Some problems on character sums in finite fields

N. V. Proskurin, PDMI, St.-Petersburg

October 14, 2020

Kloosterman sums and Sato-Tate measure

Given prime p, consider the field $\mathbb{Z}/p\mathbb{Z}$ of order p and some non-trivial additive character

$$e_p : \mathbb{Z}/p\mathbb{Z} \to \mathbb{C}^\star,$$

i.e. non-trivial homomorphism of the additive group $\mathbb{Z}/p\mathbb{Z}$ to the multiplicative group $\mathbb{C}^\star$ of the complex field $\mathbb{C}$. Then

$$Kl_p(c) = \sum_{t \in \mathbb{Z}/p\mathbb{Z} \setminus \{0\}} e_p(t^{-1} + ct) \quad \text{with} \quad c \in \mathbb{Z}$$

are well-known *Kloosterman sums*. According to Weil (1948),

$$|Kl_p(c)| \leq 2\sqrt{p}$$

and one may look on distribution of the points

$$\frac{Kl_p(c)}{2\sqrt{p}} \quad \text{in the interval} \quad [-1,1] \subset \mathbb{R}.$$

On this interval, one has a probability measure

$$[u,v] \mapsto \frac{2}{\pi} \int_u^v \sqrt{1-t^2}\, dt$$

for all $[u,v] \subset [-1,1]$, which is known as *Sato-Tate measure*.
It is expected, that

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sharp\left\{p \le x \;\middle|\; \frac{Kl_p(c)}{2\sqrt{p}} \in [u,v]\right\} = \frac{2}{\pi} \int_u^v \sqrt{1-t^2}\, dt$$

for all $[u,v] \subset [-1,1]$, $c \in \mathbb{Z}$. Hereafter $\pi(x)$ denotes the number of all prime $p \le x$.

Writing $\vartheta(p,c)$ for a unique number in $[0,\pi]$ under the condition

$$Kl_p(c) = 2\sqrt{p}\,\cos\vartheta(p,c),$$

we get an equivalent conjecture:

$$\lim_{x\to\infty}\frac{1}{\pi(x)}\sharp\left\{p\le x\;\middle|\;\theta(p,c)\in[u,v]\right\}=\frac{2}{\pi}\int_u^v \sin^2 t\,dt$$

for all $[u,v]\subset[0,\pi]$ and $c\in\mathbb{Z}$. A probability measure on $[0,\pi]$ in the right-hand side also known as *Sato-Tate measure*.

For this problem we can refer to J.-P. Serre (Asterisque 41–42, 1977) and to N. M. Katz (Ann. of Math. St. 116, 1988).

Elliptic curves

Originally, the Sato-Tate measure is related to elliptic curves.
By Hasse theorem, if E_p is an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$, then the number of its points equals

$$p + 1 + R_p \quad \text{with} \quad R_p \quad \text{satisfying} \quad |R_p| \leq 2\sqrt{p}.$$

Now, let E be an elliptic curve defined over $\mathbb{Q}$. For almost all p, its reduction E_p modulo p is an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$.
The *Sato-Tate conjecture* states

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sharp\left\{p \leq x \;\middle|\; \frac{R_p}{2\sqrt{p}} \in [u, v]\right\} = \frac{2}{\pi} \int_u^v \sqrt{1 - t^2}\, dt$$

for all $[u, v] \subset [-1, 1]$. (For exceptional p, take $R_p = 0$.)
After R. Taylor (2007), one knows the conjecture holds for non-CM curves with a non-integral j-invariants.

Polynomial character sums

Given polynomials a, b over $\mathbb{Z}$ and a multiplicative character χ_p of $\mathbb{Z}/p\mathbb{Z}$ (extended by $\chi_p(0) = 0$), let

$$S_p = \sum_{t \in \mathbb{Z}/p\mathbb{Z}} \chi_p(a(t))\, e_p(b(t)). \qquad (*)$$

That is (mixed) polynomial character sum.
We intend to consider possible analogues of the Sato-Tate type conjectures for the sums like $(*)$.

Let us remark that the Kloosterman sums are the sums of type $(*)$. Explicitly, one has Fourier series expension

$$Kl_p(c) = \sum_{t \in \mathbb{Z}/p\mathbb{Z}} \kappa_p(t^2 - 4c)\, e_q(t)$$

where κ_p is a unique quadratic character of $\mathbb{Z}/p\mathbb{Z}$, $p \neq 2$.

Under some very general assumptions, the Artin L-function attached to a, b, χ_p, S_p can be written as the product

$$L(z; a, b) = \prod_{j=1}^{k} (1 - \omega_j z) \quad \text{with some} \quad \omega_1, \ldots, \omega_k \in \mathbb{C},$$

and one has

$$S_p = -\sum_{j=1}^{k} \omega_j \quad \text{where} \quad k = n + m - 1,$$

$b \bmod p$ is a polynomial of degree n;
radical of $a \bmod p$ is a polynomial of degree m;
($m = \deg(a_1 \ldots a_r)$, if $a \bmod p = a_1^{s_1} \ldots a_r^{s_r}$ with a_j irreducible over $\mathbb{Z}/p\mathbb{Z}$.)

For the zeros of the Artin L-functions we have

$$|\omega_j| = \sqrt{p} \quad \text{for all} \quad j = 1, \ldots, k,$$

That is analoq of the Riemann hypotheses for the zeta-function. It has been proved by Weil (1948). (Some particular cases were known befor him.)
As a consequence, we have the fundamental estimate for polynomial character sums:

$$|S_p| \leq (n + m - 1)\sqrt{p}, \qquad (**)$$

We refer to J.-P. Serre (Asterisque 41–42, 1977) for review of general theory and to S. A. Stepanov for monography on arithmetic of algebraic curves (1991).

Choice of characters

To study distribution of the sums $(*)$, i. e.

$$S_p = \sum_{t \in \mathbb{Z}/p\mathbb{Z}} \chi_p(a(t))\, e_p(b(t)),$$

in dependence of prime p and to state something like the Sato-Tate conjecture, we need a natural and fruitful agreement on the choice of characters χ_p and e_p.
It seems, there is no problem with choice of additive characters e_p.
Just take any non-zero $f \in \mathbb{Z}$ and take

$$e_p(x) = \exp\left(2\pi i f x/p\right) \quad \text{for all prime } p \text{ and } x \in \mathbb{Z}.$$

Also, there is no problem with sums S_p attached to trivial and quadratic characters χ_p. That is so, because of uniqueness of such characters for each prime p.
The case of higer order multiplicative characters χ_p is entirely different. To deal with the sums S_p attached to the characters χ_p of order $h \geq 3$ we suggest the following construction.

First, introduce some 'auxiliary' $l \in \mathbb{Z}$ and some $w \in \mathbb{C}$, which is degree h primitive root of 1. Next,

Let Ω_l be the set of all prime $p \equiv 1 \pmod{h}$ under the condition: for the field $\mathbb{Z}/p\mathbb{Z}$, there exists a unique character χ_p of order h such that $\chi_p(l) = w$.

Here $p \equiv 1 \bmod h$ is a necessary and sufficient condition for existence of order h characters χ_p. The uniqueness can be restated as follows: h is coprime with the index of l relative to some (hence, any) generator of the multiplicative group of the field $\mathbb{Z}/p\mathbb{Z}$. In particular, for prime h, that means l is not h-th degree in $\mathbb{Z}/p\mathbb{Z}$.

From now on we fix l, h, w, the set Ω_l above, and the characters χ_p.

For any $x \in \mathbb{R}$, let $\pi_I(x) = \sharp \left\{ p \in \Omega_I \;\middle|\; p \le x \right\}$. Assume, the sums S_p are majorized as in $(**)$, that is $|S_p| \le (n+m-1)\sqrt{p}$.

Let $D \subset \mathbb{C}$ be the circle of radius $R = n+m-1$ with center at 0.

We suggest the following statement as an adequate analog or generalization of the conjecture above for the Kloosterman sums.

For any (good) measurable set $V \subset D$, we expect

$$\lim_{x\to\infty} \frac{1}{\pi_I(x)} \sharp \left\{ p \in \Omega_I \;\middle|\; p \le x,\ S_p/\sqrt{p} \in V \right\} = \int_V C(z)\, dz,$$

where $C : D \to \mathbb{R}$ is a real positive measurable function, depending on parameters a, b, w, I only. This function C should be determined.

In the case $S_p \in \mathbb{R}$ for all $p \in \Omega_I$, it is reasonable to replace the circle D with the interval $D \cap \mathbb{R}$ and to treat V as subintervals $\subset D \cap \mathbb{R}$.

In this context, one can consider similar questions on the limits

$$\lim_{x\to\infty} \frac{1}{\pi_I(x)} \sharp \left\{ p \in \Omega_I \;\middle|\; p \le x,\ |S_p|^2/p \in V \right\} \quad \text{with} \quad V \subset [0, R^2],$$

$$\lim_{x\to\infty} \frac{1}{\pi_I(x)} \sharp \left\{ p \in \Omega_I \;\middle|\; p \le x,\ \theta_p \in V \right\} \quad \text{with} \quad V \subset [0, 2\pi]$$

and with θ_p under the conditions $S_p = |S_p| \exp(i\theta_p)$, $\theta_p \in [0, 2\pi]$.