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

N. V. Proskurin, PDMI, St. Petersburg

April 18, 2023

Set up

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 related exponential sum of additive type

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

The sums have been studied by Gauss, Kummer, Artin, Davenport, Hasse, Weil, Birch, Patterson and other authors in connection with reciprocity lows and other problems in number theory.

One knows, the classical Weil inequality

$$|\,S_p(f)\,| \le (\deg f - 1)\sqrt{p}$$

is valid for all the sums whenever $p \nmid \deg f$. That means, one has

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

with some points $E_p(f)$ located in the unit disk

$$D = \{z \in \mathbb{C} \mid |z| \le 1\}.$$

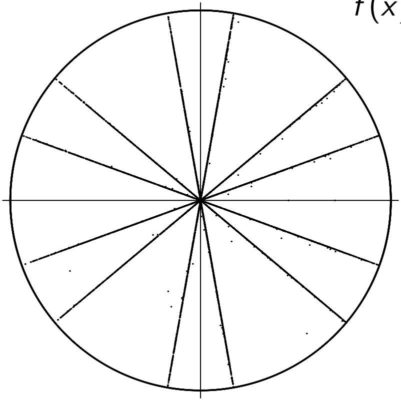
Given a polynomial f over $\mathbb{Z}$, we may naturally consider f as a polynomial over each of $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $p = 2, 3, 5, 7, \ldots$, and we may look on

Distribution of the points $E_p(f)$ in the disk D.

That is the main problem we are interested in our experiments. We have used computer algebra systems PARI and MAPLE to study numerically the sums $S_p(f)$ and the related points $E_p(f)$ for lot of polynomials f of degree 3 and 4.

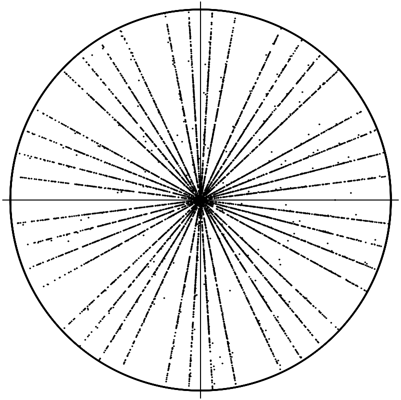
Cubic sums.

Let us begin with some instructive samples. We have plotted the real and imaginary coordinate axes, the disk D and the points $E_p(f)$ for $f(x) = 6x^3 + 3x^2 + 4\,x$ and $p \leq 100000$.



It is seen that the points $E_p(f)$ are concentrated along 6 lines passing through the point 0. The points distributed sporadically are those few $E_p(f)$ that are located far away from the limit lines.

For one more sample, we take $f(x) = 5x^3 + 6x^2 - 3x$. This case, the points $E_p(f)$ with $p \leq 100000$ are concentrated along 20 lines passing through the point 0.



One has a similar aster-type pictures for lot of cubic polynomials over $\mathbb{Z}$. The points $E_p(f)$ are concentrated along few lines passing through the point 0.

I talked about that at PCA 2022.

Now we can supply these observations with proofs.

To state our results, let us agree to write $\{t\}$ for the fractional part of $t \in \mathbb{R}$. We have 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*

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

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.

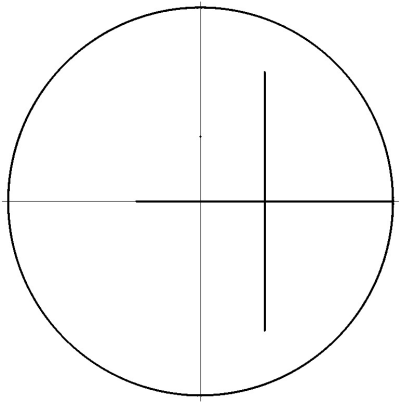
Quartic sums.

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. To illustrate this phenomenon, consider 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 $p \leq 480000$.

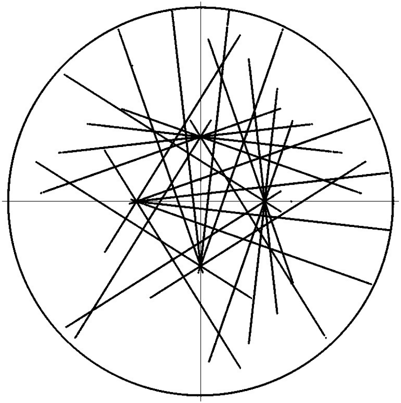
For the first sample, take $f(x) = x^4$. This case, the sums $S_p(f)$ are nothing but the biquadratic Gauss sums. These $S_p(f)$ are the only quartic sums known explicitly.

By Gauss 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 $p \equiv 3 \bmod 4$ or $p \equiv 1 \bmod 8$ or $p \equiv 5 \bmod 8$.



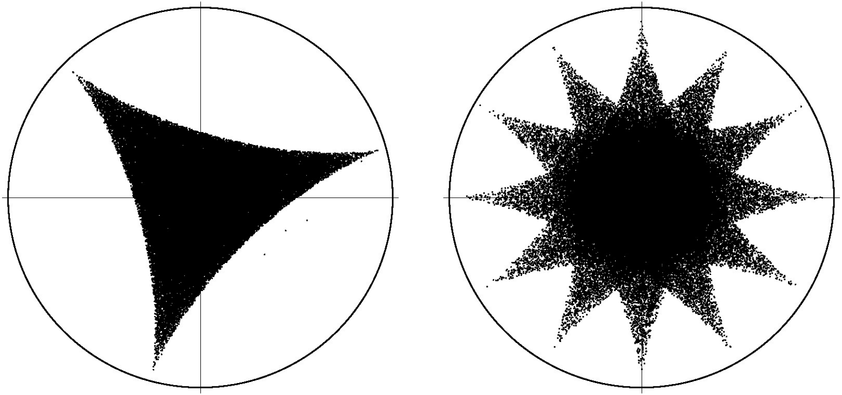
The points $E_p(f)$ form dense subsets of the intervals.

For the second sample, take $f(x) = 7x^4 + x^2$. The picture consists of 24 intervals and one more point. Assume $r \in \mathbb{Z}$ and $\gcd(r, 56) = 1$.



It seems reasonable to expect that the points $E_p(f)$ with $p \equiv r \bmod 56$ 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.

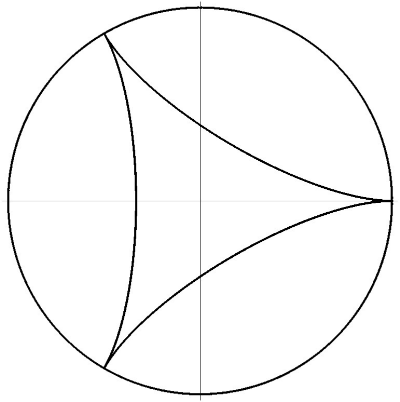


For the polynomial $f(x) = 4x^4 + 8x^3 + 3x^2 + 6$, the points $E_p(f)$ with $p \le 1000000$ forms the left-hand side picture. We see that the points $E_p(f)$ are located within some three-cusped curve. The right-hand side picture is formed similarly for $f(x) = 7x^4 + 1$. For a lot of polynomials f, 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 consists of the points $z = x + iy \in \mathbb{C}$ satisfying

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



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.

$$S_p(f) = \begin{cases} \sqrt{p} \pm \sqrt{2p + 2a\sqrt{p}} & \text{for} \quad p \equiv 1 \bmod 8 \\ \sqrt{p} \pm i\sqrt{2p - 2a\sqrt{p}} & \text{for} \quad p \equiv 5 \bmod 8 \end{cases}$$

$$a^2 + b^2 = p, \quad a \equiv -1 \bmod 4, \quad a, b \in \mathbb{Z}$$