из §4. Ниже на рисунке показан график функции (5), соответствующей любому из полиномов f рассмотренных в §5 и §6 и достаточно большому X.



Сказать точнее, на рисунке показан график функции (5) для $f(x) = 7x^4+x$ и $X = 1300000$, а для других полиномов f графики отличаются от этого разве что на толщину линии. Основываясь на этом наблюдении, *мы ожидаем, что существует предел* (4) *для любого отрезка* $\Omega \subset [0, 1]$ *и что предел не зависит от произвола в выборе полинома* f *из классов, рассмотренных в* §5 *и* §6. Если это правильно, то равенством (4) определяется одна мера, общая для всех f, и было бы желательно определить эту меру как-то более явно.

Список литературы

1. J.-P. Serre, *Majorations de sommes exponentielles.* — Société Mathématique de France, Asterisque **41–42** (1977), 111–126.
2. S. A. Stepanov, *Arithmetic of algebraic curves*, Moscow, 1991 (in Russian). English translation: Springer–Verlag, 1995.
3. Н. В. Проскурин, *О некоторых кубических экспоненциальных суммах.* — Зап. научн. семин. ПОМИ **502** (2021), 122–132.
4. Н. В. Проскурин, *Об экспоненциальных суммах и цветах.* — Зап. научн. семин. ПОМИ **502** (2021), 133–138.
5. B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi sums*, Wiley-Interscience Publication, 1998.
6. C. F. Gauss, *Theoria residuorum biquadraticorum, Commentatio prima*, Comment. Soc. Reg. Sci. Gottingensis 6 (1828), 28 pp.

Proskurin N. V. On quadric exponential sums.

By numerical experiments, some structures in distribution of quadratic additive exponential sums in finite fields were discovered.

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 12 сентября 2022 г.