Some observations on degree 3 and 4 exponential sums over finite fields

N. V. Proskurin

Abstract. By numerical experiments, it is discovered some strictures in distribution of cubic and quartic exponential sums of additive type in finite fields. Concerning the cubic sums, we give a theoretical explanation for that. For the quartic sums, we observe numerically that Euler's deltoid play role in their distribution.

Introduction

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 one-variable polynomial f over $\mathbb{F}_p$ and an additive type exponential sum

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

The Weil inequality $|\, S_p(f) \,| \le (\deg f - 1)\sqrt{p}$ is valid for all the sums whenever $p \nmid \deg f$. That means, the points

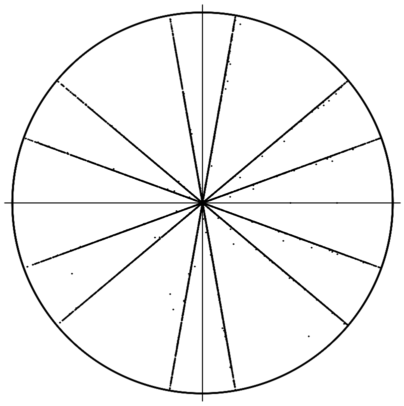
$$E_p(f) = \frac{1}{(\deg f - 1)\sqrt{p}}\, S_p(f)$$

are located in the unit disk $D = \big\{ z \in \mathbb{C} \;\big|\; |z| \le 1 \big\}$. See [1], [2].

Given a one-variable polynomial f over $\mathbb{Z}$, consider f as a polynomial over each of $\mathbb{F}_p$ just by reduction its coefficients $\bmod\, p$. Then one may look on distribution of the points $E_p(f)$ (with prime $p = 2, 3, 5, 7 \ldots$) in the disk D. We have used computer algebra systems PARI and MAPLE to study numerically the sums $S_p(f)$ for lot of polynomials f of degree 3 and 4.

Cubic sums

Consider one instructive sample in [3]. On the picture 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 $f(x) = 6x^3 + 3x^2 + 4x$ and for all prime $p \leq 100000$.



The points $E_p(f)$ are concentrated mainly along few lines passing through the point 0. One has a similar picture for other polynomials as well. The number of lines depends on f.

To state our results, let us agree to write $\{t\}$ for the fractional part of $t \in \mathbb{R}$. We have proved [4] the following two propositions.

Consider a cubic polynomial $f(x) = ax^3 + bx^2 + cx$ *over* $\mathbb{Z}$. *Let* l *be an integer,* $\gcd(l, 3a) = 1$, *and let* p *be any prime under the conditions* $lp + 1 \equiv 0 \bmod 27a^3$ *and* $p \nmid 6a$. *If* $S_p(f) \neq 0$, *then the real axis forms the angle*

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

with the line passing through the points 0 *and* $S_p(f)$.

This proposition implies easily the second one.

Consider a cubic polynomial $f(x) = ax^3 + bx^2 + cx + d$ *over* $\mathbb{Z}$. *The points* $E_p(f)$ *are concentrated along the lines that pass through the point* 0 *and intersect the real axis under the angles*

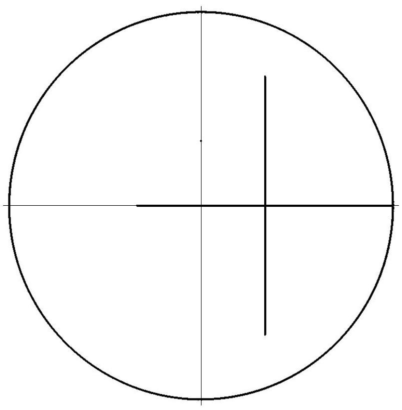
$$\theta = 2\pi \left\{ \frac{b\,(2b^2 - 9ac)}{27a^2}\, l \right\}$$

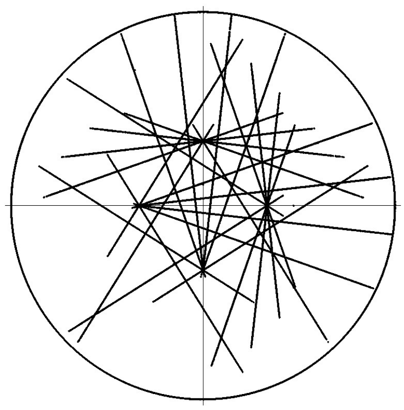
with $l \in \mathbb{Z}$ *under the condition* $\gcd(l, 3a) = 1$.

This result gives us full description of the asters attached to cubic polynomials in [3]. Also, it shows that there are no at all the clusters considered in [3].

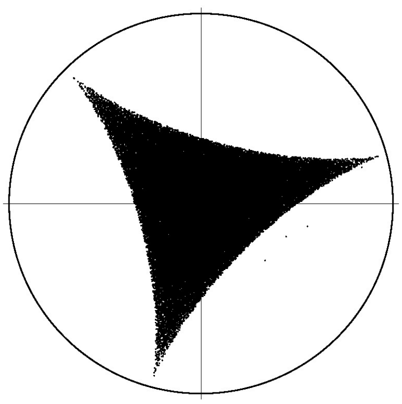
Quartic sums

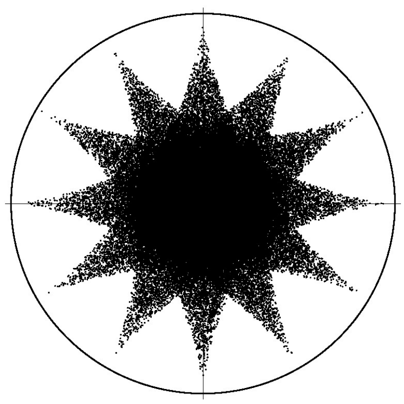
For some quartic polynomials f, we have find empirically that almost all of the points $E_p(f)$ are located on few intervals in D. Let us look on two samples. On the pictures below we have plotted the real and imaginary coordinate axes, the disk $D \subset \mathbb{C}$, and the points $E_p(f) \in D$ for chosen polynomials f and for all prime $p \leq 480000$. The sums $S_p(f)$ with $f(x) = x^4$ are nothing but the biquadratic Gauss sums. By known explicit formulas, one has either $E_p(f) = i/3$ or $E_p(f) \in [-1/3, 1]$ or $E_p(f) \in [1/3 - 2i/3, 1/3 + 2i/3]$ according to $p \equiv 3 \pmod 4$ or $p \equiv 1 \pmod 8$ or $p \equiv 5 \pmod 8$. This case is represented by the left-hand side picture below.





The right-hand side picture represents similarly the case $f(x) = 7x^4 + x^2$. Assume $r \in \mathbb{Z}$ and $\gcd(r, 56) = 1$. It seems reasonable to expect that the points $E_p(f)$ with $p \equiv r \pmod{56}$ form one of 24 intervals shown on the picture.
There are other polynomials f with entirely different distribution of the points $E_p(f)$. Two typical samples are given on the pictures below.

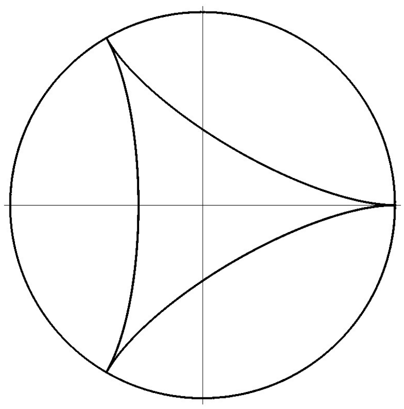




For the polynomial $f(x) = 4x^4 + 8x^3 + 3x^2 + 6$, the points $E_p(f)$ with $p \leq 1000000$ forms the left-hand side picture. We see that the points $E_p(f)$ are located within some three-cusped curve. The right-hand side picture is formed similarly for $f(x) = 7x^4 + 1$. For a lot of polynomials f, we have similar pictures "formed by 1, 2, 4, 8 triangles bounded by the same three-cusped curve".

We conjecture that the three-cusped curve discussed is the Euler deltoid considered in 1745 *in connection with an optical problem.*

The deltoid can be defined as the curve consisting of the points $z = x + iy \in \mathbb{C}$ satisfying $3(x^2 + y^2)(x^2 + y^2 + 2) = 8x^3 - 24xy^2 + 1$ with $x, y \in \mathbb{R}$.



Also, the deltoid can be created by a point on the circumference of a circle of radius 1/3 as it rolls without slipping along the inside of a circle of radius 1.

References

[1] J.-P. Serre, *Majorations de sommes exponentielles*, Société Mathématique de France, Asterisque 41–42, p. 111–126, 1977.

[2] S. A. Stepanov, *Arithmetic of algebraic curves*, Moscow, 1991 (in Russian). English translation: Springer–Verlag, 1995.

[3] N. V. Proskurin, *On some cubic exponential sums*, Zap. Nauchn. semin. POMI, vol. 502, 122–132, 2021 (in Russian).

[4] N. V. Proskurin, *Distribution of cubic exponential sums*, Zap. Nauchn. semin. POMI, vol. 511, 161–170, 2022 (in Russian).

[5] N. V. Proskurin, *On quartic exponential sums*, Zap. Nauchn. semin. POMI, vol. 517, 162–175, 2022 (in Russian).

N. V. Proskurin
St. Petersburg Department of Steklov Institute of Mathematics RAS,
191023, Fontanka 27, St. Petersburg, Russia
e-mail: `np@pdmi.ras.ru`