On some computational problems with character sums

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

April 22, 2021

Kloosterman sums, elliptic curves and Sato-Tate measure

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

$$e_p(t) = \exp(2\pi i t/p), \qquad t \in \mathbb{F}_p,$$

let us consider *Kloosterman sums*

$$Kl_p(c) = \sum_{t \in \mathbb{F}_p^\star} e_p(t^{-1} + ct), \qquad \mathbb{F}_p^\star = \mathbb{F}_p \setminus \{0\}, \quad c \in \mathbb{F}_p.$$

The sums are real satisfying

$$-2\sqrt{p} \le Kl_p(c) \le 2\sqrt{p} \qquad \text{(Weil, 1948)}$$

and one may look on their distribution in this interval.

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 $[u,v] \subset [-1,1]$. Here $\pi(x) = \sharp\{\text{prime } p \le x\}$ and

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

is known as *Sato-Tate measure*.

See J.-P. Serre (Asterisque 41–42, 1977) and N. M. Katz (Ann. of Math. St. 116, 1988).

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

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

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 $\mathbb{F}_p$.
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 $[u, v] \subset [-1, 1]$. (R. Taylor (2007) proved the conjecture holds for non-CM curves with a non-integral j-invariants.)

Polynomial character sums

Given polynomials f, g over $\mathbb{Z}$ and a character χ_p of $\mathbb{F}_p^\star$ (extended to all of $\mathbb{F}_p$ by $\chi_p(0) = 0$), let

$$S_p = \sum_{t \in \mathbb{F}_p} \chi_p(f(t))\, e_p(g(t)). \qquad (*)$$

That are *polynomial character sums*. As an example, one has

$$Kl_p(c) = \sum_{t \in \mathbb{F}_p} \kappa_p(t^2 - 4c)\, e_p(t)$$

with prime $p \neq 2$ and with a unique quadratic character κ_p of $\mathbb{F}_p^\star$.

Under some general assumptions, one has fundamental Weil estimate for polynomial character sums:

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

where $n = \deg(g \bmod p)$ and $m = \deg\big(\text{radical}\,(f \bmod p)\big)$.

If $f \bmod p = f_1^{s_1} \dots f_r^{s_r}$ with integers $s_1, \dots, s_r \geq 1$ and irreducible over $\mathbb{F}_p$ polynomials $f_1, \dots, f_r$, then $m = \deg(f_1 \dots f_r)$. In particaular, if χ_p is a character of order $h \geq 2$, $n = 0$, and $\gcd(h, s_1, \dots, s_r) = 1$ then one has $(**)$.

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

Set up

Looking for analogues of the Sato-Tate type conjectures for the polynomial character sums $(*)$ involving characters χ_p of arbitrary order, we suggest the following general construction.

Let $w \in \mathbb{C}$ be a primitive root of 1 of degree h. Given $l \in \mathbb{Z}$, let $\Omega_{l,w}$ be the set of all prime $p \equiv 1 \pmod h$ under the condition: there exists a unique character χ_p of order h, such that $\chi_p(l) = w$.

Here $p \equiv 1 \pmod h$ provides existence of order h characters χ_p of $\mathbb{F}_p^\star$. The uniqueness can be stated as follows: h is coprime with the index of l relative to any generator of $\mathbb{F}_p^\star$. For prime h, that means l is not h-th degree in $\mathbb{F}_p^\star$.

Let $\pi_{l,w}(x) = \sharp\left\{ p \in \Omega_{l,w} \;\middle|\; p \le x \right\}$ for any $x \in \mathbb{R}$.

Assume, $|S_p| \le R\sqrt{p}$ with $R = n + m - 1$ (as in $(**)$).

Let $D = \left\{ z \in \mathbb{C} \;\middle|\; |z| \le R \right\}$.

We suggest to treat the measures

$$\lim_{x\to\infty} \frac{1}{\pi_{l,w}(x)} \sharp\left\{ p \in \Omega_{l,w} \;\middle|\; p \le x,\ S_p/\sqrt{p} \in V \right\}, \quad V \subset D,$$

and their densities as analogues of the Sato-Tate ones given above.

For some classes of character sums, we have explicit equalities for $|S_p|$ instead of $(**)$. Say, we have $|S_p| = \sqrt{p}$ for the Gauss sums and the Jacobi sums. In the cases like that we should take V to be circular arc $\subset D = \left\{ z \in \mathbb{C} \;\middle|\; |z| = 1 \right\}$.

First sample

Cosider the character sums $(*)$ with simplest f and g.

If one of f, g is a polynomial of degree 0 and the second one is a polynomial of degree 1, say $ux + v$ with $u, v \in \mathbb{Z}$, $u \neq 0$, then $S_p = 0$ for all prime p excepting $p|u$. This is not interesting.

Let $\deg f = \deg g = 0$. This case is far from to be trivial. The polynomials are just constants $c, d \in \mathbb{Z}$ and S_p is the sum of p terms $\chi_p(c)\, e_p(d)$. Assume $c \neq 0$ to avoid the case $S_p = 0$.

Following our general point of view, we should consider the limit

$$\lim_{x\to\infty} \frac{1}{\pi_{I,w}(x)} \sharp \left\{ p \in \Omega_{I,w} \;\middle|\; p \le x,\ \ \chi_p(c)\, e_p(d) \in V \right\}$$

as the measure of the circular arc $V \subset \left\{ z \in \mathbb{C} \;\middle|\; |z| = 1 \right\}$. We can prove this limit is equal to the sum of limits

$$\lim_{x\to\infty} \frac{1}{\pi_{I,w}(x)} \sharp \left\{ p \in \Omega_{I,w} \;\middle|\; p \le x,\ \ \chi_p(c) = v \right\}$$

expanded over all v under the conditions $v^h = 1$ and $v \in V$. Numerical computation with Maple shows (in some cases) the latter limit does not depend on v.

Gauss sums

Let $f(t) = g(t) = t$. The character sums in $(*)$ occur to be

$$G(\chi_p) = \sum_{t \in \mathbb{F}_p} \chi_p(t)\, e_p(t).$$

That are the *Gauss sums*. For non-trivial characters χ_p, one has not only the Weil estimate $(**)$ but

$$|G(\chi_p, e_p)| = \sqrt{p}$$

as well. From our general point of view, we should consider the limit

$$\lim_{x \to \infty} \frac{1}{\pi_{I,w}(x)}\, \sharp \left\{ p \in \Omega_{I,w} \;\middle|\; p \le x,\;\; G(\chi_p, e_p)/\sqrt{p} \in V \right\}$$

as the measure of the circular arc $V \subset \left\{ z \in \mathbb{C} \,\middle|\, |z| = 1 \right\}$.

Multiplicative sums

Let us consider the polynomial character sums $(*)$ with zero polynomial g, i. e. the sums

$$S_p = \sum_{z \in \mathbb{F}_p} \chi_p\big(f(z)\big)$$

involving the multiplicative characters only. Looking for the sums convenient for numerical experiments we find the ones with

$$f(z) = az^m + b \quad \text{and} \quad a, b, m \in \mathbb{Z}, \quad ab \neq 0, \quad m \geq 0.$$

For such a binomial f and any non-trivial character χ one has

$$\sum_{z \in \mathbb{F}_p} \chi\big(f(z)\big) = \chi(b) \sum_{\theta} \theta(-b/a)\, J(\theta, \chi), \qquad (***)$$

where the summation runs over characters θ of orders dividing $\gcd(\deg f, p-1)$ and $J(\theta, \chi)$ are the *Jacobi sums*,

$$J(\theta, \chi) = \sum_{z \in \mathbb{F}_p} \theta(z)\, \chi(1-z).$$

For $(***)$ see R. Lidl, H. Niederreiter, Finite fields. There are only few terms in the right-hand side. One can evaluate the Jacobi sums in terms of the Gauss ones. Say, if the characters θ, χ and $\theta\chi$ are non-trivial, then $J(\theta, \chi) = G(\theta)\, G(\chi)/G(\theta\chi)$.
This observations provide effective method for computing the sums $(***)$ with any coefficients a, b. It is convenient to use Maple with its number theory package and primroot command.