DOI 10.1007/s10958-022-05986-7
Journal of Mathematical Sciences, Vol. 264, No. 2, June, 2022

ON SOME CUBIC EXPONENTIAL SUMS

N. V. Proskurin* UDC 511, 512.624

By numerical experiments, some unexpected structures in the distribution of cubic additive exponential sums in finite fields are discovered. A preliminary classification and some conjectures are presented. Bibliography: 2 titles.

1. Preliminaries

Consider the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of prime order p, its additive character

$$x \mapsto e_p(x) = \exp(2\pi i x/p), \quad x \in \mathbb{F}_p,$$

a polynomial f over $\mathbb{F}_p$, and the related [1, 2] exponential sum of additive type

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

The fundamental inequality

$$\Big| \sum_{x \in \mathbb{F}_p} e_p\big(f(x)\big) \Big| \le (\deg f - 1)\sqrt{p} \tag{2}$$

holds for all such sums whenever $p \nmid \deg f$. In connection with the reciprocity law, Gauss was able to evaluate the quadratic sums, i.e., those with f of degree 2. Many authors have studied, numerically and analytically, the Kummer and Birch sums. These are the sums with $f(x) = x^3$ and $f(x) = x^3 + cx$, c being a coefficient in $\mathbb{F}_p$. These sums are located in the interval $[-2\sqrt{p}, 2\sqrt{p}] \subset \mathbb{R}$.

2. Set up

Let f be a one-variable polynomial over $\mathbb{Z}$. Reducing its coefficients modulo p, we may regard f as a polynomial over an arbitrary field $\mathbb{F}_p$. We are interested in the distribution of the points

$$E_p(f) = \frac{1}{(\deg f - 1)\sqrt{p}} \sum_{x \in \mathbb{F}_p} e_p\big(f(x)\big) \tag{3}$$

in the disk $D = \big\{ z \in \mathbb{C} \;\big|\; |z| \le 1 \big\}$. For any fixed f, we consider the points (3) for all primes p. By (2), the points are located in the unit disk D (except for the case where $p \mid \deg f$). One may expect that limit formulas of the form

$$\lim_{x \to \infty} \frac{1}{\pi(x)} \sharp \Big\{ p \le x \;\Big|\; E_p(f) \in \Omega \Big\} = \int_\Omega P(z)\, dz, \quad \text{with} \quad \Omega \subset D, \tag{4}$$

are valid. Here, the probability density P depends on f only, and $\pi(x)$ denotes the number of all primes $p \le x$. One may also expect that similar formulas can be found for the limits

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

with $\Phi(z) = |z|$ and $\Omega \subset [0, 1]$ or $\Phi(z) = \arg z$ and $\Omega \subset (-\pi, \pi]$.

*St.Petersburg Department of V. A. Steklov Mathematical Institute of the Russian Academy of Sciences, St.Petersburg, Russia, e-mail: np@pdmi.ras.ru.

Translated from *Zapiski Nauchnykh Seminarov POMI*, Vol. 502, 2021, pp. 122–132. Original article submitted September 14, 2021.

In order to make an idea of a possible distribution of the points $E_p(f)$, we have evaluated them numerically in a wide range[1] of cubic polynomials f and prime numbers p. Given a polynomial f and a large integer X, we have plotted the points $E_p(f)$ for all primes $p \leq X$. The points form a certain configuration

$$E(f, X) = \left\{ E_p(f) \;\middle|\; p \text{ is prime } \leq X \right\} \subset \mathbb{C},$$

which may serve as an instructive visualization for the distribution problem.

In this paper, we report on our quite unexpected observations concerning the configurations $E(f, X)$ with cubic polynomials f. The configurations $E(f, X)$ split into two classes. One of them splits further into a series of subclasses, as we will explain below. Also, we advance a conjecture (see (7)) on the distribution of the points $|E_p(f)|$, which is similar to the Sato–Tate conjecture concerning the Kloosterman sums[2].

3. Radial distribution

Given a cubic polynomial f, consider the distribution of the points $|E_p(f)|$ in the interval $[0, 1]$. Turn to (5) with $\Phi(z) = |z|$ and $\Omega \subset [0, 1]$. The limit in (5) is approximated by

$$\frac{1}{\pi(X)} \sharp \left\{ p \leq X \;\middle|\; |E_p(f)| \in \Omega \right\} \tag{6}$$

with a large X. We may take $\Omega = [0, z]$ with $z \in [0, 1]$ and treat (6) as a function of z. We have numerically confirmed (for many different f and X) a very good agreement of the function (6) with the function

$$z \mapsto \frac{4}{\pi} \int_0^z \sqrt{1 - x^2}\, dx.$$

Based on this observation, we conjecture that

$$\lim_{x \to \infty} \frac{1}{\pi(x)} \sharp \left\{ p \leq x \;\middle|\; |E_p(f)| \in \Omega \right\} = \frac{4}{\pi} \int_\Omega \sqrt{1 - x^2}\, dx \tag{7}$$

for all cubic polynomials f and all intervals $\Omega \subset [0, 1]$. The density on the right-hand side of (7) is known in connection with the distribution of the numbers of points on elliptic curves and with the distribution of the Kloosterman sums.

4. Clusters

In Fig. 1 below, we have plotted the real coordinate axis, the imaginary coordinate axis, the unit disk $D \subset \mathbb{C}$, and the points $E_p(f) \in D$ for the polynomial $f(x) = 5x^3 + x^2 - 4x$ and all primes $p \leq X$ with $X = 150000$. The set $E(f, X)$ looks like a globular cluster. We see similar clusters $E(f, X)$ for many other polynomials f. In particular, for the polynomials

$$f(x) = ax^3 + bx^2 + cx + d$$

with the coefficients

$$a = 3, 5, 6, 7, \quad b = 1, 2, 4, \quad c = -4, \ldots, 4,$$

and an arbitrary $d \in \mathbb{Z}$. In seems probable that the cluster $E(f, X)$ remains a cluster for arbitrary values of the coefficient c.

[1] We will consider polynomials f with zero constant term only because the limits we are interested in (4), (5) are independent of the constant term of a polynomial f.

[2] For the Kloosterman sums (instead of (1)) and the interval $[-1, 1]$ (instead of D), it is conjectured that the limit formula (4) holds with $P(z) = (2/\pi)\sqrt{1 - z^2}$.

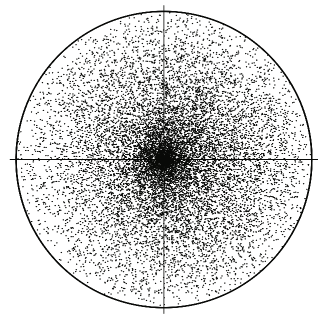

Fig. 1. The set $E(f,X)$ with $f(x) = 5x^3 + x^2 - 4x$ and $X = 150000$.

Consider the arguments of the points $E_p(f)$. One may expect that the points $\arg E_p(f)$ are uniformly distributed in $(-\pi, \pi]$, i.e.,

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sharp \Big\{ p \le x \;\Big|\; \arg E_p(f) \in \Omega \Big\} = \frac{1}{2\pi} \Lambda(\Omega),$$

where $\Lambda(\Omega)$ denotes the length of the interval $\Omega \subset (-\pi, \pi]$. However, upon performing computations with all primes $p \le 250000$, we have some doubts about this formula.

5. Asters

Consider the set $E(f,X)$ of all points $E_p(f)$ with prime numbers $p \le X$, $f(x) = 6x^3 + 3x^2 + 4x$, and $X = 100000$. The plot is presented in Fig. 2. It is seen that the points $E_p(f)$ are concentrated along 6 lines passing through the point 0. The counterclockwise angles between the lines and the real axis are equal to $\pi m/3 + \pi n/9$ with $m = 0, 1, 2$ and $n = 1, 2$. We say that the polynomial f and the set $E(f,X)$ belong to the class aster-6 or aster-6-2, where the index 2 indicates that the set of 6 lines splits into pairs of lines with a common m.

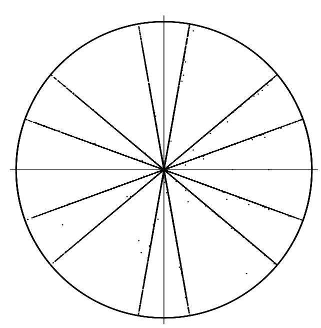

Fig. 2. The set $E(f,X)$ with $f(x) = 6x^3 + 3x^2 + 4x$ and $X = 100000$.

The points distributed sporadically are those few points $E_p(f)$ that are located far away from the limit lines.

Consider yet another example. Let $f(x) = 5x^3 + 6x^2 + 4x$, $X = 100000$. The plot is presented in Fig. 3. In this case, the points $E_p(f)$ are concentrated along 20 lines passing through the point 0. The counterclockwise angles between the lines and the real axis are equal to $\pi m/5 + \pi n/25$ with $m = 0, \dots, 4$ and $n = 1, \dots, 4$. We say that the polynomial f and the set $E(f,X)$ are of the type aster-20 or aster-20-4, where the index 4 indicates that the set of 20 lines splits into 4-line bundles with a common m.

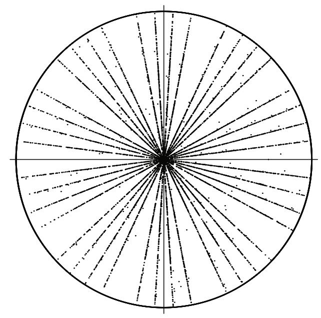

Fig. 3. The set $E(f, X)$ with $f(x) = 5x^3 + 6x^2 - 3x$ and $X = 100000$.

It is worth emphasizing once again that the points $E_p(f)$ are concentrated along the limit lines rather than lie on them.

Turning to formula (4), we see that for the aster classes, the right-hand side should be replaced with

$$\sum_L \int_{\Omega \cap L} P_L(z)\, dz,$$

where the sum is taken over the limit lines L, and P_L are some density functions.

Our computations performed for the polynomials $f(x) = ax^3 + bx^2 + cx$ with positive $a \le 7$, $b \le 3a/2$, c satisfying the condition $|c| \le 4$, and $X = 100000$, lead to the following 8 classes:

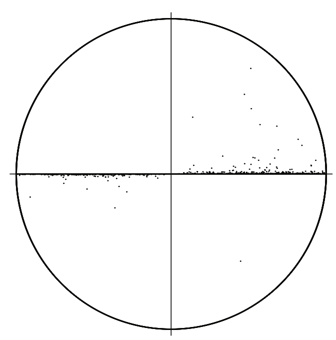

Fig. 4. $E(f, X)$ for $f(x) = 2x^3 + 3x^2 - 4x$; the points are concentrated along the real axis; aster-1.

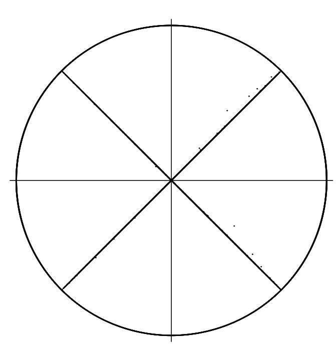

Fig. 5. $E(f, X)$ for $f(x) = 4x^3 + 3x^2$; aster-2.

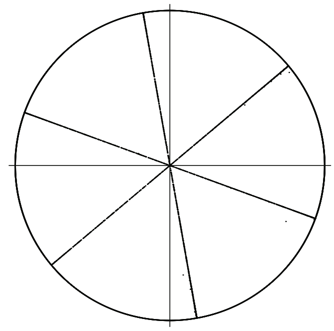

Fig. 6. $E(f,X)$ for $f(x) = 3x^3 + 3x^2 + x$; aster-3.

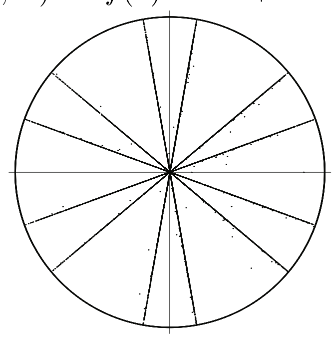

Fig. 7. $E(f,X)$ for $f(x) = 3x^3 + 3x^2 + 3x$; aster-6-2.

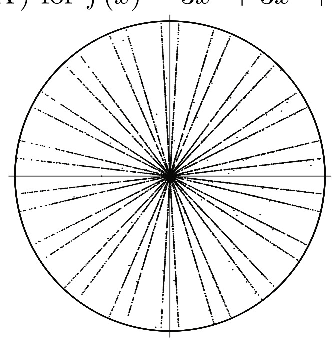

Fig. 8. $E(f,X)$ for $f(x) = 2x^3 + 2x^2 + 3x$; aster-18-2.

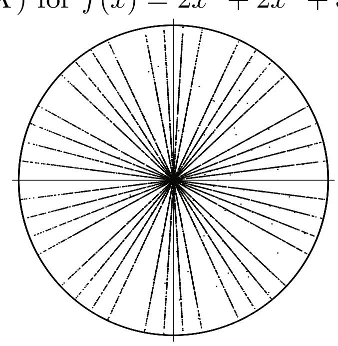

Fig. 9. $E(f,X)$ for $f(x) = 5x^3 + 3x^2 + 3x$; aster-20-4.

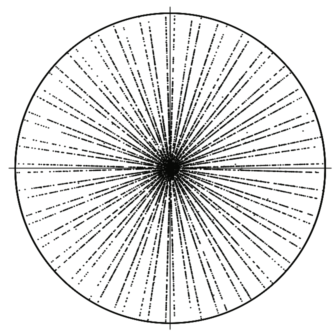

Fig. 10. $E(f,X)$ for $f(x)=4x^3+x^2-3x$; aster-36-2.

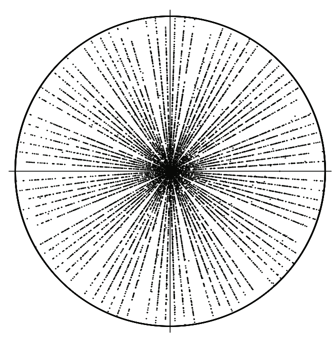

Fig. 11. $E(f,X)$ for $f(x)=7x^3+9x^2$; aster-42-6.

All the polynomials $f(x)=ax^3+bx^2+cx+d$ with an arbitrary $d\in\mathbb{Z}$ and a,b,c in the list below fall into aster classes. Of course, this list is not exhaustive.

- Let $a=2$, $b=3$, or $a=4$, $b=6$, or $a=6$, $b=9$. The polynomials f with $c=-4,\dots,4$ fall into the class aster-1. Also, all the polynomials f with $b=0$ fall into this class.
- If $a=4$, $b=3$, $c=-3,\dots,3$, then f falls into the class aster-2.
- Let $a=b=3$, or $a=b=6$, or $a=6$, $b=3$. The polynomials f with $c=-3,\dots,3$ fall into the class aster-6-2, except for those with $a=b=3$, $c=1$ and $a=b=6$, $c=2$, which fall into the class aster-3.
- Let $a=b=1,2,4,5,7$, or $a=2$, $b=1$, or $a=4$, $b=2$. The polynomials f with $c=-4,\dots,4$ fall into the class aster-18-2.
- If $a=5$, $b=3,6$, $c=-3,\dots,3$, then f falls into the class aster-20-4.
- If $a=4$, $b=1,5$, $c=-3,\dots,3$, then f falls into the class aster-36-2.
- If $a=7$, $b=3,6,9$, $c=-3,\dots,3$, then f falls into the class aster-42-6.

Translated by the author.

REFERENCES

1. J.-P. Serre, “Majorations de sommes exponentielles,” *Astérisque*, **41–42**, 111–126 (1977).
2. S. A. Stepanov, *Arithmetic of Algebraic Curves* [in Russian], Nauka, Moscow (1991).