PROCEEDINGS OF THE
ROMAN NUMBER THEORY ASSOCIATION
Volume 3, *Number* 1, *March* 2018, *pages* 7-12

René Schoof

On the argument of certain exponential sums

Written by Giacomo Cherubini

1 Statement of the main result

Consider a prime number $p > 2$, and let g be a non-square modulo p. Let χ be a non-trivial character modulo p, i.e. $\chi : \mathbb{F}_p^\times \to \mathbb{C}^\times$. Denote by $z_p = \exp(2\pi i/p) \in \mathbb{C}$.

Theorem 1. *For $n \in \mathbb{F}_p^\times$, the complex numbers*

$$\sigma_n = \chi(n) \sum_{r \in \mathbb{F}_p} \chi(r^2 - g) z_p^{rn}$$

all have the same argument modulo π.

In other words, the numbers σ_n lie on a line in the complex plane.

Theorem 2. If χ is quadratic, then the numbers σ_n are real, and therefore they are on a line. Theorem 1 has also been verified on a computer for $p < 300$ and every χ. From the numerics it seems possible that $|\sigma_n| \leq 2\sqrt{p}$.

Theorem 3. The proof of Theorem 1 uses methods from the theory of modular forms. A key formula comes from Mercuri's thesis [2]. It would be interesting to find an elementary proof that avoids such heavy machinery.

2 Proof

Since for quadratic charachters we have seen that the result is trivial, we can assume that $\chi^2 \neq 1$. Let f be a normalized eigenform of weight 2 in $S_2(\Gamma_1(p), \chi^2)$. The Fourier expansion of f has the form

$$f = \sum_{n\geq 1} a_n e^{2\pi i n\tau}, \quad \tau \in \mathbb{H}, a_n \in \mathbb{C},$$

with $a_1 = 1$ and a_n algebraic integers. It is possible to twist the form f by χ^{-1}. If we do so, a theorem of Atkin and Li [1] tells us that the result is still a modular form. More precisely, we have the following.

Theorem 4 (Atkin-Li (1978)). *The function*

$$f \otimes \chi^{-1} = \sum_{n\geq 1} a_n \chi^{-1}(n) e^{2\pi i n\tau}$$

is a modular form in $S_2(\Gamma_0(p^2))$.

We note that $\Gamma_0(p^2)$ is conjugate to another group, which we denote $\Gamma_s(p)$, defined by

$$\Gamma_s(p) := \{A \in \mathrm{SL}_2(\mathbb{Z}) : \ A \equiv \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \pmod{p}\}.$$

The group

$$T = \{\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix} \in \mathrm{GL}_2(\mathbb{F}_p)\}$$

is called *split* torus, from which the subscript for $\Gamma_s(p)$. With this notation we have

$$\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} \Gamma_0(p^2) \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}^{-1} = \Gamma_s(p).$$

Now, since the groups $\Gamma_0(p^2)$ and $\Gamma_s(p)$ are conjugate, the corresponding modular curves are isomorphic, and we can transform modular forms for one group into modular forms for the other one, they are in bijection. The result of the change is that the form $\tilde{f}$ defined by

$$\tilde{f} = \sum_{n\geq 1} a_n \chi^{-1}(n) q^n, \quad q = e^{\frac{2\pi i \tau}{p}}$$

is a modular form in $S_2(\Gamma_s(p))$. If $\Gamma(p)$ denotes the principal congruence subgroup of level p, we have the inclusions

$$S_2(\Gamma_s(p)) \subset S_2(\Gamma(p)) \subset \mathrm{Ind}_{\mathrm{SL}_2(\mathbb{F}_p)}^{\mathrm{GL}_2(\mathbb{F}_p)} S_2(\Gamma(p),$$

where the last set is constructed by inducing the action of $\mathrm{SL}_2(\mathbb{F}_p)$ on $S_2(\Gamma(p))$, and it can be identified with $\Omega^1_{X(p)}$, that is, the holomorphic differentials on the modular curve $X(p)$ (note that the induction multiplies the dimension by $p-1$).

If $X_s(p)$ denotes the modular curve associated to the group $\Gamma_s(p)$, we have the maps

$$X(p) \longrightarrow X_s(p) \longrightarrow j\text{-line},$$

where the bigger extension has Galois group $\mathrm{GL}_2(\mathbb{F}_p)/\{\pm 1\}$. This group acts also on $\Omega^1_{X(p)}$, and therefore on $\tilde{f}$. However, $\tilde{f}$ is special because it sits inside $S_2(\Gamma_s(p))$, it is a normalized eigenform and it is T-invariant.

Fact: the $\mathrm{GL}_2(\mathbb{F}_p)$-submodule V generated by $\tilde{f}$ in $\Omega^1_{X(p)}$ is an irreducible representation of $\mathrm{GL}_2(\mathbb{F}_p)$ (this follows from the multiplicity one theorem).

Now, the irreducible representations of $\mathrm{GL}_2(\mathbb{F}_p)$ are completely classified (this is a result in group theory and has nothing to do with modular forms). Moreover V has an explicit description, and it is $(p+1)$-dimensional (this follows from $\chi^2 \neq 1$). V can be realized over $\mathbb{Q}(z_d + z_d^{-1})$, where d is the order of χ. Hence the set

$$\Omega^1_{X(p)} \otimes_{\mathbb{Q}} \mathbb{Q}(z_d + z_d^{-1})$$

contains V. The Galois action on $\Omega^1_{X(p)}$ commutes with $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ because the curve is defined over $\mathbb{Q}$.

We observe that the coefficients of $\tilde{f}$ are real. This is because all eigenforms that are contained in $S_2(\Gamma_0(p^2))$ have real Fourier coefficients, and $\tilde{f}$ comes from one of such forms, therefore has real Fourier coefficients. Moreover, after tensoring with $\mathbb{Q}(z_d + z_d^{-1})$, it is still invariant under the Galois action.

We look now at the group (non-split torus)

$$T' = \{\begin{pmatrix} a & gb \\ b & a \end{pmatrix} : a, b \in \mathbb{F}_p, (a, b) \neq (0, 0)\} \cong \mathbb{F}_{p^2}^{\times}.$$

Fact. We have $\dim V^T = \dim V^{T'} = 1$. Hence there exists a generator which is invariant under the action of $G_{K(z_d+z_d^{-1})}$, where $K = \mathbb{Q}(\{\chi^{-1}(n)a_n\}_{n\geq 1})$, and a generator of $V^{T'}$ which is invariant under $G_{K(z_d+z_d^{-1},z_p)}$. This is almost sufficient to say that the coefficients themselves are invariant under the Galois action, but we must be careful with the cusps, since these are not defined over $\mathbb{Q}$ but over $\mathbb{Q}(z_p)$.

Since the space is one-dimensional, the normalizer N' of T' (it has index 2) acts as ± 1, and we discuss the two cases separately.

Case 1. N' acts as $+1$. Then the cusps are defined over $K(z_d + z_d^{-1}, z_p + z_p^{-1}) \subseteq \mathbb{R}$. The generator is

$$\sum b_n q^n, \quad b_n \in \mathbb{R}$$

and all other elements in the space are multiples of this. We can construct elements by taking traces of some element in V_χ. It turns out that the modular form

$$f = \sum a_n e^{2\pi i \tau n}$$

that we started with is contained in V, and we can take the T'-trace of this element (this result is taken from [2]). We obtain

$$\sum a_n \sum_{r\in\mathbb{F}_p} \chi(r^2 - g) z_p^{rn} q^n = \sum a_n \chi^{-1}(n)\chi(n) \sum_{r\in\mathbb{F}_p} \chi(r^2 - g) z_p^{rn} q^n,$$

and this must be equal to

$$c \sum b_n q^n, \quad c \in \mathbb{C}.$$

Comparing the coefficients of q^n (and recalling that $a_n \chi^{-1}(n)$ are real because they are the coefficients of $\tilde{f}$), it follows that the argument of the inner sum

$$\chi(n) \sum_{r \in \mathbb{F}_p} \chi(r^2 - g) z_p^{rn}$$

is the same as $\arg(c)$, for all n, unless for some $n_0 \in \mathbb{F}_p^*$ we have that $a_n = 0$ for all $n \equiv n_0 \bmod p$. To show that this cannot happen, it is enough to find $a_n \neq 0$. More precisely, for every residue class $n_0 \in \mathbb{F}_p^\times$ we need to show that there exists $n \equiv n_0 \bmod p$ with $a_n \neq 0$. It is enough to find $n = \ell$ a prime such that $a_\ell \neq 0$. Assume that this is false. Then all the primes in the class of n_0 have $a_\ell = 0$, and hence we have a set of density $(p-1)^{-1}$ of primes for which $a_\ell = 0$. But a result of Serre is saying that the set $\{\ell : a_\ell = 0\}$ has density zero. Hence a contradiction, and we conclude that there must be ℓ such that $a_\ell \neq 0$.

Case 2. When N' acts as -1 then the cusp is anti-invariant, and all the coefficients are in $i\mathbb{R}$ instead of $\mathbb{R}$. Hence they are again on a line and the rest of the argument works similarly as in case 1.

References

[1] A. O. L. Atkin and W.-C. W. Li, *Twists of newforms and pseudo-eigenvalues of W-operators*, Inventiones Mathematicae, **48** (1978), no. 3, 221–243.

[2] P. Mercuri, *Rational points on modular elliptic curves*, Ph. D. thesis, Università La Sapienza, Roma, 2014.

Giacomo Cherubini
Max Planck Institute for Mathematics
Vivatsgasse 7
53111 Bonn Germany.
email: cherubini@mpim-bonn.mpg.de