Analytic Number Theory in Function Fields (Lecture 6)

Julio Andrade

j.c.andrade.math@gmail.com
http://julioandrade.weebly.com/

University of Oxford

TCC Graduate Course
University of Oxford, Oxford
01 May 2015 - 11 June 2015

Content

Introduction

- The zeta function of a curve over a finite field may be expressed in terms of the characteristic polynomial of a unitary symplectic matrix Θ, called the Frobenius class of the curve.
- We will compute the expected value of $\mathrm{tr}(\Theta^n)$ for an ensemble of hyperelliptic curves of genus g over a fixed finite field in the limit of large genus, and compare the results to the corresponding averages over the unitary symplectic group $\mathrm{USp}(2g)$.
- We are able to compute the averages for powers n almost up to $4g$, finding agreement with the Random Matrix results except for small n and for $n = 2g$.
- As an application we compute the one-level density of zeros of the zeta function of the curves, including lower-order terms, for test functions whose Fourier transform is supported in $(-2, 2)$.
- The results confirm in part a conjecture of Katz and Sarnak, that to leading order the low-lying zeros for this ensemble have symplectic statistics.

Background Material

Fix a finite field $\mathbb{F}_q$ of odd cardinality, and let C be a non singular projective curve defined over $\mathbb{F}_q$. For each extension field of degree n of $\mathbb{F}_q$, denote by $N_n(C)$ the number of points of C in $\mathbb{F}_{q^n}$. The zeta function associated to C is defined as

$$Z_C(u) = \exp \sum_{n=1}^{\infty} N_n(C) \frac{u^n}{n}, \quad |u| < 1/q$$

and is known to be a rational function of u of the form

$$Z_C(u) = \frac{P_C(u)}{(1-u)(1-qu)} \tag{1.1}$$

where $P_C(u)$ is a polynomial of degree $2g$ with integer coefficients, satisfying a functional equation

$$P_C(u) = (qu^2)^g P_C(\frac{1}{qu}) \ .$$

The Riemann Hypothesis, proved by Weil, is that the zeros of $P(u)$ all lie on the circle $|u| = 1/\sqrt{q}$. Thus one may give a spectral interpretation of $P_C(u)$ as the characteristic polynomial of a $2g \times 2g$ unitary matrix Θ_C

$$P_C(u) = \det(I - u\sqrt{q}\Theta_C)$$

so that the eigenvalues $e^{i\theta_j}$ of Θ_C correspond to zeros $q^{-1/2}e^{-i\theta_j}$ of $Z_C(u)$.

The matrix (or rather the conjugacy class) Θ_C is called the unitarized Frobenius class of C.

We would like to study the how the Frobenius classes Θ_C change as we vary the curve over a family of hyperelliptic curves of genus g, in the limit of large genus and fixed constant field. The particular family $\mathcal{H}_{2g+1}$ we choose is the family of all curves given in affine form by an equation

$$C_Q : y^2 = Q(x)$$

where

$$Q(x) = x^{2g+1} + a_{2g} + \cdots + a_0 \in \mathbb{F}_q[x]$$

is a squarefree, monic polynomial of degree $2g+1$. The curve C_Q is thus nonsingular and of genus g.

We consider $\mathcal{H}_{2g+1}$ as a probability space (ensemble) with the uniform probability measure, so that the expected value of any function F on $\mathcal{H}_{2g+1}$ is defined as

$$\langle F \rangle := \frac{1}{\#\mathcal{H}_{2g+1}} \sum_{Q \in \mathcal{H}_{2g+1}} F(Q)$$

Katz and Sarnak showed that as $q \to \infty$, the Frobenius classes Θ_Q become equidistributed in the unitary symplectic group $\mathrm{USp}(2g)$ (in genus one this is due to Birch for q prime, and to Deligne). That is for any continuous function on the space of conjugacy classes of $\mathrm{USp}(2g)$,

$$\lim_{q\to\infty} \langle F(\Theta_Q)\rangle = \int_{\mathrm{USp}(2g)} F(U)dU$$

This implies that various statistics of the eigenvalues can, in this limit, be computed by integrating the corresponding quantities over $\mathrm{USp}(2g)$.

Our goal is to explore the opposite limit, that of fixed constant field and large genus (q fixed, $g \to \infty$). Since the matrices Θ_Q now inhabit different spaces as g grows, it is not clear how to formulate an equidistribution problem. However one can still meaningfully discuss various statistics, the most fundamental being various products of traces of powers of Θ_Q, that is $\left\langle \prod_{j=1}^{r} \mathrm{tr}(\Theta_Q^{n_j}) \right\rangle$. Here we study the basic case of the expected values $\langle \mathrm{tr}\, \Theta_Q^n \rangle$ where n is of order of the genus g.

The mean value of traces of powers when averaged over the unitary symplectic group $\mathrm{USp}(2g)$ are known to be

$$\int_{\mathrm{USp}(2g)} \mathrm{tr}(U^n)dU = \begin{cases} 2g & n=0 \\ -\eta_n & 1 \leq |n| \leq 2g \\ 0 & |n| > 2g \end{cases} \tag{1.2}$$

where

$$\eta_n = \begin{cases} 1 & n \text{ even} \\ 0 & n \text{ odd} \end{cases}$$

We will show:

Theorem

For all $n > 0$ we have

$$\langle \operatorname{tr} \Theta_Q^n \rangle = \begin{Bmatrix} -\eta_n, & 0 < n < 2g \\ -1 - \frac{1}{q-1}, & n = 2g \\ 0, & n > 2g \end{Bmatrix} + \eta_n \frac{1}{q^{n/2}} \sum_{\substack{\deg P | \frac{n}{2} \\ P \text{ prime}}} \frac{\deg P}{|P|+1}$$
$$+ O_q\left(nq^{n/2-2g} + gq^{-g}\right)$$

the sum over all irreducible monic polynomials P, and where $|P| := q^{\deg P}$.

In particular we have

Corollary

If $3\log_q g < n < 4g - 5\log_q g$ but $n \neq 2g$ then

$$\langle \operatorname{tr} \Theta_Q^n \rangle = \int_{\mathrm{USp}(2g)} \operatorname{tr} U^n dU + o(\frac{1}{g}) \ .$$

We do however get deviations from the Random Matrix Theory results (2.2) for small values of n, for instance

$$\left\langle \operatorname{tr} \Theta_Q^2 \right\rangle \sim \int_{\mathrm{USp}(2g)} \operatorname{tr} U^2 \, dU + \frac{1}{q+1}$$

and for $n = 2g$ where we have

$$\left\langle \operatorname{tr} \Theta_Q^{2g} \right\rangle \sim \int_{\mathrm{USp}(2g)} \operatorname{tr} U^{2g} \, dU - \frac{1}{q-1} \; .$$

Analogous results can be derived for mean values of products, e.g. for $\langle \operatorname{tr} \Theta_Q^m \operatorname{tr} \Theta_Q^n \rangle$, when $m + n < 4g$.

To prove these results, we cannot use the powerful equidistribution theorem of Deligne. Rather, we use a variant of the analytic methods developed to deal with such problems in the number field setting. Extending the range of this results to cover $n > 4g$ is a challenge.

The traces of powers determine all *linear* statistics, such as the number of angles θ_j lying in a subinterval of $\mathbb{R}/2\pi\mathbb{Z}$, or the one-level density, a smooth linear statistic. To define the one-level density, we start with an even test function f, say in the Schwartz space $\mathcal{S}(\mathbb{R})$, and for any $N \geq 1$ set

$$F(\theta) := \sum_{k\in\mathbb{Z}} f(N(\frac{\theta}{2\pi} - k))$$

which has period 2π and is localized in an interval of size $\approx 1/N$ in $\mathbb{R}/2\pi\mathbb{Z}$. For a unitary $N \times N$ matrix U with eigenvalues $e^{i\theta_j}$, $j = 1, \ldots N$, define

$$Z_f(U) := \sum_{j=1}^{N} F(\theta_j)$$

which counts the number of "low-lying" eigenphases θ_j in the smooth interval of length $\approx 1/N$ around the origin defined by f.

Katz and Sarnak conjectured that for fixed q, the expected value of Z_f over $\mathcal{H}_{2g+1}$ will converge to $\int_{\mathrm{USp}(2g)} Z_f(U)dU$ as $g \to \infty$ for *any* such test function f. Theorem 1 implies:

Corollary

If $f \in \mathcal{S}(\mathbb{R})$ is even, with Fourier transform $\widehat{f}$ supported in $(-2,2)$ then

$$\langle Z_f \rangle = \int_{\mathrm{USp}(2g)} Z_f(U)dU + \frac{dev(f)}{g} + o(\frac{1}{g})$$

where

$$dev(f) = \widehat{f}(0) \sum_{P \ prime} \frac{\deg P}{|P|^2 - 1} - \widehat{f}(1)\frac{1}{q-1}$$

the sum over all irreducible monic polynomials P.

To show corollary 3, one uses a Fourier expansion to see that

$$Z_f(U) = \int_{-\infty}^{\infty} f(x)dx + \frac{1}{N}\sum_{n\neq 0}\widehat{f}(\frac{n}{N})\,\mathrm{tr}\,U^n\,. \tag{2.1}$$

Averaging $Z_f(U)$ over the symplectic group USp$(2g)$, using (2.2), and assuming f is even, gives

$$\int_{\mathrm{USp}(2g)} Z_f(U)dU = \widehat{f}(0) - \frac{1}{g}\sum_{1\leq m\leq g}\widehat{f}(\frac{m}{g})$$

and then we use Theorem 1 to deduce Corollary 3.
Note that as $g\to\infty$, $\int_{\mathrm{USp}(2g)} Z_f(U)dU \sim \int_{-\infty}^{\infty} f(x)\left(1-\frac{\sin 2\pi x}{2\pi x}\right)dx$
Corollary 3 is completely analogous to what is known in the number field setting for the corresponding case of zeta functions of quadratic fields, except for the lower order term which is different: While the coefficient of $\widehat{f}(0)$ is as in the number field setting, the coefficient of $\widehat{f}(1)$ is special to our function-field setting.

In this section we give some known background on the zeta function of hyperelliptic curves.
For a nonzero polynomial $f \in \mathbb{F}_q[x]$, we define the norm $|f| := q^{\deg f}$. A "prime" polynomial is a monic irreducible polynomial. For a monic polynomial f, The von Mangoldt function $\Lambda(f)$ is defined to be zero unless $f = P^k$ is a prime power in which case $\Lambda(P^k) = \deg P$.
The analogue of Riemann's zeta function is

$$\zeta_q(s) := \prod_{P \text{ prime}} (1 - |P|^{-s})^{-1}$$

which is shown to equal

$$\zeta_q(s) = \frac{1}{1 - q^{1-s}} \tag{3.1}$$

Let $\pi_q(n)$ be the number of prime polynomials of degree n. The Prime Polynomial Theorem in $\mathbb{F}_q[x]$ asserts that

$$\pi_q(n) = \frac{q^n}{n} + O(q^{n/2})$$

which follows from the identity (equivalent to (4.1))

$$\sum_{\deg(f)=n} \Lambda(f) = q^n \tag{3.2}$$

the sum over all monic polynomials of degree n.

For a monic polynomial $D \in \mathbb{F}_q[x]$ of positive degree, which is not a perfect square, we define the quadratic character χ_D in terms of the quadratic residue symbol for $\mathbb{F}_q[x]$ by

$$\chi_D(f) = \left(\frac{D}{f}\right)$$

and the corresponding L-function

$$\mathcal{L}(u, \chi_D) := \prod_P (1 - \chi_D(P) u^{\deg P})^{-1}, \quad |u| < \frac{1}{q}$$

the product over all monic irreducible (prime) polynomials P. Expanding in additive form using unique factorization, we write

$$\mathcal{L}(u, \chi_D) = \sum_{\beta \geq 0} A_D(\beta) u^\beta$$

with

$$A_D(\beta) := \sum_{\substack{\deg B = \beta \\ B \text{ monic}}} \chi_D(B) \, .$$

If D is non-square of positive degree, then $A_D(\beta) = 0$ for $\beta \geq \deg D$ and hence the L-function is in fact a polynomial of degree at most $\deg D - 1$.

To proceed further, assume that D is square-free (and monic of positive degree). Then $\mathcal{L}(u,\chi_D)$ has a "trivial" zero at $u=1$ if and only if $\deg D$ is even. Thus

$$\mathcal{L}(u,\chi_D) = (1-u)^{\lambda}\mathcal{L}^*(u,\chi_D), \quad \lambda = \begin{cases} 1 & \deg D \text{ even} \\ 0 & \deg(D) \text{ odd} \end{cases}$$

where $\mathcal{L}^*(u,\chi_D)$ is a polynomial of even degree

$$2\delta = \deg D - 1 - \lambda$$

satisfying the functional equation

$$\mathcal{L}^*(u,\chi_D) = (qu^2)^{\delta}\mathcal{L}^*(\frac{1}{qu},\chi_D)\ .$$

In fact $\mathcal{L}^*(u,\chi_D)$ is the Artin L-function associated to the unique nontrivial quadratic character of $\mathbb{F}_q(x)(\sqrt{D(x)})$. We write

$$\mathcal{L}^*(u,\chi_D) = \sum_{\beta=0}^{2\delta} A_D^*(\beta) u^\beta$$

where $A_D^*(0) = 1$, and the coefficients $A_D^*(\beta)$ satisfy

$$A_D^*(\beta) = q^{\beta-\delta} A_D^*(2\delta - \beta)\ . \tag{3.3}$$

In particular the leading coefficient is $A_D^*(2\delta) = q^\delta$.

For D monic, square-free, and of positive degree, the zeta function (2.1) of the hyperelliptic curve $y^2 = D(x)$ is

$$Z_D(u) = \frac{\mathcal{L}^*(u, \chi_D)}{(1-u)(1-qu)} .$$

The Riemann Hypothesis, proved by Weil, asserts that all zeros of $Z_C(u)$, hence of $\mathcal{L}^*(u, \chi_D)$, lie on the circle $|u| = 1/\sqrt{q}$. Thus we may write

$$\mathcal{L}^*(u, \chi_D) = \det(I - u\sqrt{q}\Theta_D)$$

for a unitary $2\delta \times 2\delta$ matrix Θ_D.

By taking a logarithmic derivative of the identity

$$\det(I - u\sqrt{q}\Theta_D) = (1-u)^{-\lambda} \prod_P (1 - \chi_D(P) u^{\deg P})^{-1}$$

which comes from writing $\mathcal{L}^*(u, \chi_D) = (1-u)^{-\lambda} \mathcal{L}(u, \chi_D)$, we find

$$-\operatorname{tr}\Theta_D^n = \frac{\lambda}{q^{n/2}} + \frac{1}{q^{n/2}} \sum_{\deg f = n} \Lambda(f) \chi_D(f) \tag{3.4}$$

Assume now that B is monic, of positive degree and not a perfect square. Then we have a bound for the character sum over primes:

$$\left| \sum_{\substack{\deg P=n \\ P \text{ prime}}} \left(\frac{B}{P}\right) \right| \ll \frac{\deg B}{n} q^{n/2} \tag{3.5}$$

This is deduced by writing $B = DC^2$ with D square-free, of positive degree, and then using the explicit formula (4.4) and the unitarity of Θ_D (which is the Riemann Hypothesis).

We denote by $\mathcal{H}_d$ the set of square-free monic polynomials of degree d in $\mathbb{F}_q[x]$. The cardinality of $\mathcal{H}_d$ is

$$\#\mathcal{H}_d = \begin{cases} (1-\frac{1}{q})q^d, & d \geq 2 \\ q, & d = 1 \end{cases}$$

as is seen by writing

$$\sum_{d\geq 0} \frac{\#\mathcal{H}_d}{q^{ds}} = \sum_{f \text{ monic squarefree}} |f|^{-s} = \frac{\zeta_q(s)}{\zeta_q(2s)}$$

and using (4.1). In particular for $g \geq 1$,

$$\#\mathcal{H}_{2g+1} = (q-1)q^{2g} \ .$$

We consider $\mathcal{H}_{2g+1}$ as a probability space (ensemble) with the uniform probability measure, so that the expected value of any function F on $\mathcal{H}_{2g+1}$ is defined as

$$\langle F \rangle := \frac{1}{\#\mathcal{H}_{2g+1}} \sum_{Q \in \mathcal{H}_{2g+1}} F(Q) \tag{4.1}$$

We can pick out square-free polynomials by using the Möbius function μ of $\mathbb{F}_q[x]$ (as is done over the integers) via

$$\sum_{A^2 | Q} \mu(A) = \begin{cases} 1 & Q \text{ square-free} \\ 0 & \text{otherwise} \end{cases}$$

Thus we may write expected values as

$$\langle F(Q) \rangle = \frac{1}{(q-1)q^{2g}} \sum_{2\alpha+\beta=2g+1} \sum_{\deg B=\beta} \sum_{\deg A=\alpha} \mu(A) F(A^2 B) \tag{4.2}$$

the sum over all monic A, B.

Suppose now that we are given a polynomial $f \in \mathbb{F}_q[x]$ and apply (5.2) to the quadratic character $\chi_Q(f) = \left(\frac{Q}{f}\right)$. Then

$$\chi_{A^2B}(f) = \left(\frac{B}{f}\right)\left(\frac{A}{f}\right)^2 = \begin{cases} \left(\frac{B}{f}\right) & \gcd(A, f) = 1 \\ 0 & \text{otherwise} \end{cases}$$

Hence

$$\langle \chi_Q(f) \rangle = \frac{1}{(q-1)q^{2g}} \sum_{2\alpha+\beta=2g+1} \sigma(f;\alpha) \sum_{\deg B=\beta} \left(\frac{B}{f}\right)$$

where

$$\sigma(f;\alpha) := \sum_{\substack{\deg A=\alpha \\ \gcd(A,f)=1}} \mu(A) \, .$$

Suppose P is a prime of degree n, $k \geq 1$ and $\alpha \geq 0$. Set

$$\sigma_n(\alpha) := \sigma(P^k;\alpha) = \sum_{\substack{\deg A = \alpha \\ \gcd(A, P^k)=1}} \mu(A) .$$

Since the conditions $\gcd(A, P^k) = 1$ and $\gcd(A, P) = 1$ are equivalent for a prime P and any $k \geq 1$, this quantity is independent of k; the notation anticipates that it depends only on the degree n of P, as is shown in:

Lemma

i) For $n = 1$,

$$\sigma_1(0) = 1, \quad \sigma_1(\alpha) = 1 - q \text{ for all } \alpha \geq 1 .$$

ii) If $n \geq 2$ then

$$\sigma_n(\alpha) = \begin{cases} 1 & \alpha = 0 \mod n \\ -q & \alpha = 1 \mod n \\ 0 & \text{otherwise} \end{cases} .$$

Proof.

Since P is prime,

$$\sigma_n(\alpha) = \sum_{\substack{\deg A=\alpha \\ P|A}} \mu(A) - \sum_{\substack{\deg A=\alpha\\ P|A}} \mu(A) = \sum_{\deg A=\alpha} \mu(A) - \sum_{\deg A_1=\alpha-n} \mu(PA_1) .$$

Now $\mu(PA_1) \neq 0$ only when A_1 is coprime to P, in which case $\mu(PA_1) = \mu(P)\mu(A_1) = -\mu(A_1)$. Hence

$$\sigma_n(\alpha) = \sum_{\deg A=\alpha} \mu(A) + \sum_{\substack{\deg A_1=\alpha-n\\ (P,A_1)=1}} \mu(A_1) ,$$

that is

$$\sigma_n(\alpha) - \sigma_n(\alpha-n) = \sum_{\deg A=\alpha} \mu(A) = \begin{cases} 1 & \alpha=0 \\ -q & \alpha=1 \\ 0 & \alpha\geq 2 \end{cases}$$

on using

$$\sum_{A \text{ monic}} \frac{\mu(A)}{|A|^s} = \frac{1}{\zeta_q(s)} = 1-q^{1-s}$$

and (4.1). For $n \geq 2$ we get (ii) while for $n=1$ we find that $\sigma_1(0) = 1$ and for $\alpha \geq 1$,

$$\sigma_1(\alpha) = \sigma_1(\alpha-1) = \cdots = \sigma_1(1) = -q.$$

Lemma

Let P be a prime. Then

$$\left\langle \chi_Q(P^2) \right\rangle = \frac{|P|}{|P|+1} + O(q^{-2g}) \; .$$

Proof of Lemma

Since P is prime, $\chi_Q(P^2) = 1$ unless P divides Q, that is setting

$$\iota_P(f) := \begin{cases} 1, & P \nmid f \\ 0, & P \mid f \end{cases}$$

we have $\chi_Q(P^2) = \iota_P(Q)$ and thus by (5.2)

$$\left\langle \chi_Q(P^2) \right\rangle = \langle \iota_P \rangle = \frac{1}{(q-1)q^{2g}} \sum_{\deg A^2 B = 2g+1} \mu(A) \iota_P(A^2 B) \, .$$

Since P is prime, $P \nmid A^2 B$ if and only if $P \nmid A$ and $P \nmid B$. Hence

$$\left\langle \chi_Q(P^2) \right\rangle = \frac{1}{(q-1)q^{2g}} \sum_{0 \le \alpha \le g} \sum_{\deg A = \alpha, P \nmid A} \mu(A) \sum_{\deg B = 2g+1-2\alpha, P \nmid B} 1 \, .$$

Continuation of the Proof

Writing $m := \deg P$,

$$\#\{B : \deg B = \beta \quad P \nmid B\} = q^{\beta} \cdot \begin{cases} 1, & \text{if } m > \beta \\ 1 - \frac{1}{|P|}, & \text{if } m \leq \beta \end{cases}$$

and

$$\sum_{\deg A = \alpha, P \nmid A} \mu(A) = \sigma_m(\alpha)$$

is computed in Lemma 4. Hence

$$\langle \chi_Q(P^2) \rangle = \frac{1}{(q-1)q^{2g}} \sum_{0 \leq \alpha \leq g} \sigma_m(\alpha) q^{2g+1-2\alpha} \cdot \begin{cases} 1 - \frac{1}{|P|}, & 0 \leq \alpha \leq g - \frac{m-1}{2} \\ 1, & g - \frac{m-1}{2} < \alpha \leq g \end{cases}$$

$$= (1 - \frac{1}{|P|}) \frac{1}{1 - \frac{1}{q}} \left(\sum_{\alpha=0}^{\infty} \frac{\sigma_m(\alpha)}{q^{2\alpha}} + O(q^{-2g}) \right) .$$

Continuation of the Proof

Moreover, inserting the values of $\sigma_m(\alpha)$ given by Lemma 4 gives

$$\sum_{\alpha=0}^{\infty} \frac{\sigma_m(\alpha)}{q^{2\alpha}} = \frac{1-\frac{1}{q}}{1-\frac{1}{|P|^2}}$$

(this is valid both for $m = 1$ and $m \geq 2$!) and hence

$$\left\langle \chi_Q(P^2) \right\rangle = (1 - \frac{1}{|P|}) \frac{1}{1-\frac{1}{q}} \frac{1-\frac{1}{q}}{1-\frac{1}{|P|^2}} + O(q^{-2g}) = \frac{|P|}{|P|+1} + O(q^{-2g})$$

as claimed.

We consider the double character sum

$$S(\beta;n) := \sum_{\substack{\deg P = n \\ P \text{ prime}}} \sum_{\substack{\deg B = \beta \\ B \text{ monic}}} \left(\frac{B}{P}\right) .$$

We may express $S(\beta, n)$ in terms of the coefficients $A_P(\beta) = \sum_{\deg B=\beta} \chi_P(B)$ of the L-function $\mathcal{L}(u, \chi_P) = \sum_\beta A_P(\beta) u^\beta$:

$$S(\beta;n) = (-1)^{\frac{q-1}{2}\beta n} \sum_{\deg P=n} A_P(\beta) ,$$

which follows from the law of quadratic reciprocity: If A, B are monic then

$$\left(\frac{B}{P}\right) = (-1)^{\frac{q-1}{2}\deg P \deg B} \left(\frac{P}{B}\right) = (-1)^{\frac{q-1}{2}\deg P \deg B} \chi_P(B) .$$

Since $A_P(\beta) = 0$ for $\beta \geq \deg P$, we find:

Lemma

For $n \leq \beta$ *we have*

$$S(\beta; n) = 0 \; .$$

Proposition

i) If n is odd and $0 \leq \beta \leq n-1$ then

$$S(\beta; n) = q^{\beta - \frac{n-1}{2}} S(n-1-\beta; n) \tag{5.1}$$

and

$$S(n-1; n) = \pi_q(n) q^{\frac{n-1}{2}}, \quad n \text{ odd}. \tag{5.2}$$

ii) If n is even and $1 \leq \beta \leq n-2$ then

$$S(\beta; n) = q^{\beta - \frac{n}{2}} \left(-S(n-1-\beta; n) + (q-1) \sum_{j=0}^{n-\beta-2} S(j; n) \right) \tag{5.3}$$

and

$$S(n-1; n) = -\pi_q(n) q^{\frac{n-2}{2}}, \quad n \text{ even}. \tag{5.4}$$

Proof of Proposition

Assume that $n = \deg P$ is odd. Then $\mathcal{L}(u, \chi_P) = \mathcal{L}^*(u, \chi_P)$, and so the coefficients $A_P(\beta) = A_P^*(\beta)$ coincide. Therefore the functional equation in the form (4.3) implies

$$A_P(\beta) = A_P(n-1-\beta) q^{\beta - \frac{n-1}{2}}, \quad n \text{ odd}, \quad 0 \le \beta \le n-1 .$$

Consequently we find that for n odd,

$$S(\beta; n) = q^{\beta - \frac{n-1}{2}} S(n-1-\beta; n), \quad n \text{ odd}, \quad 0 \le \beta \le n-1 .$$

In particular we have

$$S(n-1; n) = q^{\frac{n-1}{2}} S(0, n) = q^{\frac{n-1}{2}} \pi_q(n), \quad n \text{ odd} .$$

Continuation of the Proof

Next, assume that $n = \deg P$ is even. Then $\mathcal{L}(u, \chi_P) = (1-u)\mathcal{L}^*(u, \chi_P)$, which implies that the coefficients of $\mathcal{L}(u, \chi_P)$ and $\mathcal{L}^*(u, \chi_P)$ satisfy

$$A_P(\beta) = A_P^*(\beta) - A_P^*(\beta - 1), \qquad \beta \geq 1$$

and

$$A_P^*(\beta) = A_P(\beta) + A_P(\beta - 1) + \cdots + A_P(0) \,. \tag{5.5}$$

Moreover

$$A_P(0) = A_P^*(0), \quad A_P(n-1) = -A_P^*(n-2) \,.$$

In particular, since

$$A_P^*(0) = 1, \quad A_P^*(n-2) = q^{\frac{n-2}{2}}$$

(see (4.3)) we get

$$A_P(n-1) = -A_P^*(n-2) = -q^{\frac{n-2}{2}}, \quad n \text{ even}$$

so that

$$S(n-1; n) = -\pi_q(n) q^{\frac{n-2}{2}}, \quad n \text{ even} \,.$$

Continuation of the Proof

The functional equation (4.3) implies

$$A_P^*(\beta) = A_P^*(n-2-\beta)q^{\beta-\frac{n-2}{2}}, \quad 0 \le \beta \le n-2$$

and hence for $1 \le \beta \le n-2$

$$A_P(\beta) = A_P^*(\beta) - A_P^*(\beta-1) = A_P^*(n-2-\beta)q^{\beta-\frac{n-2}{2}} - A_P^*(n-1-\beta)q^{\beta-\frac{n}{2}}$$

and inserting (6.5) gives

$$A_P(\beta) = q^{\beta-\frac{n}{2}}\left(-A_P(n-1-\beta) + (q-1)\sum_{j=0}^{n-\beta-2} A_P(j)\right) .$$

Summing over all primes P of degree n gives

$$S(\beta;n) = q^{\beta-\frac{n}{2}}\left(-S(n-1-\beta;n) + (q-1)\sum_{j=0}^{n-\beta-2} S(j;n)\right)$$

as claimed.

Lemma

Suppose $\beta < n$. *Then*

$$S(\beta; n) = \eta_\beta \pi_q(n) q^{\frac{\beta}{2}} + O(\frac{\beta}{n} q^{\frac{n}{2}+\beta}) \tag{5.6}$$

where $\eta_\beta = 1$ *for* β *even, and* $\eta_\beta = 0$ *for* β *odd.*

Proof of Lemma

We write

$$S(\beta; n) = \sum_{\substack{B=\square \\ \deg B=\beta}} \sum_{\deg P=n} \left(\frac{B}{P}\right) + \sum_{\substack{B\neq\square \\ \deg B=\beta}} \sum_{\deg P=n} \left(\frac{B}{P}\right)$$

where the squares only occur when β is even.
For B not a perfect square, we use the Riemann Hypothesis for curves in the form (4.5):

$$\sum_{\deg P=n} \left(\frac{B}{P}\right) \ll \frac{\deg B}{n} q^{n/2} .$$

Continuation of the Proof

Hence summing over all nonsquare B of degree β, of which there are at most q^{β}, gives

$$\sum_{\substack{B \neq \square \\ \deg B = \beta}} \sum_{\deg P = n} \left(\frac{B}{P}\right) \ll \frac{\beta}{n} q^{\beta + \frac{n}{2}} .$$

Assume now that β is even. For $B = C^2$, we have P and B are coprime since $\deg C = \beta/2 < n = \deg P$, and hence $\left(\frac{B}{P}\right) = \left(\frac{C^2}{P}\right) = +1$ and so the squares, of which there are $q^{\beta/2}$, contribute $\pi_q(n) q^{\beta/2}$. This proves (6.6).

By using duality, (6.6) can be bootstrapped into an improved estimate when β is odd:

Proposition

If β is odd and $\beta < n$ then

$$S(\beta; n) = -\eta_n \pi_q(n) q^{\beta - \frac{n}{2}} + O(q^n) \ . \qquad (5.7)$$

Proof of Proposition

Assume n odd with $\beta < n$. Then by (6.1) for odd n,

$$S(\beta; n) = q^{\beta - \frac{n-1}{2}} S(n-1-\beta; n)$$

and inserting the inequality (6.6) with β replaced by $n-1-\beta$ (which is odd in this case) we get

$$S(n-1-\beta; n) \ll q^{\frac{n}{2}+(n-1-\beta)}$$

hence

$$S(\beta; n) \ll q^{\beta - \frac{n-1}{2}} q^{\frac{n}{2}+(n-1-\beta)} \ll q^n$$

as claimed.

Proof of Proposition

Assume n even, with $\beta < n$. Using (6.3) and the bound (6.6) gives

$$S(\beta; n) = q^{\beta - \frac{n}{2}} \left(-S(n-1-\beta; n) + (q-1) \sum_{j=0}^{n-\beta-2} S(j; n) \right)$$

$$= q^{\beta - \frac{n}{2}} \left(-\eta_{n-1-\beta} \pi_q(n) q^{\frac{n-1-\beta}{2}} + (q-1) \sum_{j=0}^{n-\beta-2} \eta_j \pi_q(n) q^{\frac{j}{2}} \right)$$

$$+ O\left(q^{\beta - \frac{n}{2}} \sum_{j=0}^{n-1-\beta} \frac{j}{n} q^{\frac{n}{2}+j} \right) .$$

Continuation of the Proof

The remainder term is $O(q^n)$. For the main term, we note that $n - 1 - \beta = 2L$ is even since β is odd and n is even, and then we can write the sum as

$$q^{\beta - \frac{n}{2}} \pi_q(n) \left(-q^L + (q-1) \sum_{l=0}^{L-1} q^l \right) = -q^{\beta - \frac{n}{2}} \pi_q(n)$$

which is our claim.

The explicit formula (4.4) says that for $n > 0$,

$$\operatorname{tr}\Theta_Q^n = -\frac{1}{q^{n/2}} \sum_{\deg f = n} \Lambda(f)\chi_Q(f)$$

the sum over all monic primes powers. We will separately treat the contributions $\mathcal{P}_n$ of primes, $\square_n$ of squares and $\mathbb{H}_n$ of higher odd powers of primes:

$$\operatorname{tr}\Theta_Q^n = \mathcal{P}_n + \square_n + \mathbb{H}_n \ . \tag{6.1}$$

When n is even, we have a contribution to $\operatorname{tr}\Theta_Q^n$ coming from squares of prime powers (for odd n this term does not appear), which give

$$\square_n = -\frac{1}{q^{n/2}} \sum_{\deg h = \frac{n}{2}} \Lambda(h)\chi_Q(h^2) \; .$$

Since $\chi_Q(h^2) = 0$ or 1, we clearly have $\square_n \leq 0$ and

$$\square_n \geq -\frac{1}{q^{n/2}} \sum_{\deg h = \frac{n}{2}} \Lambda(h) = -1 \; .$$

by (4.2). Hence the contribution of squares is certainly bounded.

Now for $h = P^k$ a prime power,

$$\left\langle \chi_Q(h^2) \right\rangle = \left\langle \chi_Q(P^2) \right\rangle = 1 - \frac{1}{|P|+1} + O(q^{-2g}) \,. \tag{6.2}$$

by Lemma 5. Thus, recalling that $\sum_{\deg h = m} \Lambda(h) = q^m$ (4.2), the contribution of squares to the average is

$$\begin{aligned} \langle \square_n \rangle &= -1 + \frac{1}{q^{n/2}} \sum_{\deg P | \frac{n}{2}} \left(\deg(P) \frac{1}{|P|+1} + O(q^{-2g}) \right) \\ &= -1 + \frac{1}{q^{n/2}} \sum_{\deg P | \frac{n}{2}} \frac{\deg(P)}{|P|+1} + O(q^{-2g}) \,. \end{aligned} \tag{6.3}$$

In particular, we find that the contribution of squares to the average is

$$\langle \square_n \rangle = -1 + O(\frac{n}{q^{n/2}}) + O(q^{-2g})$$

and thus if $n \gg 3 \log_q g$ we get

$$\langle \square_n \rangle = -\eta_n (1 + o(\frac{1}{g})) \ .$$

The contribution to $\operatorname{tr}\Theta_Q^n$ of primes is

$$\mathcal{P}_n = -\frac{n}{q^{n/2}} \sum_{\deg P = n} \chi_Q(P) \ .$$

Proposition

$$\langle \mathcal{P}_n \rangle = -\frac{n}{(q-1)q^{2g+n/2}} \sum_{\substack{\beta+2\alpha=2g+1 \\ \alpha,\beta\geq 0}} \sigma_n(\alpha) S(\beta; n) \ . \tag{6.4}$$

Moreover, if $n > g$ then

$$\langle \mathcal{P}_n \rangle = -\frac{n}{(q-1)q^{2g+n/2}} \left(S(2g+1; n) - qS(2g-1; n) \right) \ . \tag{6.5}$$

Proof.

Using (5.2) we have

$$\begin{aligned}
\langle \mathcal{P}_n \rangle &= -\frac{n}{(q-1)q^{2g+n/2}} \sum_{\deg P = n} \sum_{\substack{\beta+2\alpha=2g+1 \\ \alpha,\beta\geq 0}} \sigma_n(\alpha) \sum_{\deg B=\beta} \left(\frac{B}{P}\right) \\
&= -\frac{n}{(q-1)q^{2g+n/2}} \sum_{\substack{\beta+2\alpha=2g+1 \\ \alpha,\beta\geq 0}} \sigma_n(\alpha) S(\beta; n)
\end{aligned}$$

which gives the first assertion.

Now assume that $n > g$. Then $\sigma_n(\alpha) \neq 0$ forces $\alpha = 0, 1 \mod n$ by Lemma 4(ii) and together with $\alpha \leq g < n$ we must have $\alpha = 0, 1$. Hence in (7.4) the only nonzero terms are those with $\alpha = 0, 1$ which gives (7.5). □

Assume first that $n \leq g$. In (7.4), if $S(\beta; n) \neq 0$ then $\beta < n$ by Lemma 6. For those, we use the bound $|S(\beta; n)| \ll \frac{\beta}{n} q^{\beta + n/2}$ of Lemma 8 and hence

$$\langle \mathcal{P}_n \rangle \ll \frac{n}{q^{2g+\frac{n}{2}}} \sum_{\beta < n} \frac{\beta}{n} q^{n/2+\beta} \ll n q^{n-2g} \leq g q^{-g} \tag{6.6}$$

since $n \leq g$, which vanishes as $g \to \infty$.
For $g < n < 2g$, use (7.5), and note that $S(2g \pm 1; n) = 0$ by Lemma 6. Hence

$$\langle \mathcal{P}_n \rangle = 0, \quad g < n < 2g \, .$$

We have $S(2g+1;2g)=0$ by Lemma 6, and $S(2g-1;2g)=-\pi(2g)q^{\frac{2g-2}{2}}$ by (6.4). Hence

$$
\begin{aligned}
\langle \mathcal{P}_n \rangle &= -\frac{2g}{(q-1)q^{2g+g}}\left(S(2g+1,2g)-qS(2g-1,2g)\right) \\
&= -\frac{2g}{(q-1)q^{2g+g}}q\pi(2g)q^{\frac{2g-2}{2}} \\
&= -\frac{1}{q-1}+O(gq^{-g})\ .
\end{aligned}
$$

Here we use (6.7) to find

$$
\begin{aligned}
\langle \mathcal{P}_n \rangle &= -\frac{n}{(q-1)q^{2g+\frac{n}{2}}} \left(S(2g+1;n) - qS(2g-1;n) \right) \\
&= -\frac{n}{(q-1)q^{2g+\frac{n}{2}}} \left(-\eta_n \pi_q(n) q^{2g+1-\frac{n}{2}} + q\eta_n \pi_q(n) q^{2g-1-\frac{n}{2}} \right) \\
&+ O\left(\frac{n}{q^{2g+\frac{n}{2}}} q^n \right) \\
&= \eta_n \frac{n\pi_q(n)}{q^n} + O\left(nq^{\frac{n}{2}-2g} \right) \\
&= \eta_n \left(1 + O(gq^{-g}) \right) + O(nq^{\frac{n}{2}-2g}) \ .
\end{aligned}
$$

The main term is asymptotic to η_n, and the remainder is $o(1/g)$ provided

$$
2g < n < 4g - 5 \log_q g \ .
$$

The contribution of odd powers of primes P^d, $d > 1$ odd, $\deg P^d = n$, is

$$\mathbb{H}_n = -\frac{1}{q^{\frac{n}{2}}} \sum_{\substack{d|n \\ 3\le d \text{ odd}}} \sum_{\deg P=\frac{n}{d}} \frac{n}{d}\chi_Q(P^d) \, .$$

Since $\chi_Q(P^d) = \chi_Q(P)$ for d odd, the average is

$$\begin{aligned} \langle \mathbb{H}_n \rangle &= -\frac{1}{(q-1)q^{2g+\frac{n}{2}}} \sum_{\substack{d|n \\ 3\le d \text{ odd}}} \frac{n}{d} \sum_{\deg P=\frac{n}{d}} \sum_{2\alpha+\beta=2g+1} \sigma_{n/d}(\alpha) \sum_{\deg B=\beta} \left(\frac{B}{P}\right) \\ &= -\frac{1}{(q-1)q^{2g+\frac{n}{2}}} \sum_{\substack{d|n \\ 3\le d \text{ odd}}} \frac{n}{d} \sum_{2\alpha+\beta=2g+1} \sigma_{n/d}(\alpha) S(\beta; \frac{n}{d}) \, . \end{aligned}$$

In order that $S(\beta; \frac{n}{d}) \neq 0$ we need $\beta < n/d$. Thus using the bound $S(\beta; \frac{n}{d}) \ll q^{\beta + \frac{n}{2d}}$ of (6.6) (recall that $\beta \leq 2g+1$ is odd here) gives

$$\langle \mathbb{H}_n \rangle \ll \frac{1}{q^{2g+\frac{n}{2}}} \sum_{\substack{d|n \\ 3 \leq d \text{ odd}}} \frac{n}{d} \sum_{\beta \leq \min(n/d, 2g+1)} q^{\frac{n}{2d}+\beta}$$

$$\ll \frac{n}{q^{2g+\frac{n}{2}}} \sum_{\substack{d|n \\ 3 \leq d \text{ odd}}} q^{\frac{n}{2d}+\min(2g, \frac{n}{d})} .$$

Treating separately the cases $n/3 < 2g$ and $n/3 \geq 2g$ we see that we have in either case

$$\langle \mathbb{H}_n \rangle \ll g q^{-2g} . \tag{6.7}$$

We saw that

$$\langle \mathrm{tr}\, \Theta_Q^n \rangle = \langle \mathcal{P}_n \rangle + \langle \square_n \rangle + \langle \mathbb{H}_n \rangle$$

with the individual terms giving

$$\langle \mathcal{P}_n \rangle = \begin{cases} O(gq^{-g}), & 0 < n < 2g \\ -\frac{1}{q-1} + O(gq^{-g}), & n = 2g \\ \eta_n + O(nq^{n/2-2g}), & 2g < n \end{cases} ,$$

$$\langle \square_n \rangle = -\eta_n + \eta_n \frac{1}{q^{n/2}} \sum_{\deg P | \frac{n}{2}} \frac{\deg P}{|P|+1} + O(q^{-2g}) ,$$

and

$$\langle \mathbb{H}_n \rangle = O(gq^{-2g}) .$$

Putting these together gives Theorem 1. In particular

$$\langle \operatorname{tr} \Theta_Q^n \rangle = \left\{ \begin{matrix} -\eta_n, & 3\log_q g < n < 2g \\ -1 - \frac{1}{q-1}, & n = 2g \\ 0, & 2g < n < 4g - 8\log_q g \end{matrix} \right\} + o(\frac{1}{g}) \ .$$