Math. Res. Lett. **17** (2010), *no.* 04, 689–699

ON THE DISTRIBUTION OF THE NUMBER OF POINTS ON ALGEBRAIC CURVES IN EXTENSIONS OF FINITE FIELDS

Omran Ahmadi and Igor E. Shparlinski

Abstract. Let $\mathcal{C}$ be a smooth absolutely irreducible curve of genus $g \geq 1$ defined over $\mathbb{F}_q$, the finite field of q elements. Let $\#\mathcal{C}(\mathbb{F}_{q^n})$ be the number of $\mathbb{F}_{q^n}$-rational points on $\mathcal{C}$. Under a certain multiplicative independence condition on the roots of the zeta-function of $\mathcal{C}$, we derive an asymptotic formula for the number of $n = 1, \ldots, N$ such that $(\#\mathcal{C}(\mathbb{F}_{q^n}) - q^n - 1)/2gq^{n/2}$ belongs to a given interval $\mathcal{I} \subseteq [-1, 1]$. This can be considered as an analogue of the Sato–Tate distribution which covers the case when the curve $\mathbf{E}$ is defined over $\mathbb{Q}$ and considered modulo consecutive primes p, although in our scenario the distribution function is different. The above multiplicative independence condition has, recently, been considered by E. Kowalski in statistical settings. It is trivially satisfied for ordinary elliptic curves and we also establish it for a natural family of curves of genus $g = 2$.

1. Introduction

Let $\mathcal{C}$ be a smooth absolutely irreducible curve of genus $g \geq 1$ defined over the finite field $\mathbb{F}_q$ of q elements. We denote by $\mathcal{C}(\mathbb{F}_{q^n})$ the set of the $\mathbb{F}_{q^n}$-rational points on the projective model of $\mathcal{C}$.

By the Weil theorem,

$$|\#\mathcal{C}(\mathbb{F}_{q^n}) - q^n - 1| \leq 2gq^{n/2}$$

see [24, Section VIII.5, Bound (5.7)], however the distribution of values of $\#\mathcal{C}(\mathbb{F}_{q^n})$ inside of the interval $[q^n + 1 - 2gq^{n/2}, q^n + 1 + 2gq^{n/2}]$, in particular, the distribution of the ratios

$$\frac{\#\mathcal{C}(\mathbb{F}_q) - q - 1}{2gq^{1/2}} \in [-1, 1]. \tag{1}$$

is not understood well enough.

In the case of elliptic curves $\mathcal{C} = \mathcal{E}$ more is known. For example, the distribution of the ratios (1), where the curve $\mathcal{E}$ is defined over $\mathbb{Q}$ and reduced modulo consecutive primes p (that is, $q = p$) is described by the *Sato–Tate conjecture*, which has been recently proven by R. Taylor [33]. In particular, the proportion of primes $p \leq x$ for which the analogue of the above ratios belongs to the interval $[\beta, \gamma]$ is given by

$$\mu_{ST}(\beta, \gamma) = \frac{2}{\pi} \int_{\max\{0,\beta\}}^{\min\{1,\gamma\}} \sqrt{1 - \alpha^2}\, d\,\alpha,$$

as $x \to \infty$.

B. J. Birch [6] has also established an analogue of the Sato–Tate conjecture in the dual case when the finite field $\mathbb{F}_q$ is fixed and the ratios (1) are taken over all elliptic curves $\mathbf{E}$ over $\mathbb{F}_q$, see also [35].

Received by the editors August 11, 2009. Revision received January 14, 2010.

Finally, there is also a series of works showing that similar type of behavior also holds in mixed situations (when both the field and the curve vary) over various families of curves, see [2, 5].

Here we fix a smooth absolutely irreducible curve $\mathcal{C}$ of genus $g \geq 1$ over $\mathbb{F}_q$ and consider analogue of the ratios (1) taken in the consecutive extensions of $\mathbb{F}_q$, that is, for $\mathbb{F}_{q^n}$-rational points on $\mathcal{C}$. We write the cardinality $\#\mathcal{C}(\mathbb{F}_{q^n})$ of the sets of $\mathbb{F}_{q^n}$-rational points on the projective model of $\mathcal{C}$ as

$$\#\mathcal{C}(\mathbb{F}_{q^n}) = q^n + 1 - a_n.$$

and study the distribution of the ratios

$$\alpha_n = \frac{a_n}{2gq^{n/2}} \in [-1, 1], \qquad n = 1, 2, \ldots. \tag{2}$$

Under a certain additional condition or multiplicative independence of so-called *Frobenius eigenvalues* of $\mathcal{C}$ we obtain an asymptotic formula for the distribution function of the ratios (2). By a result of E. Kowalski [18], the additional condition needed for our proofs to work is satisfied for a wide class of curves. We are also grateful to Nick Katz for an observation that a result of N. Chavdarov [8] can also be used to show that the desired property holds for a "typical" curve.

Here, we also show that this additional condition holds for so called *ordinary* elliptic curves and ordinary smooth curves of genus $g = 2$ whose Jacobians are absolutely simple. The latter result can be of independent interest.

In particular, for $g = 1$, that is, when $\mathcal{C} = \mathcal{E}$ is an ordinary elliptic curve, our result implies that the distribution of the ratios (2) is not governed by $\mu_{ST}(\beta, \gamma)$ but rather by a different distribution function

$$\lambda_1(\beta, \gamma) = \frac{1}{\pi} \int_{\max\{0,\beta\}}^{\min\{1,\gamma\}} (\sqrt{1 - \alpha^2})^{-1} d\,\alpha. \tag{3}$$

We also remark that for supersingular elliptic curves we have $a_n = 0$ for every odd n (and $a_n = 2q^{n/2}$ for every even n).

Throughout this paper, the implied constants in the symbols 'O' and '$\ll$' may depend on the base field $\mathbb{F}_q$ (we recall that $A \ll B$ and $B \gg A$ are equivalent to $A = O(B)$).

2. Main Results

2.1. Frobenius Angles. We refer to [24] for a background on curves and their zeta-functions.

For a smooth projective curve $\mathcal{C}$ over the finite field $\mathbb{F}_q$ we define the zeta-function of C as

$$Z(T) = \exp\left(\sum_{n=1}^{\infty} \#\mathcal{C}(\mathbb{F}_{q^n}) \frac{T^n}{n}\right).$$

It is well-known that if $\mathcal{C}$ is of genus $g \geq 1$ then

$$Z(T) = \frac{P(T)}{(1-t)(1-qt)},$$

where $P(T)$ is a polynomial of degree $2g$ with integer coefficients.

Furthermore we have

$$P(t) = \prod_{j=1}^{2g} (1 - \tau_j T)$$

where $\tau_1, \ldots, \tau_{2g}$ are called the *Frobenius eigenvalues* and satisfy

$$|\tau_j| = q^{1/2}, \quad \tau_{j+g} = \overline{\tau}_j, \qquad j = 1, \ldots, g, \tag{4}$$

(where $\overline{\tau}$ means complex conjugate of τ), see [24, Section VIII.5].

If C is considered over the degree m extension of $\mathbb{F}_q$, then

$$Z_m(T) = \exp\left(\sum_{n=1}^{\infty} \#\mathcal{C}(\mathbb{F}_{q^{mn}}) \frac{T^n}{n} \right) = \frac{P_m(T)}{(1-T)(1-qT)}, \tag{5}$$

where

$$P_m(T) = \prod_{j=1}^{2g} (1 - \tau_j^m T)$$

It is also well-known that

$$\#\mathcal{C}(\mathbb{F}_{q^n}) = q^n + 1 - \sum_{j=1}^{2g} \tau_j^n \tag{6}$$

which underlies our method.

Furthermore, we write (4) as

$$\tau_j = q^{1/2} e^{\pi i \vartheta_j} \qquad \text{and} \qquad \tau_{j+g} = q^{1/2} e^{-\pi i \vartheta_j}, \tag{7}$$

with some $\vartheta_j \in [0, 1]$, $j = 1, \ldots, g$, which we call *Frobenius angles*. (sometimes $\pi\vartheta_j$ is called a Frobenius angle)

We show that if $1, \vartheta_1, \ldots, \vartheta_g$ are linearly independent over $\mathbb{Z}$, or alternatively $q^{1/2}$, $\tau_1, \ldots, \tau_g$ are multiplicatively independent over $\mathbb{Z}$, then the ratios (2) are distributed in accordance with the distribution function $\lambda_g(\beta, \gamma)$ which for $g = 1$ is defined by (3) and then recursively as

$$\lambda_g(\beta, \gamma) = \frac{1}{\pi} \int_0^1 \lambda_{g-1} \left(g\beta - \cos(\pi\alpha), g\gamma - \cos(\pi\alpha) \right) d\,\alpha \tag{8}$$

and give an estimate on the error term.

2.2. Distribution of the Number of Points in Extensions. For a fixed absolutely irreducible curve $\mathcal{C}$ over $\mathbb{F}_q$, let $T_{\beta,\gamma}(N)$ be the number of ratios $\alpha_n \in [\beta, \gamma]$ for $n = 1, \ldots, N$.

We say that real numbers $\psi_1, \ldots, \psi_s$ are linearly independent modulo 1 if and only if $1, \psi_1, \ldots, \psi_s$ are linearly independent over $\mathbb{Z}$.

Theorem 1. *Suppose $\mathcal{C}$ is a smooth absolutely irreducible curve of genus $g \geq 1$ over $\mathbb{F}_q$ such that $\vartheta_1, \ldots, \vartheta_g$ are linearly independent modulo 1. Then there is a constant $\eta > 0$ depending only on q and g such that uniformly over $-1 \leq \beta \leq \gamma \leq 1$ we have*

$$T_{\beta,\gamma}(N) = \lambda_g(\beta, \gamma) N + O(N^{1-\eta}).$$

where λ_g is defined by (8).

2.3. Linear Independence of Frobenius Angles. We say that $\mathcal{C}$ is an ordinary curve if and only if at least half of the Frobenius eigenvalues $\tau_1, \overline{\tau}_1, \ldots, \tau_g, \overline{\tau}_g$ are p-adic units where p is the characteristic of $\mathbb{F}_q$, see [13, Definition 3.1] for several equivalent definitions. Notice that all the Frobenius eigenvalues are algebraic numbers. So whenever they are considered as p-adic numbers it is implied that we have chosen an embedding of $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}}_p$ allowing us to view Frobenius eigenvalues as p-adic numbers.

Theorem 2. *Suppose $\mathcal{C}$ is a smooth projective curve of genus $g \le 2$ over $\mathbb{F}_q$. Furthermore suppose that $\mathcal{C}$ is either an ordinary elliptic curve or is a curve of genus $g = 2$ which has an absolutely simple Jacobian. Then the Frobenius angles $\vartheta_1, \ldots, \vartheta_g$ are linearly independent modulo* 1.

3. Proof of Theorem 1

3.1. Preparation. We see from (6) and (7) that

$$\alpha_n = \frac{1}{g} \sum_{j=1}^{g} \cos(\pi \vartheta_j n). \tag{9}$$

Therefore, denoting via $\mathcal{V}_g(\beta, \gamma)$ the g-dimensional domain consisting of points $(\psi_1, \ldots, \psi_g) \in [0,1]^g$ such that

$$\beta \le \frac{1}{g} \sum_{j=1}^{g} \cos(\pi \psi_j) \le \gamma$$

we see that

$$T_{\beta,\gamma}(N) = \#\{n = 1, \ldots, N \ : \ (\vartheta_1 n, \ldots, \vartheta_g n) \in \mathcal{V}_g(\beta, \gamma)\}. \tag{10}$$

Thus it is natural that we use tools from the theory of uniformly distributed sequences to estimate $T_{\beta,\gamma}(N)$.

3.2. Background on the Uniform Distribution. For a finite set $\mathcal{F} \subseteq [0,1]^s$ of the s-dimensional unit cube, we define its *discrepancy with respect to a domain* $\Xi \subseteq [0,1]^s$ as

$$\Delta(\mathcal{F}, \Xi) = \left| \frac{\#\{\mathbf{f} \in \mathcal{F} : \ \mathbf{f} \in \Xi\}}{\#\mathcal{F}} - \mu(\Xi) \right|,$$

where μ is the Lebesgue measure on $[0,1]^s$.

We now define the *discrepancy* of $\mathcal{F}$ as

$$D(\mathcal{F}) = \sup_{\Pi \subseteq [0,1]^s} \Delta(\mathcal{F}, \Pi),$$

where the supremum is taken over all boxes $\Pi = [\alpha_1, \beta_1) \times \ldots \times [\alpha_s, \beta_s) \subseteq [0,1]^s$, see [9, 20].

We define the distance between a vector $\mathbf{u} \in [0,1]^s$ and a set $\Xi \subseteq [0,1]^s$ by

$$\operatorname{dist}(\mathbf{u}, \Xi) = \inf_{\mathbf{w} \in \Xi} \|\mathbf{u} - \mathbf{w}\|,$$

where $\|\mathbf{v}\|$ is the Euclidean norm of $\mathbf{v}$. Given $\varepsilon > 0$ and a domain $\Xi \subseteq [0,1]^s$ we define the sets

$$\Xi_\varepsilon^+ = \{\mathbf{u} \in [0,1]^s \backslash \Xi \ : \ \operatorname{dist}(\mathbf{u}, \Xi) < \varepsilon\}$$

and

$$\Xi_\varepsilon^- = \{\mathbf{u} \in \Xi \ : \ \operatorname{dist}(\mathbf{u}, [0,1]^s \backslash \Xi) < \varepsilon\}.$$

Let $h(\varepsilon)$ be an arbitrary increasing function defined for $\varepsilon > 0$ such that

$$\lim_{\varepsilon \to 0} h(\varepsilon) = 0.$$

As in [21, 30], we define the class $\mathcal{S}_h$ of domains to include domains $\varXi \subseteq [0,1]^s$ for which

$$\mu\left(\varXi_\varepsilon^+\right) \le h(\varepsilon) \qquad \text{and} \qquad \mu\left(\varXi_\varepsilon^-\right) \le h(\varepsilon).$$

A relation between $D(\mathcal{F})$ and $\varDelta(\mathcal{F}, \varXi)$ for $\varXi \in \mathcal{S}_h$ is given by the following inequality of [21] (see also [30]).

Lemma 3. *For any domain $\varXi \in \mathcal{S}_h$, we have*

$$\varDelta(\mathcal{F}, \varXi) \ll h\left(s^{1/2} D(\mathcal{F})^{1/s}\right).$$

Finally, the following bound, which is a special case of a more general result of H. Weyl [34] shows that if $\varXi$ has a piecewise smooth boundary then $\varXi \in \mathcal{S}_h$ for some function $h(\varepsilon) = O(\varepsilon)$.

Lemma 4. *For any domain $\varXi \in [0,1]^s$ with piecewise smooth boundary, we have*

$$\mu\left(\varXi_\varepsilon^\pm\right) = O(\varepsilon).$$

Clearly the domain $\mathcal{V}_g(\beta, \gamma)$ satisfies the condition of Lemma 4. Thus we see from Lemma 4 that we need to estimate the discrepancy of the points

$$(\vartheta_1 n, \ldots, \vartheta_g n), \qquad n = 1, \ldots, N. \tag{11}$$

This is a well-studied question, however the answer depends on the Diophantine properties of $\vartheta_1, \ldots, \vartheta_g$, see [9, 20]. More specifically, we denote by $\mathbb{R}^+$ the set of positive real numbers and by $\|z\|$ the distance between a real z and the closest integer. We now recall [9, Theorem 1.80]

Lemma 5. *Suppose that $\psi_1, \ldots, \psi_s$ are linearly independent modulo 1 and that for some continuous function $\varphi(t) : \mathbb{R}^+ \to \mathbb{R}^+$ such that $\varphi(t)/t$ is monotonically increasing for real $t \ge 1$ we have*

$$\|k_1\psi_1 + \ldots + k_s\psi_s\| \ge \frac{1}{\varphi\left(\max\{|k_1|, \ldots, |k_s|\}\right)}$$

for any non-zero vector $(k_1, \ldots, k_s) \in \mathbb{Z}^s$. Then the discrepancy $D(N)$ of the sequence

$$(\psi_1 n, \ldots, \psi_s n), \qquad n = 1, \ldots, N,$$

satisfies

$$D(N) \ll \frac{\log N \log \varphi^{-1}(N)}{\varphi^{-1}(N)},$$

where $\varphi^{-1}(t)$ is the inverse function of $\varphi(t)$.

3.3. Linear Forms in Logarithms and Linear Combinations of Frobenius Angles. We need to present a classical result of A. Baker [3] in the following greatly simplified form (see also [4, 26] for more recent achievements, which can be used to make our estimates more explicit).

Lemma 6. *For arbitrary algebraic numbers $\xi_1 \ldots, \xi_s$ there are constants $C_1 > 0$ and $C_2 > 1$ such that the inequality*

$$\begin{aligned} 0 &< |\xi_1^{k_1} \ldots \xi_s^{k_s} - 1| \\ &\le C_1 \left(\max\{|k_1|, \ldots, |k_s|\} + 1\right)^{-C_2} \end{aligned}$$

has no solution in $(k_1, \ldots, k_s) \in \mathbb{Z}^s \setminus (0, \ldots, 0)$.

We are now ready to establish a necessary result which is needed for an application of Lemma 5.

Lemma 7. *There are constants $c_1 > 0$ and $c_2 > 1$ depending only on q and g such that if $\mathcal{C}$ is a smooth projective curve of genus $g \ge 1$ over $\mathbb{F}_q$ and $\vartheta_1, \ldots, \vartheta_g$ are linearly independent modulo 1 then*

$$\|k_1\vartheta_1 + \ldots + k_g\vartheta_g\| \ge c_1 \left(\max\{|k_1|, \ldots, |k_g|\} + 1\right)^{-c_2}$$

for any non-zero vector $(k_1, \ldots, k_g) \in \mathbb{Z}^g$.

Proof. Suppose that for some integer k_0 we have

$$k_1\vartheta_1 + \ldots + k_g\vartheta_g - k_0 = \delta$$

where $\delta \in [-1/2, 1/2]$. Then, recalling (7), we derive

$$\tau_1^{2k_1} \ldots \tau_g^{2k_g} = q^{k_1 + \ldots + k_g} e^{-\pi i \delta}$$

We see that because of the linear independence of $1, \vartheta_1, \ldots, \vartheta_g$ we have $\delta > 0$. We can assume that δ is sufficiently small (as otherwise there is nothing to prove). Hence

$$0 < \left|\tau_1^{2k_1} \ldots \tau_g^{2k_g} q^{-k_1 - \ldots - k_g} - 1\right| = \left|e^{-\pi i \delta} - 1\right| = \pi\delta + O(\delta^2) \le 4\delta$$

Applying Lemma 6, we obtain the desired result with the constants c_1 and c_2 depending on $\vartheta_1, \ldots, \vartheta_g$. However, examining the zeta-function of the curve $\mathcal{C}$, see [24, Section VIII.5], we conclude for each q and g there are only finitely many possibilities for $\vartheta_1, \ldots, \vartheta_g$ thus c_1 and c_2 can be made to depend only on q and g. ☐

3.4. Concluding the Proof. We see from Lemma 7 that Lemma 5 applies to the discrepancy $\Delta(N)$ of the points (11) with $\varphi(t) = c_1(t+1)^{c_2}$, thus

$$\Delta(N) \le N^{-\kappa} \tag{12}$$

where κ depends only on $\mathcal{C}$. As we have mentioned, the domain $\mathcal{V}_g(\beta, \gamma)$ satisfies the condition of Lemma 4. Recalling (10) and combining the bound (12) with Lemmas 3 and 4, we obtain

$$T_{\beta,\gamma}(N) = N\mu\left(\mathcal{V}_g(\beta, \gamma)\right) + O\left(N^{1-\eta}\right),$$

where μ denotes the Lebesgue measure on $[0, 1]^g$. Since

$$\mu\left(\mathcal{V}_g(\beta, \gamma)\right) = \lambda_g(\beta, \gamma)$$

we conclude the proof.

4. Proof of Theorem 2

4.1. Elliptic Curves. In the case of $g = 1$ the result follows immediately from [25, Lemma 2.5]. However here we present a more general statement which maybe of independent interest.

Lemma 8. *Suppose that $\mathcal{C}$ is an ordinary smooth projective curve of genus $g \geq 1$ over $\mathbb{F}_q$. Then all Frobenius angles $\vartheta_1, \ldots, \vartheta_g$ are irrational.*

Proof. Since for every pair of conjugated Frobenius eigenvalues we have $\tau_j\overline{\tau}_j = q$, then for $j = 1, \ldots, g$ from τ_j and $\overline{\tau}_j$ at most one can be a p-adic unit. From the definition of an ordinary curve we conclude that for every $j = 1, \ldots, g$, exactly one from τ_j and $\overline{\tau}_j$, is a p-adic unit.

However, if $\vartheta_i = r/s$ is a rational Frobenius angle, then for the corresponding Frobenius eigenvalues we obtain

$$\tau_i^{2s} = \overline{\tau}_i^{2s} = q^s.$$

Thus neither of τ_i and $\overline{\tau}_i$ can be a p-adic unit. This contradiction concludes the proof. □

4.2. Curves of Genus $g = 2$. Every curve of genus 2 is either ordinary or supersingular or of p-rank 1. (equivalently the Jacobian of the curve is either ordinary or supersingular or of $K3$ type); for example, this follows from [31, n. 133, pp. 1–20]. If a curve of genus $g = 2$ is supersigular, then its Jacobian over $\overline{\mathbb{F}}_q$ is isogenous to a product of supersingular elliptic curves and cannot be absolutely simple. On the other hand, if a curve is of p-rank 1 and its Jacobian is absolutely simple, then the claim follows from a result of Yu. G. Zarhin [36]. Thus the only remaining case is the case of ordinary curves which we deal with in the following.

In fact here we establish the linear independence of ϑ_1, ϑ_2 modulo 1 for any two Frobenius angles ϑ_1, ϑ_2 (with $\vartheta_1 \neq \pm\vartheta_2$) for an ordinary smooth projective curve of arbitrary genus $g \geq 2$ which has an absolutely simple Jacobian. It is slightly more general than what we need for the proof of Theorem 2 and can be of independent interest.

First of all, we need the following property of the numerator $P_m(T)$ in (5) of the zeta-function of $\mathcal{C}$ which is a result of Honda-Tate theory for ordinary varieties (see [13, Theorem 3.3]).

Lemma 9. *If an ordinary smooth projective curve of arbitrary genus $g \geq 2$ has an absolutely simple Jacobian, then the polynomials $P_m(T)$ are irreducible over $\mathbb{Z}$ for every $m = 1, 2, \ldots$.*

We are now ready to prove our principal result.

Lemma 10. *Let $\mathcal{C}(\mathbb{F}_q)$ be an ordinary smooth projective curve of genus $g \geq 2$ which has an absolutely simple Jacobian. Then ϑ_1, ϑ_2 are linearly independent modulo 1 for any two Frobenius angles ϑ_1 and ϑ_2 .*

Proof. Suppose ϑ_1, ϑ_2 and 1 are $\mathbb{Z}$-linear dependent and for some integers u, v and w which are not zero simultaneously we have $u\vartheta_1 + v\vartheta_2 + w = 0$. We know that for an ordinary curve two of the eigenvalues corresponding to two different angles are p-adic units in $\overline{\mathbb{Q}}_p$ (see the proof of Lemma 8). If we assume that $\tau_1 = \sqrt{q}e^{\pi i\vartheta_1}$ and

$\tau_2 = \sqrt{q}e^{\pi i\vartheta_2}$ are p-adic units in $\overline{\mathbb{Q}}_p$, then from $u\vartheta_1 + v\vartheta_2 + w = 0$ it follows that

$$\tau_1^{2u}\tau_2^{2v}e^{i\pi 2w} = q^{u+v}.$$

Now since τ_1 and τ_2 are p-adic units in $\overline{\mathbb{Q}}_p$ we have $u + v = 0$. This along with $u\vartheta_1 + v\vartheta_2 + w = 0$ implies that either $u = v = 0$ or $\vartheta_1 - \vartheta_2 = w/v$. If the former case happens, then we have $w = 0$ which is a contradiction. If the latter happens, then we have $\tau_1^{2v} = \tau_2^{2v}$. This means that the numerator of the zeta-function of $\mathcal{C}(\mathbb{F}_{q^{2v}})$ has a double root and hence it splits which is a contradiction since we have assumed that the Jacobian of the curve is absolutely simple and hence the numerator of its zeta-function remains irreducible when considered over any extension of $\mathbb{F}_q$.

On the other hand if we assume that τ_1 and $\overline{\tau}_2$ are p-adic units, then from $u\vartheta_1 + v\vartheta_2 + w = 0$ it follows that

$$\tau_1^{2u}\overline{\tau}_2^{-2v}e^{i\pi 2w} = q^{u-v}.$$

Now since r_1 and $\overline{\tau}_2$ are p-adic units in $\overline{\mathbb{Q}}_p$, we have $u = v$. This along with $u\vartheta_1 + v\vartheta_2 + w = 0$ implies that either $u = v = 0$ and hence $w = 0$ or $\vartheta_1 + \vartheta_2 = -w/v$. The former is a contradiction and the latter is impossible since it would imply that $\tau_1^{2v}\tau_2^{2v} = 1$ which in turn implies that τ_2 is a p-adic unit too while this cannot happen as from τ_2 and $\overline{\tau}_2$ exactly one of them is a p-adic unit. The remaining cases can be dealt with similarly. □

5. Comments

5.1. Statistics of linear independence of Frobenius angles in families of curves. When $\mathcal{C}$ is a smooth projective ordinary curve of genus $g \geq 3$ over $\mathbb{F}_q$, then it seems to be more subtle to establish the linear independence modulo 1 of the Frobenius angles of $\mathcal{C}$. E. Kowalski [18] gives a statistical result that Frobenius angles of most algebraic curves from a certain natural family are linear independent modulo 1. One can also find in [18] examples of Abelian varieties or curves with $\mathbb{Z}$-linear dependent Frobenius angles. However, the examples given in [18] correspond to Abelian varieties which are neither ordinary nor absolutely simple. We think it is natural to conjecture that Frobenius angles of a smooth projective ordinary curve $\mathcal{C}$ whose Jacobian is absolutely simple are linearly independent modulo 1. Notice that in [14] it has been shown that most of the smooth curve are ordinary and have an absolutely simple Jacobian. A natural way to attack this conjecture would be to investigate the Galois group of the numerator $P(T)$ of the zeta-function of such curves and employ methods of [18]. Finally it is worth mentioning the following independence result from [19] attributed to B. Poonen which actually goes back to an earlier paper by M. Spieß [32]: If $\mathcal{E}_1, \ldots, \mathcal{E}_k$ are pairwise absolutely non-isogenous elliptic curves over the finite field $\mathbb{F}_q$ and τ_i is a Frobenius eigenvalue of E_i, then $\tau_1, \ldots, \tau_k$ are multiplicatively independent and hence the corresponding Frobenius angles are $\mathbb{Z}$-linearly independent. This result may be used to study joint distributions of $\#\mathcal{E}_1(\mathbb{F}_q^n), \ldots, \#\mathcal{E}_k(\mathbb{F}_q^n)$. Notice that the above result implies that if the Jacobian of a curve of genus g is isogenous to the direct product of g pairwise absolutely non-isogenous elliptic curves, then the Frobenius angles of the curve are linearly independent modulo 1. Another independence result can be found in [23].

Another "statistical" approach to linear independence modulo 1 of the Frobenius angles stems from the work of N. Chavdarov [8], which asserts that for a fixed genus $g \geq 1$, as q grows, the numerator $P(T)$ of the zeta-function $Z(T)$ of "most" curves of genus g over $\mathbb{F}_q$ is irreducible over Q, and, furthermore, the Galois group of $P(T)$ is the *Weyl group* $\mathcal{W}_g$ of the symplectic group $\mathrm{Sp}(2g)$. Now, suppose $\mathcal{C}$ be such an ordinary smooth absolutely irreducible curve of genus $g \geq 1$ defined over $\mathbb{F}_q$, (that is, the Galois group of $P(T)$ is $\mathcal{W}_g$). Assume the Frobenius angles of $\mathcal{C}$ whose Jacobian is absolutely simple are linearly dependent modulo 1, that is

$$\prod_{i=1}^{g} \tau_i^{k_i} = q^{k_0} \tag{13}$$

for some nonzero vector $(k_0, \ldots, k_g) \in \mathbb{Z}^{g+1}$. Since the the Weyl group contains a subgroup generated by transpositions of $(\tau_i, \overline{\tau_i})$, $i = 1, \ldots, g$, see the discussion in [8, Section 5], we infer that for each $i = 1, \ldots, g$, we have an automorphism $\eta_i \in \mathcal{W}_g$, which is complex conjugation on τ_i but which is the identity on any τ_j and $\overline{\tau_j}$ with $j \neq i$.

Clearly if $k_1 = \ldots = k_g = 0$ then also $k_0 = 0$. Thus without loss of generality we can assume that $k_1 \neq 0$. Applying the automorphism η_1, we obtain a new relation

$$\overline{\tau_1}^{k_1} \prod_{i=2}^{g} \tau_i^{k_i} = q^{k_0}. \tag{14}$$

From (13) and (14) we infer that

$$\overline{\tau_1}^{k_1} = \tau_1^{k_1}.$$

Multiplying both sides by $\tau_1^{k_1}$, we deduce

$$\tau_1^{2k_1} = q^{k_1}.$$

Thus $\tau_1 = q^{1/2}\rho$ for a root of unity ρ, contradicting ordinarity, (see, for example, Lemma 8).

5.2. Possible generalisations. Our method also applies to studying the distribution of the number of points on the Jacobians $J_{\mathcal{C}}(\mathbb{F}_{q^n})$ of a given curve $\mathcal{C}$ (certainly for an elliptic curve $\mathcal{C} = \mathcal{E}$ it is the same question as the question of studying $\mathcal{E}(\mathbb{F}_{q^n})$ and this is covered by Theorems 1 and 2). For example, we recall that

$$\# J_{\mathcal{C}}(\mathbb{F}_{q^n}) = \prod_{j=1}^{2g} \left(1 - \tau_j^n\right)$$

see [24, Corollary VIII.6.3].

We note that the analogue of the Sato-Tate conjecture for elliptic curves is also believed to be true for Kloosterman sums, see [1, 7, 10, 11, 12, 16, 17, 22, 27, 28, 29] for various modifications and generalizations of this conjecture and further references. However, in this case the original conjecture is still open as the result of R. Taylor [33] does not seem to apply to Kloosterman sums.

For $a \in \mathbb{F}_q^*$ we consider the Kloosterman sum

$$K_{q^n}(a) = \sum_{x \in \mathbb{F}_{q^n}^*} \psi\left(\mathrm{Tr}_{\,\mathbb{F}_{q^n}/\mathbb{F}_q}\left(x + a x^{-1}\right)\right),$$

where ψ is a fixed nonprincipal additive character of $\mathbb{F}_q$ and

$$\mathrm{Tr}_{\,\mathbb{F}_{q^n}/\mathbb{F}_q}(z) = \sum_{j=0}^{n-1} z^{q^j}$$

is the trace of $z \in \mathbb{F}_{q^n}$ in $\mathbb{F}_q$. We have

$$|K_{q^n}(a)| \le 2q^{n/2}, \qquad a \in \mathbb{F}_q^*.$$

see [15, Theorem 11.11]. Therefore, again, for a fixed $a \in \mathbb{F}_q^*$ we can define and study the sequence

$$\kappa_n = \frac{K_{q^n}(a)}{2q^{n/2}} \in [-1, 1], \qquad n = 1, 2, \ldots .$$

Since we have the analogue of (6), that is,

$$K_{q^n}(a) = \sigma^n + \overline{\sigma}^n,$$

for some complex conjugate quadratic irrationalities σ and $\overline{\sigma}$ with

$$|\sigma| = |\overline{\sigma}| = q^{1/2},$$

see [15, Section 11.7] our arguments apply to Kloosterman sums as well.

Acknowledgements

We are grateful to Nick Katz for explaining to us the argument linking linear independence modulo 1 of the Frobenius angles with the work of N. Chavdarov [8], which is presented in Section 5.1.

We would also like to thank Emmanuel Kowalski and Alexey Zaytsev for very insightful discussions and Sandro Mattarei for a very careful reading of the manuscript.

The comments and suggestions of the anonymous referee have been very helpful as well.

This paper was initiated during a very enjoyable visit of I. S. at the Department of Combinatorics & Optimization of the University of Waterloo whose hospitality, support and stimulating research atmosphere are gratefully appreciated. Research of O. A is supported by the Claude Shannon Institute, Science Foundation Ireland Grant 06/MI/006 and research of I. S. was supported by ARC grant DP0556431.

References

[1] A. Adolphson, 'On the distribution of angles of Kloosterman sums', *J. Reine Angew. Math.* **395** (1989), 214–220.

[2] S. Baier and L. Zhao, 'The Sato–Tate conjecture on average for small angles', *Trans. Amer. Math. Soc.*, **361** (2009), 1811–1832.

[3] A. Baker, A. The theory of linear forms in logarithms', *Transcendence theory: Advances and applications*, Academic Press, London-New York, 1977, 1–27.

[4] A. Baker and G. Wüstholz, *Logarithmic forms and Diophantine geometry*, Cambridge Univ. Press, Cambridge, 2007.

[5] W. D. Banks and I. E. Shparlinski, 'Sato–Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height', *Israel J. Math.* **173** (2009), 253–277.

[6] B. J. Birch, 'How the number of points of an elliptic curve over a fixed prime field varies', *J. Lond. Math. Soc.* **43** (1968), 57–60.

[7] C.-L. Chai and W.-C. W. Li, 'Character sums, automorphic forms, equidistribution, and Ramanujan graphs. I: The Kloosterman sum conjecture over function fields', *Forum Math.* **15** (2003), 679–699.

[8] N. Chavdarov, 'The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy', *Duke Math. J.*, **78** (1997), 151–180.

[9] M. Drmota and R. Tichy, *Sequences, discrepancies and applications*, Springer-Verlag, Berlin, 1997.

[10] É. Fouvry and P. Michel, 'Sommes de modules de sommes d'exponentielles', *Pacific J. Math.* **209** (2003), 261–288.

[11] É. Fouvry and P. Michel, 'Sur le changement de signe des sommes de Kloosterman', *Ann. Math.* **165** (2007), 675–715.
[12] É. Fouvry, P. Michel, J. Rivat and A. Sárközy, 'On the pseudorandomness of the signs of Kloosterman sums', *J. Aust. Math. Soc.* **77** (2004), 425–436.
[13] E. Howe, 'Principally polarized ordinary abelian varieties over finite fields', *Trans. Amer. Math. Soc.* **347** (1995), 2361–2401.
[14] E. Howe and H. J. Zhu, 'On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field', *J. Number Theory* **92** (2002), 139–163.
[15] H. Iwaniec and E. Kowalski, *Analytic number theory*, Amer. Math. Soc., Providence, RI, 2004.
[16] N. M. Katz, *Gauss sums, Kloosterman sums, and monodromy groups*, Princeton Univ. Press, Princeton, NJ, 1988.
[17] N. M. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy*, Amer. Math. Soc, Providence, RI, 1999.
[18] E. Kowalski, 'The large sieve, monodromy, and zeta functions of algebraic curves. II. Independence of the zeros', *International Mathematical Research Notices*, (2008), Art. ID rnn 091, 1–57.
[19] J. Krajicek and T. Scanlon, 'Combinatorics with definable sets: Euler characteristics and Grothendieck rings', *Bull. Symbolic Logic* **6** (2000), 311 – 330.
[20] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences*, Wiley-Interscience Publ., 1974.
[21] M. Laczkovich, 'Discrepancy estimates for sets with small boundary', *Studia Sci. Math. Hungar.*, **30** (1995), 105–109.
[22] G. Laumon, 'Exponential sums and l-adic cohomology: A survey', *Israel J. Math.* **120** (2000), 225–257.
[23] H. W. Lenstra, Jr and Yu. G. Zarhin, 'The Tate conjecture for almost ordinary Abelian varieties over finite fields', *Advances in number theory, Proc. 3rd Conference of the Canadian Number Theory Association*, Oxford Univ. Press, 1993, 179–194.
[24] D. Lorenzini, *An invitation to arithmetic geometry*, Amer. Math. Soc., 1996.
[25] F. Luca and I. E. Shparlinski, 'On the exponent of the group of points on elliptic curves in extension fields', *Intern. Math. Research Notices*, **2005** (2005), 1391–1409.
[26] E. M. Matveev, 'An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II', *Izv. Ross. Akad. Nauk Ser. Mat.*, **64** (2000), no. 6, 125–180 (in Russian); translation in *Izv. Math.*, **64** (2000), 1217–1269.
[27] P. Michel, 'Autour de la conjecture de Sato-Tate pour les sommes de Kloosterman, II', *Duke Math. J.* **92** (1998), 221–254.
[28] P. Michel, 'Minoration de sommes d'exponentielles', *Duke Math. J.* **95** (1998), 227–240.
[29] H. Niederreiter, 'The distribution of values of Kloosterman sums', *Arch. Math.* **56** (1991), 270–277.
[30] H. Niederreiter and J. M. Wills, 'Diskrepanz und Distanz von Massen bezuglich konvexer und Jordanscher Mengen', *Math. Z.*, **144** (1975), 125–134.
[31] J.-P. Serre, 'Œuvres, IV, 1985–1998'. Springer-Verlag, Berlin, 2000.
[32] M. Spieß, 'Proof of the Tate conjecture for products of elliptic curves over finite fields.', *Math. Ann.*, **314** (1999), 285–290.
[33] R. Taylor, 'Automorphy for some l-adic lifts of automorphic mod l representations, II', *Pub. Math. IHES*, **108** (2008), 183–239.
[34] H. Weyl, 'On the volume of tubes', *Amer. J. Math.* **61**, (1939), 461–472.
[35] H. Yoshida, 'On an analogue of the Sato conjecture', *Inventiones Math.*, **19** (1973), 261–277.
[36] Yu. G. Zarhin, 'Abelian varieties of $K3$ type', *Séminaire de Théorie des Nombres*, Paris, 1990–91, Progr. Math. **108**, Birkhäuser, (1993), 263–279.

Claude Shannon Institute, University College Dublin, Dublin 4, Ireland
E-mail address: omran.ahmadi@ucd.ie

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: igor@ics.mq.edu.au