On some numerical experiments with character sums over finite fields

N. V. Proskurin

Abstract. By numerical experiments, it is discovered some strictures in distribution of cubic exponential sums in finite fields. It is given a conjecture on distribution of these sums.

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 [1], [2] character (or exponential) sum of additive type

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

By Weil, the fundamental inequality

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

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

$$E_p(f) = \frac{1}{(\deg f - 1)\sqrt{p}} \sum_{x\in\mathbb{F}_p} e_p\big(f(x)\big) \tag{2}$$

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

Let f be a one-variable polynomial over $\mathbb{Z}$. By reduction its coefficients mod p, we may consider f as a polynomial over any $\mathbb{F}_p$. Then one may look on distribution of the points $E_p(f)$ $(p = 2, 3, 5, 7 \dots)$ in the disk D. One may also look on distribution of the points $|E_p(f)|$ $(p = 2, 3, 5, 7 \dots)$ in the interval $[0, 1]$. We have studied numerically the sums (1) for lot of cubic polynomials f. We have used computer algebra systems PARI and MAPLE. Our main observations are as follows.

(I) For any positive $x \in \mathbb{R}$, let $\pi(x)$ be the number of prime $p \le x$. Given a cubic polynomial f, some positive $X \in \mathbb{R}$, and some interval $\Omega \subset [0,1]$ consider

$$\frac{1}{\pi(X)} \sharp \Big\{ p \le X \;\Big|\; |E_p(f)| \in \Omega \Big\}. \tag{3}$$

We may take $\Omega = [0,z]$ with $z \in [0,1]$ to treat (3) as a function of z. We find numerically (for many different f and large X) very good agreement of the function (3) with the function

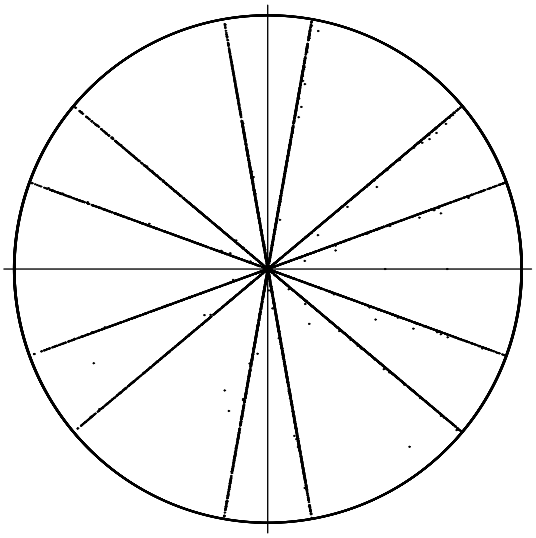
$$z \mapsto \frac{4}{\pi} \int\limits_0^z \sqrt{1-x^2}\, dx.$$

Based on this observation, *we conjecture*

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

for all cubic polynomials f and all intervals $\Omega \subset [0,1]$. That may be considered as an analogue of the classical Sato–Tate conjecture on distribution of the Kloosterman sums. The density on the right-hand side is known also in connection with the distribution of the numbers of points on elliptic curves.

(II) Let us consider one instructive sample. 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 numbers $p \le 100000$.



The points $E_p(f)$ with $f(x) = 6x^3 + 3x^2 + 4x$ and prime $p \le 100000$.

It is seen that the points $E_p(f)$ are concentrated along 6 lines passing through the point 0. We see that the points $E_p(f)$ are just concentrated along the limit lines rather than lie on them. The counterclockwise angles between the lines and the real axis are $\pi m/3 + \pi n/9$ with $m = 0, 1, 2$ and $n = 1, 2$. The points distributed sporadically are those few $E_p(f)$ that are located far away from the limit lines.

We have found a similar aster-type pictures for many other cubic polynomials $ax^3 + bx^2 + cx + d$ over $\mathbb{Z}$. We have no theoretical explanation to this phenomenon. The number of lines depends on the coefficients a, b, c. Looking for possible classification, we may say the polynomial f falls to the class aster-m if we see m limit lines on the picture. In this sense, the above polynomial f falls to the class aster-6. Some other classes are given in [3].

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).

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