ANGLES OF GAUSSIAN PRIMES

BY

Zeév Rudnick and Ezra Waxman

Raymond and Beverly Sackler School of Mathematical Sciences
Tel Aviv University, Tel Aviv 69978, Israel
e-mail: rudnick@post.tau.ac.il, ezrawaxman@gmail.com

ABSTRACT

Fermat showed that every prime $p = 1 \bmod 4$ is a sum of two squares: $p = a^2 + b^2$. To any of the 8 possible representations (a, b) we associate an angle whose tangent is the ratio b/a. In 1919 Hecke showed that these angles are uniformly distributed as p varies, and in the 1950's Kubilius proved uniform distribution in somewhat short arcs. We study fine scale statistics of these angles, in particular the variance of the number of such angles in a short arc. We present a conjecture for this variance, motivated both by a random matrix model, and by a function field analogue of this problem, for which we prove an asymptotic form for the corresponding variance.

CONTENTS

1

1. Introduction

1.1. ANGLES OF GAUSSIAN PRIMES. An odd prime p is a sum of two squares
if and only if $p = 1 \bmod 4$, and in that case there are exactly 8 representations.
Each representation corresponds to a Gaussian integer $a + ib = \sqrt{p}e^{i\theta_{a,b}}$. We
wish to understand the statistics of the resulting angles.

It is useful to formulate the results in terms of prime ideals of the ring of
Gaussian integers $\mathbb{Z}[i]$, which is the ring of integers of the imaginary quadratic
field $\mathbb{Q}(i)$. The basic infra-structure that we need is complex conjugation $z \mapsto \bar{z}$,
the norm map $\mathrm{Norm} : \mathbb{Q}(i)^\times \to \mathbb{Q}^\times$, $\mathrm{Norm}(z) = z\bar{z}$, and the norm one elements

$$S^1_{\mathbb{Q}} = \{z \in \mathbb{Q}(i) : \mathrm{Norm}(z) = 1\} = \mathbb{Q}(i) \cap S^1.$$

For a Gaussian number $\alpha \in \mathbb{Q}(i)^\times$, we have a direction vector given by

$$u(\alpha) := \left(\frac{\alpha}{\bar{\alpha}}\right)^2 \in \mathbb{S}^1_{\mathbb{Q}}$$

so that $u(\alpha) = e^{4i\theta}$, $\theta = \arg \alpha$.

Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Z}[i]$. If $\mathfrak{p} = \langle \alpha \rangle$ is generated by the Gaussian
integer α, we associate a direction vector $u(\mathfrak{p}) := u(\alpha) \in \mathbb{S}^1_{\mathbb{Q}}$. Since all generators
of the ideal differ by multiplication by a unit $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$, the direction
vector $u(\mathfrak{p}) = e^{i4\theta_{\mathfrak{p}}}$ is well-defined on ideals, while the angle $\theta_{\mathfrak{p}}$ is only defined
modulo $\pi/2$. We can choose $\theta_{\mathfrak{p}}$ to lie say in $[0, \pi/2)$, corresponding to taking
$\alpha = a + ib$, with $a > 0$, $b \geq 0$.

Hecke [5] showed that as $\mathfrak{p}$ varies over prime ideals of $\mathbb{Z}[i]$, the angles $\theta_{\mathfrak{p}}$
become uniformly distributed in $[0, \frac{\pi}{2})$: For a fixed sector, defined by an interval
$I \subseteq [0, \frac{\pi}{2})$,

$$(1.1) \qquad \frac{\#\{\mathrm{Norm}\,\mathfrak{p} \leq x : \theta_{\mathfrak{p}} \in I\}}{\#\{\mathrm{Norm}\,\mathfrak{p} \leq x\}} \sim \frac{|I|}{\pi/2}, \quad x \to \infty$$

where $|I|$ is the length of the interval I.

The validity of (1.1) for shrinking sectors was studied by Kubilius and his
school [11, 12, 10, 14, 15, 16], obtaining that (1.1) holds for any sector as
long as $|I| > x^{-\delta}$ for some $1/4 < \delta < 1/2$. See also [4] for existence of prime
angles in somewhat smaller sectors without the full force of (1.1). Assuming the
Generalized Riemann Hypothesis (GRH), we know that (1.1) holds for intervals
with $\mathrm{length}(I) \gg x^{-1/2+o(1)}$. This regime is the limit of what can be expected
to hold for individual sectors, because it is easy to see that there are no Gaussian

integers (let alone primes) in the sector

$$\left\{a, b > 0 : a^2 + b^2 \leq x, 0 < \arctan\frac{b}{a} < x^{-1/2}\right\}.$$

Hence for smaller sectors we can only hope for a statistical theory, rather than individual results.

To formulate the theory, we introduce some notation: Given $x \gg 1$, let N be the number of prime ideals $\mathfrak{p} \subset \mathbb{Z}[i]$ of norm at most x:

$$N := \#\{\mathfrak{p} \text{ prime} : \operatorname{Norm}\mathfrak{p} \leq x\} \sim \frac{x}{\log x},$$

where the asymptotic holds by the Prime Ideal Theorem for $\mathbb{Q}(i)$. Given an interval $I_K(\theta) = [\theta - \frac{\pi}{4K}, \theta + \frac{\pi}{4K}]$ of length $\pi/(2K)$ centered at θ, define a sector

$$\operatorname{Sect}(\theta, x) = \{z \in \mathbb{C} : \operatorname{Norm}(z) = z\bar{z} \leq x, \arg(z) \in I_K(\theta)\}$$

of radius $\sqrt{x}$ and opening angle defined by $I_K(\theta)$.

Given $K \gg 1$, we divide the interval $[0, \pi/2)$ into K disjoint arcs

$$I_K(\theta_1), \ldots, I_K(\theta_K)$$

of equal length, which in turn define K disjoint sectors $\operatorname{Sect}(\theta_j, x)$, and study the number of prime angles falling into each such sector. If the sectors are too small, in the sense that the number K of sectors is larger than the number N of angles involved, then the typical such sector will not contain any Gaussian prime. We want to show that in the range $K \ll N^{1-\epsilon}$, almost all sectors with opening angles of size $\approx 1/K$ contain at least one angle $\theta_{\mathfrak{p}}$, $\operatorname{Norm}(\mathfrak{p}) \leq x$. We can do so assuming GRH (for the family of Hecke L-functions):

THEOREM 1.1: *Assume GRH. Then almost all arcs of length $1/K$ contain at least one angle $\theta_{\mathfrak{p}}$ for a prime ideal with $\operatorname{Norm}(\mathfrak{p}) \leq K(\log K)^{2+o(1)}$.*

Unconditionally, one may use zero-density theorems as in [16] to obtain a result with $\operatorname{Norm}(\mathfrak{p}) < K^{2-\delta}$ for some small $\delta > 0$.

It is surprising that something like Theorem 1.1 does not seem to have been considered long ago. It has come up independently in the recent work of Ori Parzanchevski and Peter Sarnak [17].

1.2. THE NUMBER VARIANCE. One way to obtain such an "almost-everywhere" result is by computing the variance of a suitable counting function. The study of the structure of the variance is the main point of this paper.

Let

$$
\mathcal{N}_{K,x}(\theta) = \#\{\mathfrak{p} \text{ prime, Norm } \mathfrak{p} \le x,\ \theta_{\mathfrak{p}} \in I_K(\theta)\}
\tag{1.2}
$$

be the number of angles $\theta_{\mathfrak{p}}$ in $I_K(\theta)$.

The expected number is

$$
\langle \mathcal{N}_{K,x} \rangle := \int_0^{\pi/2} \mathcal{N}_{K,x}(\theta) \frac{d\theta}{\pi/2} = \frac{N}{K}.
$$

We wish to study the number variance

$$
\mathrm{Var}(\mathcal{N}_{K,x}) = \int_0^{\pi/2} |\mathcal{N}_{K,x} - \langle \mathcal{N}_{K,x} \rangle|^2 \frac{d\theta}{\pi/2}.
$$

If $N = o(K)$, then for almost all intervals, we do not have any angles $\theta_{\mathfrak{p}}$ in the interval $I_K(\theta)$. We can easily compute the variance in this "trivial" regime:

$$
\mathrm{Var}(\mathcal{N}_{K,x}) \sim \frac{N}{K}, \quad N = o(K).
$$

For the interesting range, when $K \ll N^{1-\epsilon}$, we expect:

CONJECTURE 1.2: *For* $1 \ll K \ll N^{1-o(1)}$

$$
\mathrm{Var}(\mathcal{N}_{K,x}) \sim \frac{N}{K} \min\left(1, 2\frac{\log K}{\log N}\right).
$$

For random angles (N uniform independent points in $[0, \pi/2)$), the variance would be $\sim N/K$. Thus we expect the Gaussian angles to display a marked deviation from randomness, in that there is a crossover from purely random behavior for very short intervals ($K \gg N^{1/2}$), to a saturation for moderately short intervals ($1 \ll K \ll N^{1/2}$), where the variance is smaller than that of random angles, so one can say that they display some measure of rigidity. See Figure 1 for numerical evidence. For an explanation of the underlying rigidity present here and for other deviations from randomness, see §2.

A related saturation effect was previously observed by Bui, Keating and Smith [2], in the context of computing the variance of sums in short intervals of coefficients of a fixed L-function of higher degree.

One of our main goals is to justify Conjecture 1.2. In §3 we define a suitably smoothed version of the counting function $\mathcal{N}_{K,x}$ and express the corresponding variance in terms of zeros of a family of Hecke L-functions. This enables us, in §4, to use GRH to give an upper bound for this variance and consequently deduce the almost-everywhere result of Theorem 1.1. Moreover, in §5 we go
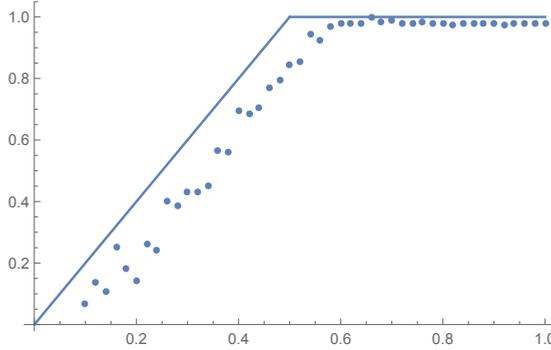
Figure 1. A plot of the ratio $\mathrm{Var}(\mathcal{N}_{K,x})/\mathbb{E}(\mathcal{N}_{K,x})$ versus $\beta = \log K/\log N$, for $x \approx 10^8$. The smooth line is $\min(1, 2\beta)$.

on to develop a suitable random matrix theory model of this result, which gives a result corresponding to Conjecture 1.2. We now turn to formulating a similar problem in a function field setting, where we can prove an analogue of Conjecture 1.2.

1.3. A FUNCTION FIELD ANALOGUE. Let $\mathbb{F}_q$ be a finite field of cardinality q, from now on assumed to be odd. We want to write prime (irreducible monic) polynomials as

$$(1.3) \qquad\qquad P(T) = A(T)^2 + TB(T)^2$$

with $A, B \in \mathbb{F}_q[T]$, which is equivalent to the constant term $P(0)$ being a square in $\mathbb{F}_q$ (see, e.g., [1]). If additionally $P(0) \neq 0$, then there are exactly four such representations, obtained from (1.3) by changing the signs of A and B. This decomposition gives a factorization in $\mathbb{F}_q[T][\sqrt{-T}] = \mathbb{F}_q[\sqrt{-T}]$ as

$$P = \mathfrak{p} \cdot \tilde{\mathfrak{p}} = (A + \sqrt{-T}B)(A - \sqrt{-T}B)$$

and the corresponding factorization of the ideal $(P) \subset \mathbb{F}_q[T]$ into a pair of conjugate prime ideals of $\mathbb{F}_q[\sqrt{-T}]$. The number N of such prime polynomials $\mathfrak{p}(\sqrt{-T})$ of degree ν with $\mathfrak{p}(0) \neq 0$ satisfies

$$N = \frac{q^\nu}{\nu} + O\left(\frac{q^{\nu/2}}{\nu}\right)$$

by the Prime Polynomial Theorem in $\mathbb{F}_q[\sqrt{-T}]$.

Denote $S = \sqrt{-T}$ and consider the quadratic extension $\mathbb{F}_q(T)(\sqrt{-T}) = \mathbb{F}_q(S)$, which is still rational (genus zero). Let $\mathbb{F}_q[[S]]$ be the ring of formal power series. It is equipped with the Galois involution

$$\sigma : S \mapsto -S, \quad \sigma(f)(S) = f(-S),$$

and the norm map

$$\text{Norm} : \mathbb{F}_q[[S]]^\times \to \mathbb{F}_q[[T]]^\times, \quad \text{Norm}(f) = f(S)f(-S).$$

We denote

$$\mathbb{S}^1 := \{g \in \mathbb{F}_q[[S]]^\times : g(0) = 1, \ \text{Norm}(g) = 1\}$$

the formal power series with constant term 1 and unit norm. This is a group, which is our analogue of the unit circle. It is important to note that since q is odd, Hensel's Lemma tells us that the square map $u \mapsto u^2$ is an automorphism of $\mathbb{S}^1$, and in particular each element of $\mathbb{S}^1$ admits a unique square root $\sqrt{u}$.

We put an absolute value $|f| = q^{-\operatorname{ord}(f)}$ on $\mathbb{F}_q[[S]]$, where

$$\operatorname{ord}(f) = \max(j : S^j \mid f).$$

We then divide $\mathbb{S}^1$ into "sectors"

$$\text{Sect}(u; k) = \{v \in \mathbb{S}^1 : |v - u| \le q^{-k}\}.$$

We denote by

$$\mathbb{S}^1_k = \{f \in \mathbb{F}_q[S]/(S^k) : f(0) = 1, \ \text{Norm}(f) := f(-S)f(S) = 1 \bmod S^k\}$$

the elements of unit norm and constant term unity in $(\mathbb{F}_q[S]/(S^k))^\times$. The group $\mathbb{S}^1_k$ parameterizes the different sectors. The order of $\mathbb{S}^1_k$ is

$$K := \#\mathbb{S}^1_k = q^\kappa,$$

where

$$\kappa := \lfloor \frac{k}{2} \rfloor, \quad \text{so that} \quad k = \begin{cases} 2\kappa + 1, \\ 2\kappa. \end{cases}$$

We next want to define the notion of direction (essentially an angle) for any nonzero polynomial

$$f = A(T) + \sqrt{-T}B(T) \in \mathbb{F}_q[\sqrt{-T}].$$

To motivate the definition below, recall that for a nonzero complex number $\alpha = |\alpha|e^{i\theta}$, we have $\alpha/\overline{\alpha} = e^{2i\theta}$. To any nonzero $f \in \mathbb{F}_q[S]$ which is coprime to S, we associate a norm-one element $U(f) \in \mathbb{S}^1$ via the map

$$(1.4) \qquad\qquad U : f \mapsto \sqrt{\frac{f}{\sigma(f)}}.$$

Note that since $f(0) \neq 0$, $f/\sigma(f)$ has constant term one, lies in $\mathbb{F}_q[[S]]$, and has unit norm, that is $f/\sigma(f) \in \mathbb{S}^1$, and hence $\sqrt{f/\sigma(f)} \in \mathbb{S}^1$ exists and is unique. Moreover,

$$U(cf) = U(f)$$

for all scalars $c \in \mathbb{F}_q^\times$, so that if $f \in \mathbb{F}_q[S]$ then $U(f)$ only depends on the ideal $(f) \subset \mathbb{F}_q[S]$ generated by f.

We want to count the number of prime ideals $(\mathfrak{p}) \subset \mathbb{F}_q[S]$ with $\mathfrak{p}(0) \neq 0$, whose directions $U(\mathfrak{p})$ lie in a given sector. For $u \in \mathbb{S}^1$, let

$$\mathcal{N}_{k,\nu}(u) := \#\{(\mathfrak{p}) \text{ prime}, \mathfrak{p}(0) \neq 0 : \deg \mathfrak{p} = \nu, \ U(\mathfrak{p}) \in \text{Sect}(u,k)\}.$$

The mean value is clearly

$$\langle \mathcal{N}_{k,\nu} \rangle := \frac{1}{q^\kappa} \sum_{u \in \mathbb{S}_k^1} \mathcal{N}_{k,\nu}(u) = \frac{N}{K} \sim \frac{q^\nu/\nu}{q^\kappa}.$$

For $k \leq \nu$ we can show (see Corollary 6.5) that as $q \to \infty$,

$$(1.5) \qquad\qquad \mathcal{N}_{k,\nu}(u) = \frac{N}{K} + O(q^{\nu/2})$$

which gives an asymptotic result if $\kappa < \nu/2$. For larger values of κ, there are sectors which do not contain prime directions, as in the number field case; see Remark 6.6.

Our main result is the computation, in the large q limit, of the number variance

$$\text{Var}(\mathcal{N}_{k,\nu}) := \frac{1}{q^\kappa} \sum_{u \in \mathbb{S}_k^1} |\mathcal{N}_{k,\nu} - \langle \mathcal{N}_{k,\nu} \rangle|^2.$$

THEOREM 1.3: *Assume that $\kappa \geq 3$, or if $\kappa = 2$ that $5 \nmid q$. Then as $q \to \infty$,*

$$\text{Var}(\mathcal{N}_{k,\nu}) \sim \frac{q^{\nu-\kappa}}{\nu^2} \times \begin{cases} 2\kappa - 2, & \nu \geq 2\kappa - 2 \\ \nu - 1 + \eta(\nu), & \kappa \leq \nu \leq 2\kappa - 2 \end{cases}$$

where $\eta(\nu) = 1$ if ν is even, and 0 otherwise.

To compare it to our number field conjecture, here the number of sectors is $K = q^{\kappa}$, the number of directions (the number of Gaussian prime ideals $\mathfrak{p}$ of degree ν) is $N \sim q^{\nu}/\nu$, so that the expected value is N/K, and the variance satisfies, as $q \to \infty$,

$$
\frac{\mathrm{Var}(\mathcal{N}_{\kappa,\nu})}{N/K} \sim
\begin{cases}
2\frac{\log_q K}{\log_q N} - \frac{2}{\log_q N}, & \log_q K \leq \frac{1}{2}\log_q N + 1, \\
1 + \frac{\eta(\log_q N)-1}{\log_q N}, & \frac{1}{2}\log_q N + 1 \leq \log_q K \leq \log_q N.
\end{cases}
$$

Our Conjecture 1.2 for the number-field variance is

$$
\frac{\mathrm{Var}(\mathcal{N}_{K,N})}{N/K} \sim \min\left(1, 2\frac{\log K}{\log N}\right)
$$

which is analogous to the above.

2. Repulsion between angles

2.1. REPULSION AND ITS CONSEQUENCES. Let $\mathfrak{a}$ be a nonzero ideal in $\mathbb{Z}[i]$. If $\mathfrak{a} = \langle \alpha \rangle$ is generated by the Gaussian integer α, we associate a direction vector $u(\mathfrak{p}) := u(\alpha) \in \mathbb{S}^1_{\mathbb{Q}}$. Since all generators of the ideal differ by multiplication by a unit $\mathbb{Z}[i]^{\times} = \{\pm 1, \pm i\}$, the direction vector $u(\mathfrak{a}) = e^{i4\theta_{\mathfrak{a}}}$ is well-defined on ideals, while the angle $\theta_{\mathfrak{a}}$ is only defined modulo $\pi/2$. We can choose $\theta_{\mathfrak{a}}$ to lie say in $[0, \pi/2)$, corresponding to taking $\alpha = a + ib$, with $a > 0$, $b \geq 0$. If $\mathfrak{a} = \langle \alpha \rangle$ for nonzero $\alpha \in \mathbb{Z}$, then $\theta_{\mathfrak{a}} = 0$.

LEMMA 2.1: (i) If $\theta_{\mathfrak{a}} \neq 0$ then

$$
\theta_{\mathfrak{a}} \gg \frac{1}{\sqrt{\mathrm{Norm}\,\mathfrak{a}}}.
$$

(ii) If $\mathfrak{p} \neq \mathfrak{q}$ are ideals with distinct angles $\theta_{\mathfrak{p}} \neq \theta_{\mathfrak{q}}$ then

$$
|\theta_{\mathfrak{p}} - \theta_{\mathfrak{q}}| \geq \frac{1}{\sqrt{\mathrm{Norm}\,\mathfrak{p}\,\mathrm{Norm}\,\mathfrak{q}}}.
$$

Proof. (i) Write $\mathfrak{a} = \langle a + ib \rangle$ with $a, b > 0$. Then

$$\tan \theta_{\mathfrak{a}} = \frac{b}{a} \geq \frac{1}{a} \geq \frac{1}{\sqrt{a^2 + b^2}} = \frac{1}{\sqrt{\text{Norm } \mathfrak{a}}}.$$

Since we may assume that $\theta_{\mathfrak{a}} \in (0, \pi/4)$, we have $\tan \theta_{\mathfrak{a}} \leq \sqrt{2} \theta_{\mathfrak{a}}$ which gives our claim.

(ii) Write $\mathfrak{p} = \langle a + ib \rangle$, $\mathfrak{q} = \langle c + id \rangle$, with $a, b > 0$ and $c > 0$, $d \geq 0$. Consider the triangle having vertices at the origin, $a + ib$ and $c + id$. Since $\theta_{\mathfrak{p}} \neq \theta_{\mathfrak{q}}$, its area is positive and being a lattice triangle, its area is at least $1/2$.

On the other hand, its area is given in terms of the angle $\theta_{\mathfrak{p}} - \theta_{\mathfrak{q}}$ between the sides $a + ib$ and $c + id$ as

$$\text{area} = \frac{1}{2} \sqrt{\text{Norm } \mathfrak{p}} \sqrt{\text{Norm } \mathfrak{q}} \sin |\theta_{\mathfrak{p}} - \theta_{\mathfrak{q}}|.$$

Thus we find

$$\sqrt{\text{Norm } \mathfrak{p}} \sqrt{\text{Norm } \mathfrak{q}} \sin |(\theta_{\mathfrak{p}} - \theta_{\mathfrak{q}})| \geq 1$$

and hence

$$|\theta_{\mathfrak{p}} - \theta_{\mathfrak{q}}| \geq \sin |\theta_{\mathfrak{p}} - \theta_{\mathfrak{q}}| \geq \frac{1}{\sqrt{\text{Norm } \mathfrak{p} \, \text{Norm } \mathfrak{q}}}. \qquad \blacksquare$$

Lemma 2.1 implies that the interval $\{0 < \theta < 1/\sqrt{x}\}$ will contain no angles $\theta_{\mathfrak{p}}$ for $\text{Norm } \mathfrak{p} \ll x$, so that the number $\mathcal{N}_{K,x}$ of prime angles $\theta_{\mathfrak{p}}$ in this interval is zero. Hence we cannot expect an asymptotic formula $\mathcal{N}_{K,x} \sim N/K$ to hold for all intervals if $K \ll N^{1/2}$, while it does hold (assuming GRH) for larger intervals. Theorem 1.1 guarantees that almost all intervals will contain angles if $K \ll N^{1-o(1)}$.

2.2. DEVIATIONS FROM RANDOMNESS. The existence of a "big hole" as above displays a striking deviation from randomness of the angles, when compared to N random angles in $[0, \pi/2)$. For these, the maximal gap is almost surely of order $\log N / N$, while Lemma 2.1(i) guarantees a much larger gap, of size $N^{-1/2 - o(1)}$.

Another statistic which indicates that Gaussian angles behave differently than random points is the minimal spacing statistic: For N random angles in $[0, \pi/2)$ as above, the smallest gap is almost surely of size $\approx 1/N^2$ [13]. In contrast, the minimal gap between the angles $\{\theta_{\mathfrak{p}} \neq 0 : \text{Norm } \mathfrak{p} \leq x\}$ is by Lemma 2.1

$$\min\{|\theta_{\mathfrak{p}} - \theta_{\mathfrak{p}'}| : \text{Norm } \mathfrak{p}, \text{Norm } \mathfrak{p}' \leq x, \mathfrak{p} \neq \mathfrak{p}'\} \gg \frac{1}{x} \approx \frac{1}{N \log N},$$

which is much bigger than the random case.

2.3. THE VARIANCE IN THE TRIVIAL REGIME. We want to study fluctuations in
the number $\mathcal{N}_{K,x}$ of angles falling in "random" short intervals. Take the interval
length $1/K = o(1/x)$, equivalently the number K of intervals, to be much larger
than the number $N \sim x/\log x$ of angles: $N = o(K)$. Then for almost all intervals,
we do not have any angles $\theta_{\mathfrak{p}}$ in the interval $I_K(\theta)$. Nonetheless we can compute
the variance in this "trivial" regime.

PROPOSITION 2.2: If $x = o(K)$ then
$$\mathrm{Var}(\mathcal{N}_{K,x}) \sim \frac{N}{K}.$$

Proof. We recall definition (1.2): Given an interval $I_K(\theta) = [\theta - \frac{\pi}{4K}, \theta + \frac{\pi}{4K}]$ of
length $\pi/2K$ centered at θ, let[1]
$$\mathcal{N}_{K,x}(\theta) = \#\{\mathfrak{p} \text{ prime, Norm}\,\mathfrak{p} \leq x : \theta_{\mathfrak{p}} \in I_K(\theta)\} = \sum_{\substack{\text{Norm}\,\mathfrak{p} \leq x \\ \text{prime}}} I_K(\theta_{\mathfrak{p}} - \theta)$$
be the number of prime angles $\theta_{\mathfrak{p}}$ in $I_K(\theta)$. We will take the center θ of the
interval to be random, that is uniform in $(0, \pi/2)$.

We compute the second moment of $\mathcal{N} = \mathcal{N}_{K,x}$ using its definition
$$\langle \mathcal{N}^2 \rangle = \sum_{\text{Norm}\,\mathfrak{p} \leq x} \sum_{\text{Norm}\,\mathfrak{q} \leq x} \langle I_K(\theta_{\mathfrak{p}} - \theta) I_K(\theta_{\mathfrak{q}} - \theta) \rangle,$$
where throughout we use
$$\langle H \rangle := \frac{1}{\pi/2} \int_0^{\pi/2} H(\theta) d\theta.$$
The contribution of pairs of inert primes, where $\theta_{\mathfrak{p}} = 0$, $\mathfrak{p} = \langle p \rangle$, $p = 3 \bmod 4$,
Norm $\mathfrak{p} = p^2 \leq x$, is
$$(\#\{p = 3 \bmod 4, p \leq \sqrt{x}\})^2 \cdot \langle I_K(-\theta)^2 \rangle.$$
Note that $I_K^2 = I_K$ and
$$\langle I_K(-\theta)^2 \rangle = \langle I_K(\theta) \rangle = \frac{\text{length}(I_K)}{\pi/2} = \frac{1}{K}.$$
Moreover, the number of $p = 3 \bmod 4$, $p \leq \sqrt{x}$ is $\ll \sqrt{x}/\log x$. Hence the
contribution of pairs of inert primes is $O(\frac{x}{K(\log x)^2})$.

---
[1] We abuse notation and use the same symbol for the interval and its indicator function.

If $\mathfrak{p} \neq \mathfrak{q}$ and at least one of $\mathfrak{p}$, $\mathfrak{q}$ is not inert, so that $\theta_{\mathfrak{p}} \neq \theta_{\mathfrak{q}}$, then Lemma 2.1 gives

$$|\theta_{\mathfrak{p}} - \theta_{\mathfrak{q}}| \geq \frac{1}{x}.$$

For the integral $\langle I_K(\theta_{\mathfrak{p}} - \theta) I_K(\theta_{\mathfrak{q}} - \theta) \rangle$ to be nonzero, it is necessary that there be some θ so that both $\theta_{\mathfrak{p}}, \theta_{\mathfrak{q}} \in I_K(\theta)$, which forces the distance between the two angles to be at most $\pi/2K$:

$$|\theta_{\mathfrak{p}} - \theta_{\mathfrak{q}}| \leq \frac{\pi}{2K}.$$

Hence if $x = o(K)$ then such off-diagonal pairs contribute nothing.

We conclude that the second moment of $\mathcal{N}_{K,x}$ is essentially given by the sum of the diagonal terms

$$\langle \mathcal{N}^2 \rangle = \sum_{\text{Norm } \mathfrak{p} \leq x} \langle I_K(\theta_{\mathfrak{p}} - \theta)^2 \rangle + O\left(\frac{x}{K(\log x)^2} \right)$$

$$= \sum_{\text{Norm } \mathfrak{p} \leq x} \frac{1}{K} + O\left(\frac{x}{K(\log x)^2} \right) \sim \frac{N}{K}.$$

We can now compute the variance:

$$\text{Var}(\mathcal{N}) = \langle \mathcal{N}^2 \rangle - \langle \mathcal{N} \rangle^2 \sim \frac{N}{K} - \left(\frac{N}{K} \right)^2.$$

Since $N = o(K)$ we find

$$\text{Var}(\mathcal{N}) \sim \frac{N}{K}$$

as claimed. ∎

3. Almost all sectors contain an angle

3.1. A SMOOTH COUNT. Our goal in this section is to prove Theorem 1.1, which claims (assuming GRH) that in the non-trivial range $K \ll X^{1-\epsilon}$, almost all arcs of size $\approx 1/K$ contain at least one angle $\theta_{\mathfrak{p}}$, $\text{Norm}(\mathfrak{p}) \leq X$. We can do so assuming GRH (for the family of Hecke L-functions).

To count the number of angles $\theta_{\mathfrak{p}}$ lying in a short segment of $[0, \pi/2)$, pick a window function $f \in C_c^\infty(\mathbb{R})$, which we take to be even and real valued, and for $K \gg 1$ define

$$F_K(\theta) := \sum_{j \in \mathbb{Z}} f\left(\frac{K}{\pi/2} \left(\theta - j\frac{\pi}{2} \right) \right)$$

which is $\pi/2$-periodic, and localized on a scale of $1/K$. The Fourier expansion of F_K is

$$(3.1) \qquad F_K(\theta) = \sum_{k \in \mathbb{Z}} \widehat{F}_K(k) e^{i4k\theta}, \quad \widehat{F}_K(k) = \frac{1}{K} \widehat{f}\Big(\frac{k}{K}\Big),$$

where the Fourier transform is normalized as $\widehat{f}(y) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i y x} dx$. Note that since f is even and real valued, the same holds for $\widehat{f}$.

Let $\Phi \in C_c^\infty(0, \infty)$. Now set

$$\psi_{K,X}^{\mathrm{prime}}(\theta) := \sum_{\mathfrak{p} \text{ prime}} \Phi\Big(\frac{\mathrm{Norm}\,\mathfrak{p}}{X}\Big) \log \mathrm{Norm}(\mathfrak{p}) F_K(\theta_\mathfrak{p} - \theta),$$

the sum over all prime ideals of $\mathbb{Z}[i]$, which gives a smooth count of prime angles $\theta_\mathfrak{p}$ lying in a smooth window defined F_K around θ. We also define

$$\psi_{K,X}(\theta) := \sum_{\mathfrak{a}} \Phi\Big(\frac{\mathrm{Norm}\,\mathfrak{a}}{X}\Big) \Lambda(\mathfrak{a}) F_K(\theta_\mathfrak{a} - \theta),$$

the sum over all powers of prime ideals, with the von Mangoldt function $\Lambda(\mathfrak{a}) = \log \mathrm{Norm}(\mathfrak{p})$ if $\mathfrak{a} = \mathfrak{p}^r$ is a power of a prime ideal $\mathfrak{p}$, and equal to zero otherwise.

We next compute the mean value.

LEMMA 3.1: *The mean values of $\psi_{K,X}$ and $\psi_{K,X}^{\mathrm{prime}}$ are asymptotically*

$$(3.2) \qquad \langle \psi_{K,X} \rangle \sim \langle \psi_{K,X}^{\mathrm{prime}} \rangle \sim \frac{X}{K} \int_{-\infty}^{\infty} f(x) dx \int_0^\infty \Phi(u) du.$$

Moreover,

$$|\langle \psi_{K,X} \rangle - \langle \psi_{K,X}^{\mathrm{prime}} \rangle| \ll \frac{X^{1/2}}{K}.$$

Proof. The mean value is

$$\langle \psi_{K,X} \rangle = \frac{1}{K} \widehat{f}(0) \sum_{\mathfrak{p} \text{ prime}} \Phi\Big(\frac{\mathrm{Norm}\,\mathfrak{p}}{X}\Big) \Lambda(\mathfrak{p}).$$

We can evaluate this using the Prime Ideal Theorem to obtain

$$\langle \psi_{K,X} \rangle \sim \frac{X}{K} \int_{-\infty}^{\infty} f(x) dx \int_0^\infty \Phi(u) du,$$

and likewise for $\langle \psi_{K,X}^{\mathrm{prime}} \rangle$. If in addition we use GRH, we obtain a remainder term of $O(\frac{X^{1/2}}{K})$ for both.

We bound the difference by

$$\langle \psi_{K,X} \rangle - \langle \psi_{K,X}^{\mathrm{prime}} \rangle = \sum_{\mathfrak{a} \neq \mathrm{prime}} \Lambda(\mathfrak{a}) \Phi\Big(\frac{\mathrm{Norm}\,\mathfrak{a}}{X}\Big) \frac{\widehat{f}(0)}{K}$$

$$\ll \frac{1}{K} \sum_{\substack{\mathrm{Norm}(\mathfrak{a}) \ll X \\ \mathfrak{a} \neq \mathrm{prime}}} \Lambda(\mathfrak{a}) \ll \frac{X^{1/2}}{K},$$

which shows that the mean values are close. ∎

Note that the inert primes $\mathfrak{p} = \langle p \rangle$ give angle $\theta_{\mathfrak{p}} = 0$, but that $\mathrm{Norm}\,\mathfrak{p} = p^2$ so that in $\psi_{K,X}^{\mathrm{prime}}$, we get a contribution of size $\sqrt{X}$ if $\theta \approx 0$. This is significantly larger than the mean value if $K \gg X^{1/2}$.

3.2. VARIANCE IN THE TRIVIAL REGIME. The variance of $\psi_{K,X}^{\mathrm{prime}}$ in the trivial regime $X = o(K)$ is

$$(3.3) \qquad \mathrm{Var}(\psi_{K,X}) \sim \mathrm{Var}(\psi_{K,X}^{\mathrm{prime}}) \sim c_2(f, \Phi) \cdot \frac{X \log X}{K},$$

where

$$c_2(f, \Phi) := \int_{-\infty}^{\infty} f(y)^2 dy \int_0^{\infty} \Phi(t)^2 dt.$$

Indeed, if $X = o(K)$ then the same argument of repulsion between angles as in §2.3 allows us to compute the second moment as asymptotically equal to the sum over the diagonal pairs

$$\langle |\psi_{K,X}|^2 \rangle \sim \langle |F_K(\theta)|^2 \rangle \sum_{\mathfrak{a}} \Phi\Big(\frac{\mathrm{Norm}(\mathfrak{a})}{X}\Big)^2 \Lambda(\mathfrak{a})^2.$$

By Parseval's theorem, we have

$$\langle |F_K(\theta)|^2 \rangle = \frac{1}{\pi/2} \int_0^{\pi/2} |F_K(\theta)|^2 d\theta = \sum_{k \in \mathbb{Z}} |\widehat{F}_K(k)|^2$$

$$= \frac{1}{K^2} \sum_{k \in \mathbb{Z}} \widehat{f}\Big(\frac{k}{K}\Big)^2 \sim \frac{1}{K} \int_{-\infty}^{\infty} f(y)^2 dy$$

and

$$\sum_{\mathfrak{a}} \Phi\Big(\frac{\mathrm{Norm}(\mathfrak{a})}{X}\Big)^2 \Lambda(\mathfrak{a})^2 \sim \int_0^{\infty} \Phi(t)^2 dt \cdot X \log X$$

by the Prime Ideal Theorem. This gives the second moment as

$$\langle |\psi_{K,X}^{\mathrm{prime}}|^2 \rangle \sim \int_{-\infty}^{\infty} f(y)^2 dy \int_0^{\infty} \Phi(t)^2 dt \cdot \frac{X \log X}{K},$$

and since $X = o(K)$, we obtain (3.3) for $\mathrm{Var}(\psi_{K,X})$. The argument for $\mathrm{Var}(\psi_{K,X}^{\mathrm{prime}})$ is identical.

3.3. AN UPPER BOUND. We give an upper bound on the variance of $\psi_{K,X}^{\mathrm{prime}}$ in the non-trivial regime $K \ll X$, assuming GRH.

THEOREM 3.2: *Assume GRH. Then*

$$\mathrm{Var}(\psi_{K,X}^{prime}) \ll \frac{X}{K}(\log K)^2.$$

From this bound we easily deduce Theorem 1.1: We use Chebyshev's inequality and Theorem 3.2 to deduce

$$\mathrm{Prob}\{\theta : |\psi_{K,X}^{\mathrm{prime}}(\theta) - \mathbb{E}(\psi_{K,X}^{\mathrm{prime}})| > \frac{1}{2}\mathbb{E}(\psi_{K,X}^{\mathrm{prime}})\} \leq \frac{\mathrm{Var}(\psi_{K,X}^{\mathrm{prime}})}{\frac{1}{4}(\mathbb{E}(\psi_{K,X}^{\mathrm{prime}}))^2}$$
$$\ll \frac{\frac{X}{K}(\log K)^2}{(\frac{X}{K})^2} \ll \frac{K(\log K)^2}{X}.$$

Taking $X = K(\log K)^{2+o(1)}$ we find that for almost all θ,

$$\psi_{K,X}^{\mathrm{prime}}(\theta) \gg \frac{X}{K}$$

is nonzero. Therefore the sum defining $\psi_{K,X}^{\mathrm{prime}}$ is non-empty, and since it is a sum over prime ideals giving angles $\theta_{\mathfrak{p}}$ in the arc of length $\approx 1/K$ around θ, we find that for almost all θ, such arcs contain an angle $\theta_{\mathfrak{p}}$ for a prime ideal with $\mathrm{Norm}(\mathfrak{p}) \leq X = K(\log K)^{2+o(1)}$. $\blacksquare$

The proof of Theorem 3.2 will be presented in §4.4.

4. Relation to zeros of Hecke L-functions

4.1. HECKE CHARACTERS AND THEIR L-FUNCTIONS. The Hecke characters

$$\Xi_k(\alpha) = (\alpha/\bar{\alpha})^{2k}, \quad k \in \mathbb{Z},$$

give well defined functions on the ideals of $\mathbb{Z}[i]$. In terms of the angles associated to ideals, we have

$$e^{i4k\theta_{\mathfrak{p}}} = \Xi_k(\mathfrak{p}).$$

To each such character Hecke [5] associated its L-function

$$L(s, \Xi_k) = \sum_{0 \neq \mathfrak{a} \subseteq \mathbb{Z}[i]} \frac{\Xi_k(\mathfrak{a})}{(\mathrm{Norm}\,\mathfrak{a})^s} = \prod_{\substack{\mathfrak{p} \\ \mathrm{prime}}} (1 - \Xi_k(\mathfrak{p})(\mathrm{Norm}\,\mathfrak{p})^{-s})^{-1}, \quad \mathrm{Re}(s) > 1.$$

Note that $L(s, \Xi_k) = L(s, \Xi_{-k})$. Hecke showed that if $k \neq 0$, these functions have an analytic continuation to the entire complex plane, and satisfy a functional equation:

$$(4.1) \qquad \xi_k(s) := \pi^{-(s+2|k|)} \Gamma(s + 2|k|) L(s, \Xi_k) = \xi_k(1 - s).$$

The completed L-function $\xi_k(s)$ has all its zeros in the critical strip $0 < \mathrm{Re}(s) < 1$ (the non-trivial zeros of $L(s, \Xi_k)$), and the Generalized Riemann Hypothesis asserts that they all lie on the critical line $\mathrm{Re}(s) = 1/2$. The growth of the number of non-trivial zeros of $L(s, \Xi_k)$ in a fixed rectangle is

$$(4.2) \qquad \#\{\rho : 0 \leq \mathrm{Im}(\rho) \leq T_0\} \sim \frac{T_0 \log k}{\pi}, \quad k \to \infty, \quad T_0 > 0 \text{ fixed},$$

in other words, the density of zeros is $\frac{\log |k|}{\pi}$.

LEMMA 4.1:

$$(4.3) \qquad \psi_{K,X}(\theta) = \sum_k e^{-i4k\theta} \frac{1}{K} \widehat{f}\Big(\frac{k}{K}\Big) \sum_{\mathfrak{a}} \Phi\Big(\frac{\mathrm{Norm}\,\mathfrak{a}}{X}\Big) \Lambda(\mathfrak{a}) \Xi_k(\mathfrak{a})$$

and

$$(4.4) \qquad \psi_{K,X}^{prime}(\theta) = \sum_k e^{-i4k\theta} \frac{1}{K} \widehat{f}\Big(\frac{k}{K}\Big) \sum_{\mathfrak{p}\ prime} \Phi\Big(\frac{\mathrm{Norm}\,\mathfrak{p}}{X}\Big) \Lambda(\mathfrak{p}) \Xi_k(\mathfrak{p}).$$

Proof. Inserting the Fourier expansion (3.1) of F_K gives

$$\psi_{K,X}^{\mathrm{prime}}(\theta) = \sum_k e^{-i4k\theta} \frac{1}{K} \widehat{f}\Big(\frac{k}{K}\Big) \sum_{\mathfrak{p}} \Phi\Big(\frac{\mathrm{Norm}\,\mathfrak{p}}{X}\Big) \Lambda(\mathfrak{p}) e^{i4k\theta_{\mathfrak{p}}}.$$

Now note that $e^{i4k\theta_{\mathfrak{p}}} = \Xi_k(\mathfrak{p})$ is the Hecke character, to obtain (4.4). The same argument gives (4.3). ∎

The zero mode $k{=}0$ in (4.4) is the mean value (3.2). The same holds for $\psi_{K,X}$.

4.2. An Explicit Formula.

PROPOSITION 4.2: *Let* $\Phi \in C_c^\infty(0, \infty)$, *and let*

$$\tilde{\Phi}(s) = \int_0^\infty \Phi(x) x^s \frac{dx}{x}$$

be its Mellin transform. Then for $k \neq 0$ *and* $X \gg_\Phi 1$,

$$\sum_{\mathfrak{a}} \Lambda(\mathfrak{a}) \Xi_k(\mathfrak{a}) \Phi\left(\frac{\text{Norm}(\mathfrak{a})}{X}\right)$$

$$= -\sum_{\xi_k(\rho)=0} \tilde{\Phi}(\rho) X^\rho + \frac{1}{2\pi i} \int_{(2)} \left\{ \frac{\Gamma'}{\Gamma}(s + 2|k|) + \frac{\Gamma'}{\Gamma}(1 - s + 2|k|) \right\} \tilde{\Phi}(s) X^s ds,$$

where the sum on the RHS is over all non-trivial zeros of $L(s, \Xi_k)$.

Proof. We abbreviate $L_k(s) := L(s, \Xi_k)$. Using Mellin inversion

$$\Phi(x) = \frac{1}{2\pi i} \int_{\text{Re}(s)=2} \tilde{\Phi}(s) x^{-s} ds$$

we obtain

$$\sum_{\mathfrak{a}} \Lambda(\mathfrak{a}) \Xi_k(\mathfrak{a}) \Phi\left(\frac{\text{Norm}(\mathfrak{a})}{X}\right) = \frac{1}{2\pi i} \int_{(2)} \sum_{\mathfrak{a}} \Lambda(\mathfrak{a}) \Xi_k(\mathfrak{a}) \frac{X^s}{\text{Norm}(\mathfrak{a})^s} \tilde{\Phi}(s) ds$$

$$= \frac{1}{2\pi i} \int_{(2)} -\frac{L_k'}{L_k}(s) \tilde{\Phi}(s) X^s ds.$$

In terms of the completed L-function $\xi_k(s)$, the logarithmic derivative of $L(s, \Xi_k)$ is

$$-\frac{L_k'}{L_k}(s) = -\log \pi + \frac{\Gamma'}{\Gamma}(s + 2|k|) - \frac{\xi_k'}{\xi_k}(s).$$

Inserting into the above gives

$$\frac{1}{2\pi i} \int_{(2)} -\frac{L_k'}{L_k}(s) \tilde{\Phi}(s) X^s ds = \frac{1}{2\pi i} \int_{(2)} \left(-\log \pi + \frac{\Gamma'}{\Gamma}(s + 2|k|) \right) \tilde{\Phi}(s) X^s ds$$

$$+ \frac{1}{2\pi i} \int_{(2)} -\frac{\xi_k'}{\xi_k}(s) \tilde{\Phi}(s) X^s ds.$$

We shift the contour in the integral to $\text{Re}(s) = -1$, picking up the poles of $-\frac{\xi_k'}{\xi_k}(s)$, which are all simple poles with residue -1 at the non-trivial zeros of $L_k(s)$, giving

$$\frac{1}{2\pi i} \int_{(2)} -\frac{\xi_k'}{\xi_k}(s) \tilde{\Phi}(s) X^s ds = -\sum_{\rho} \tilde{\Phi}(\rho) X^\rho + \frac{1}{2\pi i} \int_{(-1)} -\frac{\xi_k'}{\xi_k}(s) \tilde{\Phi}(s) X^s ds.$$

Changing variables $s \mapsto 1 - s$ gives

$$\frac{1}{2\pi i}\int_{(-1)} -\frac{\xi_k'}{\xi_k}(s)\tilde{\Phi}(s)X^s ds = \frac{1}{2\pi i}\int_{(2)} -\frac{\xi_k'}{\xi_k}(1-s)\tilde{\Phi}(1-s)X^{1-s} ds.$$

The functional equation (4.1) of $L(s, \Xi_k)$ implies

$$-\frac{\xi_k'}{\xi_k}(s) = \frac{\xi_k'}{\xi_k}(1-s),$$

which gives

$$\frac{1}{2\pi i}\int_{(2)} -\frac{\xi_k'}{\xi_k}(1-s)\tilde{\Phi}(1-s)X^{1-s} ds = \frac{1}{2\pi i}\int_{(2)} \frac{\xi_k'}{\xi_k}(s)\tilde{\Phi}(1-s)X^{1-s} ds.$$

Returning to the incomplete L-function gives

$$\frac{1}{2\pi i}\int_{(2)} \frac{\xi_k'}{\xi_k}(s)\tilde{\Phi}(1-s)X^{1-s} ds$$

$$=\frac{1}{2\pi i}\int_{(2)} \Big(-\log\pi + \frac{\Gamma'}{\Gamma}(s+2|k|) + \frac{L_k'}{L_k}(s)\Big)\tilde{\Phi}(1-s)X^{1-s} ds$$

$$= -\log\pi\frac{1}{2\pi i}\int_{(2)} \tilde{\Phi}(s)X^s ds + \frac{1}{2\pi i}\int_{(2)} \frac{\Gamma'}{\Gamma}(1-s+2|k|)\tilde{\Phi}(s)X^s ds$$

$$+ \frac{1}{2\pi i}\int_{(2)} \frac{L_k'}{L_k}(s)\tilde{\Phi}(1-s)X^{1-s} ds.$$

By Mellin inversion,

$$\frac{1}{2\pi i}\int_{(2)} \tilde{\Phi}(s)X^s ds = \Phi\Big(\frac{1}{X}\Big),$$

which vanishes for $X \gg 1$ as Φ is compactly supported in $(0, \infty)$. Likewise,

$$\frac{1}{2\pi i}\int_{(2)} \frac{L_k'}{L_k}(s)\tilde{\Phi}(1-s)X^{1-s} ds$$

$$= -\frac{1}{2\pi i}\int_{(2)} \sum_{\mathfrak{a}} \frac{\Lambda(\mathfrak{a})\Xi_k(\mathfrak{a})}{\mathrm{Norm}(\mathfrak{a})^s}X^{1-s}\tilde{\Phi}(1-s) ds$$

$$= -\sum_{\mathfrak{a}} \frac{\Lambda(\mathfrak{a})\Xi_k(\mathfrak{a})}{\mathrm{Norm}(\mathfrak{a})}\frac{1}{2\pi i}\int_{(2)} \tilde{\Phi}(1-s)(X\,\mathrm{Norm}(\mathfrak{a}))^{1-s} ds$$

$$= -\sum_{\mathfrak{a}} \frac{\Lambda(\mathfrak{a})\Xi_k(\mathfrak{a})}{\mathrm{Norm}(\mathfrak{a})}\Phi\Big(\frac{1}{X\,\mathrm{Norm}(\mathfrak{a})}\Big) = 0,$$

since each term vanishes for $X \gg 1$ (independently of $\mathfrak{a}$, since $\mathrm{Norm}(\mathfrak{a}) \geq 1$).

Collecting terms, we find

$$\sum_{\mathfrak{a}} \Lambda(\mathfrak{a})\Xi_k(\mathfrak{a})\Phi\left(\frac{\mathrm{Norm}(\mathfrak{a})}{X}\right)$$

$$= -\sum_{\rho} \tilde{\Phi}(\rho)X^{\rho} + \frac{1}{2\pi i}\int_{(2)}\left\{\frac{\Gamma'}{\Gamma}(s+2|k|) + \frac{\Gamma'}{\Gamma}(1-s+2|k|)\right\}\tilde{\Phi}(s)X^s ds,$$

as claimed. ■

LEMMA 4.3: *For* $k \neq 0$,

$$\frac{1}{2\pi i}\int_{(2)}\left\{\frac{\Gamma'}{\Gamma}(s+2|k|) + \frac{\Gamma'}{\Gamma}(1-s+2|k|)\right\}\tilde{\Phi}(s)X^s ds \ll \frac{X^{1/2}\log 2|k|}{(\log X)^{100}}.$$

Proof. Note that the integrand is analytic in $-2 < \mathrm{Re}(s) < 3$, so we may shift the contour of integration to $\mathrm{Re}(s) = 1/2$. Let

$$h_k(t) := \left\{\frac{\Gamma'}{\Gamma}\left(\frac{1}{2}+it+2|k|\right) + \frac{\Gamma'}{\Gamma}\left(\frac{1}{2}-it+2|k|\right)\right\}\tilde{\Phi}\left(\frac{1}{2}+it\right).$$

The integral is essentially $X^{1/2}$ times the Fourier transform $\widehat{h}_k(\log X)$, that is

$$X^{1/2}\frac{1}{2\pi}\int_{-\infty}^{\infty}h_k(t)e^{it\log X}dt.$$

We can estimate the derivatives of $h_k(t)$ by using Stirling's formula and the rapid decay of $\tilde{\Phi}(\frac{1}{2}+it)$ as being bounded by

$$|h_k^{(j)}(t)| \ll \frac{\log 2|k|}{(1+|t|)^{200}}.$$

Hence integration by parts shows that the Fourier transform of h_k is bounded by

$$|\widehat{h}_k(\log X)| \ll \frac{\log 2|k|}{(\log X)^{100}},$$

which proves the Lemma. ■

From Lemma 4.1, Proposition 4.2 and Lemma 4.3 we deduce

COROLLARY 4.4: *Assume GRH. Then*

$$\psi_{K,X}(\theta) - \langle\psi_{K,X}\rangle$$

$$= -X^{1/2}\sum_{k\neq 0}e^{-i4k\theta}\frac{1}{K}\widehat{f}\left(\frac{k}{K}\right)\left(\sum_{\xi_k(\frac{1}{2}+i\gamma_{k,n})=0}\tilde{\Phi}\left(\frac{1}{2}+i\gamma_{k,n}\right)X^{i\gamma_{k,n}} + O\left(\frac{\log K}{(\log X)^{100}}\right)\right).$$

Averaging Corollary 4.4 over θ we find

COROLLARY 4.5: *Assume GRH. Then*

$$\mathrm{Var}(\psi_{K,X})$$

$$= \frac{X}{K^2} \sum_{k \neq 0} \widehat{f}\Big(\frac{k}{K}\Big)^2 \Big(\sum_{\xi_k(\frac{1}{2}+i\gamma_{k,n})=0} \tilde{\Phi}\Big(\frac{1}{2}+i\gamma_{k,n}\Big)X^{i\gamma_{k,n}} + O\Big(\frac{\log K}{(\log X)^{100}}\Big)\Big)^2.$$

COROLLARY 4.6: *Assume GRH. Then*

$$\mathrm{Var}(\psi_{K,X}) \ll \frac{X}{K}(\log K)^2.$$

Proof. We use GRH to obtain $|X^{i\gamma_{k,n}}| = 1$ so that

$$(4.5) \qquad \Big| \sum_n \tilde{\Phi}\Big(\frac{1}{2}+i\gamma_{k,n}\Big)X^{i\gamma_{k,n}} \Big| \leq \sum_n \Big| \tilde{\Phi}\Big(\frac{1}{2}+i\gamma_{k,n}\Big) \Big|.$$

We use a standard bound for the number of zeros of $L(s, \Xi_k)$ in an interval (see [6, Proposition 5.7]):

$$(4.6) \qquad \#\{n : \mathrm{Im}(\rho_{n,k}) \in [T-1, T+1]\} \ll \log\Big(\Big|\frac{1}{2}+iT\Big| + 2|k|\Big).$$

Note that $\tilde{\Phi}$ decays rapidly in vertical strips, say

$$\Big| \tilde{\Phi}\Big(\frac{1}{2}+iu\Big) \Big| \ll_{\Phi} \frac{1}{(1+|u|)^{100}},$$

which together with (4.6) gives

$$(4.7) \qquad \Big| \sum_n \tilde{\Phi}\Big(\frac{1}{2}+i\gamma_{k,n}\Big) \Big| \leq \sum_{j \in \mathbb{Z}} \sum_{n:j \leq \gamma_{k,n} < j+1} \Big| \tilde{\Phi}\Big(\frac{1}{2}+i\gamma_{k,n}\Big) \Big|$$

$$\ll_{\Phi} \sum_{j \in \mathbb{Z}} \frac{1}{(1+|j|)^{100}} \log(|2k|+|j|) \ll \log(2|k|).$$

Inserting (4.7) into Corollary 4.5 gives

$$\mathrm{Var}(\psi_{K,X}) \ll \frac{X}{K^2} \sum_{k>0} \Big| \widehat{f}\Big(\frac{k}{K}\Big) \Big|^2 (\log 2k)^2 \ll \frac{X}{K}(\log K)^2,$$

as claimed. ∎

4.3. PRIMES VS PRIME POWERS. We pass from a sum over prime ideals to a sum over all prime powers:

LEMMA 4.7: *Assume GRH. For $k \neq 0$ such that $\log|k| \ll \log X$,*

$$\sum_{\mathfrak{a}} \Lambda(\mathfrak{a})\Xi_k(\mathfrak{a})\Phi\Big(\frac{\mathrm{Norm}(\mathfrak{a})}{X}\Big) = \sum_{\mathfrak{p}\ prime} \Lambda(\mathfrak{p})\Xi_k(\mathfrak{p})\Phi\Big(\frac{\mathrm{Norm}(\mathfrak{p})}{X}\Big) + O(X^{1/3}).$$

Proof. We denote

$$\Sigma_{\text{prime}}(X, k, \Phi) := \sum_{\mathfrak{p} \text{ prime}} \Lambda(\mathfrak{p}) \Xi_k(\mathfrak{p}) \Phi\Big(\frac{\text{Norm}(\mathfrak{p})}{X}\Big)$$

and

$$\Sigma_{\text{all}}(X, k, \Phi) := \sum_{\mathfrak{a}} \Lambda(\mathfrak{a}) \Xi_k(\mathfrak{a}) \Phi\Big(\frac{\text{Norm}(\mathfrak{a})}{X}\Big).$$

Assuming GRH, we have

$$\Sigma_{\text{all}}(X, k, \Phi) \ll X^{1/2} \log(2|k|).$$

Indeed, from the Explicit Formula (Proposition 4.2), Lemma 4.3, and GRH we have

$$\Sigma_{\text{all}}(X, k, \Phi)$$

$$= - \sum_{\xi_k(\frac{1}{2}+i\gamma)=0} \tilde{\Phi}\Big(\frac{1}{2}+i\gamma\Big) X^{\frac{1}{2}+i\gamma} + \frac{1}{2\pi i} \int_{(2)} \Big\{ \frac{\Gamma'}{\Gamma}(s+2k) + \frac{\Gamma'}{\Gamma}(1-s+2k) \Big\} \tilde{\Phi}(s) X^s ds$$

$$\ll X^{1/2} \sum_{\xi_k(\frac{1}{2}+i\gamma)=0} \Big| \tilde{\Phi}\Big(\frac{1}{2}+i\gamma\Big) \Big| + \frac{X^{1/2} \log 2|k|}{(\log X)^{100}}$$

$$\ll X^{1/2} \log(2|k|)$$

on using the density of zeros of $L(s, \Xi_k)$ (4.2).

Next we crudely bound the contribution $\Sigma_{\geq 2}(X, k, \Phi)$ to $\Sigma_{\text{all}}(X, k, \Phi)$ of the higher prime powers $\mathfrak{p}^j$, $j \geq 2$:

$$\Sigma_{\geq 2}(X, k, \Phi) := \sum_{\mathfrak{p} \text{ prime}} \sum_{j \geq 2} \Lambda(\mathfrak{p}^j) \Xi_k(\mathfrak{p}^j) \Phi\Big(\frac{\text{Norm}(\mathfrak{p}^j)}{X}\Big)$$

$$\leq \sum_{\mathfrak{p} \text{ prime}} \log \text{Norm}(\mathfrak{p}) \sum_{j \geq 2} \Phi\Big(\frac{\text{Norm}(\mathfrak{p})^j}{X}\Big)$$

$$\ll \sum_{\substack{\mathfrak{p} \text{ prime} \\ \text{Norm}(\mathfrak{p}) \ll X^{1/2}}} \log \text{Norm}(\mathfrak{p}) \frac{\log X}{\log \text{Norm}(\mathfrak{p})}$$

$$\ll X^{1/2}.$$

Therefore we obtain a crude a priori bound on the contribution of primes:

$$(4.8) \qquad \Sigma_{\text{prime}}(X, k, \Phi) = \Sigma_{\text{all}}(X, k, \Phi) - \Sigma_{\geq 2}(X, k, \Phi) \ll X^{1/2} \log(2|k|).$$

We now seek a more refined estimate. In the sum $\Sigma_{\mathrm{all}}(X, k, \Phi)$ over all prime powers, we separately treat the contributions of primes, of squares of primes, and of higher powers:

$$\Sigma_{\mathrm{all}}(X, k, \Phi) = \Sigma_{\mathrm{prime}}(X, k, \Phi) + \Sigma_2(X, k, \Phi) + \Sigma_{\geq 3}(X, k, \Phi),$$

where

$$\Sigma_{\geq 3}(X, k, \Phi) := \sum_{\mathfrak{p}\,\mathrm{prime}} \sum_{j \geq 3} \Lambda(\mathfrak{p}^j) \Xi_k(\mathfrak{p}^j) \Phi\Big(\frac{\mathrm{Norm}(\mathfrak{p}^j)}{X}\Big)$$

and

$$\Sigma_2(X, k, \Phi) = \sum_{\mathfrak{p}\,\mathrm{prime}} \Lambda(\mathfrak{p}^2) \Xi_k(\mathfrak{p}^2) \Phi\Big(\frac{\mathrm{Norm}(\mathfrak{p}^2)}{X}\Big)$$

$$= \sum_{\mathfrak{p}\,\mathrm{prime}} \log \mathrm{Norm}(\mathfrak{p}) \Xi_{2k}(\mathfrak{p}) \Phi\Big(\frac{\mathrm{Norm}(\mathfrak{p})^2}{X}\Big).$$

By definition,

$$\Sigma_2(X, k, \Phi) = \Sigma_{\mathrm{prime}}(X^{1/2}, 2k, \Phi_2)$$

where $\Phi_2(u) = \Phi(u^2)$. Therefore inputting the a priori bound (4.8) (which uses GRH to get cancellation) gives

$$\Sigma_2(X, k, \Phi) \ll X^{1/4} \log(2|k|).$$

For the contribution of higher powers, we use

$$\Sigma_{\geq 3}(X, k, \Phi) \ll \sum_{\mathfrak{p}\,\mathrm{prime}} \log \mathrm{Norm}(\mathfrak{p}) \sum_{j \geq 3} \Phi\Big(\frac{\mathrm{Norm}(\mathfrak{p})^j}{X}\Big)$$

$$\ll \sum_{\substack{\mathfrak{p}\,\mathrm{prime} \\ \mathrm{Norm}(\mathfrak{p}) \ll X^{1/3}}} \log \mathrm{Norm}(\mathfrak{p}) \frac{\log X}{\log \mathrm{Norm}(\mathfrak{p})}$$

$$\ll X^{1/3}.$$

Thus we obtain

$$\Sigma_{\mathrm{all}}(X, k, \Phi) = \Sigma_{\mathrm{prime}}(X, k, \Phi) + O(X^{1/4} \log(2|k|)) + O(X^{1/3}),$$

which gives us the result since $\log |k| \ll \log X$. ∎

LEMMA 4.8: *Assume GRH. Then*

$$\langle |\psi_{K,X} - \psi_{K,X}^{prime}|^2 \rangle \ll \frac{X^{2/3}}{K}.$$

Proof. We use Lemma 4.1 to write

$$\psi_{K,X}(\theta) - \psi_{K,X}^{\text{prime}}(\theta) = \frac{1}{K}\sum_k e^{-i4k\theta}\widehat{f}\Big(\frac{k}{K}\Big)\sum_{\mathfrak{a}\neq\text{prime}}\Lambda(\mathfrak{a})\Phi\Big(\frac{\text{Norm}\,\mathfrak{a}}{X}\Big)\Xi_k(\mathfrak{a}).$$

The term $k = 0$ is the difference between mean values, which by Lemma 3.1 is $O(X^{1/2}/K)$. Hence

$$\psi_{K,X}(\theta) - \psi_{K,X}^{\text{prime}}(\theta)$$
$$= \frac{1}{K}\sum_{k\neq 0} e^{-i4k\theta}\widehat{f}\Big(\frac{k}{K}\Big)\sum_{\mathfrak{a}\neq\text{prime}}\Lambda(\mathfrak{a})\Phi\Big(\frac{\text{Norm}\,\mathfrak{a}}{X}\Big)\Xi_k(\mathfrak{a}) + O\Big(\frac{X^{1/2}}{K}\Big)$$
$$= I + O\Big(\frac{X^{1/2}}{K}\Big)$$

say. Hence it suffices to show that $\langle I^2 \rangle \ll X^{2/3}/K$.

We have

$$\langle I^2 \rangle = \frac{1}{K^2}\sum_{k\neq 0}\widehat{f}\Big(\frac{k}{K}\Big)^2 \Big|\sum_{\mathfrak{a}\neq\text{prime}}\Lambda(\mathfrak{a})\Phi\Big(\frac{\text{Norm}\,\mathfrak{a}}{X}\Big)\Xi_k(\mathfrak{a})\Big|^2.$$

By Lemma 4.7, the sum over $\mathfrak{a}$ non-prime is $O(X^{1/3})$ (assuming $\log K \ll \log X$), and therefore

$$\langle I^2 \rangle \ll \frac{1}{K^2}\sum_{k\neq 0}\widehat{f}\Big(\frac{k}{K}\Big)^2 X^{2/3} \ll \frac{X^{2/3}}{K}$$

as desired. ∎

4.4. PROOF OF THEOREM 3.2. We want to show that

$$\text{Var}(\psi_{K,X}^{\text{prime}}) = ||\psi_{K,X}^{\text{prime}} - \langle\psi_{K,X}^{\text{prime}}\rangle||_2^2 \ll \frac{X}{K}(\log K)^2,$$

where

$$||f||_2^2 = \frac{1}{\pi/2}\int_0^{\pi/2}|f(\theta)|^2 d\theta$$

is the standard L^2 norm on $[0, \pi/2]$.

Using the triangle inequality, we have

$$||\psi_{K,X}^{\text{prime}} - \langle\psi_{K,X}^{\text{prime}}\rangle||_2 \leq ||\psi_{K,X}^{\text{prime}} - \psi_{K,X}||_2 + ||\psi_{K,X} - \langle\psi_{K,X}\rangle||_2$$
$$+ |\langle\psi_{K,X}\rangle - \langle\psi_{K,X}^{\text{prime}}\rangle|.$$

By Lemma 4.8

$$||\psi_{K,X}^{\text{prime}} - \psi_{K,X}||_2 = \langle|\psi_{K,X} - \psi_{K,X}^{\text{prime}}|^2\rangle^{1/2} \ll \left(\frac{X^{2/3}}{K}\right)^{1/2};$$

by Corollary 4.6,

$$||\psi_{K,X} - \langle\psi_{K,X}\rangle||_2 = (\text{Var}(\psi_{K,X}))^{1/2} \ll \left(\frac{X}{K}(\log K)^2\right)^{1/2},$$

and by Lemma 3.1, the mean values are close:

$$|\langle\psi_{K,X}\rangle - \langle\psi_{K,X}^{\text{prime}}\rangle| \ll \frac{X^{1/2}}{K}.$$

Thus we obtain

$$||\psi_{K,X}^{\text{prime}} - \langle\psi_{K,X}^{\text{prime}}\rangle||_2 \ll \left(\frac{X^{2/3}}{K}\right)^{1/2} + \left(\frac{X}{K}(\log K)^2\right)^{1/2} + \frac{X^{1/2}}{K}$$
$$\ll \left(\frac{X}{K}(\log K)^2\right)^{1/2},$$

hence

$$\text{Var}(\psi_{K,X}^{\text{prime}}) \ll \frac{X}{K}(\log K)^2$$

which proves Theorem 3.2.   ∎

5. A random matrix theory model

In this section we present a conjecture for the variance of the smooth count $\psi_{K,X}$:

CONJECTURE 5.1:

$$\text{Var}(\psi_{K,X}) \sim c_2(f,\Phi)\frac{X}{K} \cdot \min(\log X, 2\log K)$$

where

$$c_2(f,\Phi) = \int_{-\infty}^{\infty} f(y)^2 dy \int_0^{\infty} \Phi(t)^2 dt.$$

Note that Conjecture 5.1 coincides with our result (3.3) in the trivial regime range $K \gg X$.

To recover Conjecture 1.2 from Conjecture 5.1, we can (at a heuristic level) pass to an actual count with sharp cutoffs: Take $f = \mathbf{1}_{[-1/2,1/2]}$ and $\Phi = \mathbf{1}_{(0,1]}$, and replace the weight $\Lambda(\mathfrak{p})$ by $\log X$ throughout, and ignore the contribution of higher powers of primes.

We use Corollary 4.5 with $X = K^\alpha$ for $\alpha > 0$, and note that since $\widehat{f}$ is even, and $\xi_{-k}(s) = \xi_k(s)$, we can pass to a sum over positive k's, to obtain

$$\text{(5.1)} \qquad \text{Var}(\psi_{K,X}) \sim \frac{2X}{K^2} \sum_{k>0} \widehat{f}\Big(\frac{k}{K}\Big)^2 \Big| \sum_j \tilde{\Phi}\Big(\frac{1}{2} + i\gamma_{k,j}\Big) e^{i\alpha \log K \gamma_{k,j}} \Big|^2,$$

the inner sums over all non-trivial zeros of $L(s, \Xi_k)$; we have ignored the remainder term in Corollary 4.5 as it can be seen to be $o(X/K)$ by using (4.7).

Let

$$\text{(5.2)} \qquad\qquad n := \frac{\alpha}{2} \frac{\log K}{\pi},$$

and

$$\mathcal{S}_n(\Xi_k) = \sum_j \tilde{\Phi}\Big(\frac{1}{2} + i\gamma_{k,j}\Big) e^{2\pi i n \gamma_{k,j}}.$$

Since the density of zeros of $L(s, \Xi_k)$ is about $\approx \log|k|$, the sum in $\mathcal{S}_n(\Xi_k)$ is over $O(\log K)$ zeros.

Conjecture 5.1 is clearly implied by

CONJECTURE 5.2: *Fix $\alpha > 0$. Then as $K \to \infty$,*

$$\text{(5.3)} \qquad\qquad \frac{2}{K} \sum_{k>0} \widehat{f}\Big(\frac{k}{K}\Big)^2 |\mathcal{S}_n(\Xi_k)|^2 \sim c_2(f, \Phi) \log K \min(\alpha, 2).$$

5.1. THE MODEL. We model the sum $\mathcal{S}_n(\Xi_k)$ by replacing the zeros of $L(s, \Xi_k)$ by the eigenvalues of a fictitious $N \times N$ (diagonal) unitary matrix

$$U = \text{diag}(e^{2\pi i \gamma_j})_{j=1,\ldots,N}.$$

We may want to require that U be symplectic,[2] in which case $N = 2g$ is even and the eigenphases γ_j will come in conjugate pairs $\gamma_{N-j} = -\gamma_j$, $j = 1, \ldots, g$.

We choose N so that the density of angles, namely N, matches the density of zeros of $L(s, \Xi_k)$ by requiring

$$\text{(5.4)} \qquad\qquad N \approx \frac{\log K}{\pi}.$$

We replace $\tilde{\Phi}(\frac{1}{2} + i\gamma)$ by a periodic function $w(\gamma) = w(\gamma + 1)$, to get a linear statistic

$$S_n(U) := \sum_{j=1}^N w(\gamma_j) e^{2\pi i n \gamma_j}.$$

---

[2] or orthogonal

Expanding $w(\gamma) = \sum_{\ell \in \mathbb{Z}} \widehat{w}(\ell) e^{2\pi i \ell \gamma}$ in a Fourier series we obtain

$$(5.5) \qquad S_n(U) = \sum_{\ell} \widehat{w}(\ell) \sum_j e^{2\pi i (n+\ell)\gamma_j} = \sum_m \widehat{w}(m-n) \operatorname{tr}(U^m).$$

We obtain the following model for the sum (5.3):

$$(5.3) \quad \longleftrightarrow \quad \frac{2}{K} \sum_{k>0} \widehat{f}\left(\frac{k}{K}\right)^2 |S_n(U_k)|^2,$$

where the unitary matrices U_k are picked uniformly and independently from a certain subgroup $G(N) \subseteq U(N)$ of unitary $N \times N$ matrices, $N \approx \frac{1}{\pi} \log K$, say $G(N) = U(N)$ is the full unitary group, or the symplectic group $G(N) = \mathrm{USp}(N)$ (possible only when N is even).

We now replace the discrete average

$$\frac{2}{K} \sum_{k>0} \widehat{f}\left(\frac{k}{K}\right)^2 H(U_k)$$

by the continuous average

$$c_f \int_{G(N)} H(U) dU$$

with respect to the Haar probability measure on $G(N)$, with c_f chosen so that the two averages coincide when the test function $H(U) \equiv 1$ is constant, that is

$$c_f := \lim_{K \to \infty} \frac{2}{K} \sum_{k>0} \widehat{f}\left(\frac{k}{K}\right)^2 = \int_{-\infty}^{\infty} f(y)^2 dy$$

(recalling that f is even and real valued). Therefore we model (5.3) by the matrix integral

$$(5.6) \qquad\qquad (5.3) \longleftrightarrow c_f \int_{G(N)} |S_n(U)|^2 dU,$$

where $n \approx N$ grows linearly with the matrix size N, precisely so that under the correspondence (5.4) and (5.2), $n \longleftrightarrow \frac{\alpha}{2} \frac{\log K}{\pi}$ is assumed to be an integer.

We claim that for all the classical groups $(G = U, \mathrm{USp}, O)$ under these conditions the answer is

PROPOSITION 5.3: *For* $G(N) = \mathrm{U}(N)$, $\mathrm{USp}(2N)$, $\mathrm{SO}(2N)$, *and* $n \approx N$, *as* $N \to \infty$

$$\int_{G(N)} |S_n(U)|^2 dU \sim \min(n, N) \int_0^1 |w(\gamma)|^2 d\gamma.$$

Therefore we are led to Conjecture 5.2, once we understand the analogue of $\int_0^1 |w(\gamma)|^2 d\gamma$: Recall that $w(\gamma)$ corresponded to $\tilde{\Phi}(\frac{1}{2} + i\gamma)$, which we can write in terms of $\phi(t) := \Phi(e^t)e^{t/2}$ as

$$\tilde{\Phi}\Big(\frac{1}{2} + i\gamma\Big) = \int_0^\infty \Phi(x)x^{\frac{1}{2}+i\gamma}\frac{dx}{x} = \int_{-\infty}^\infty \Phi(e^y)e^{y/2}e^{i\gamma y}dy = \widehat{\phi}\Big(-\frac{\gamma}{2\pi}\Big).$$

Hence $\int_0^1 |w(\gamma)|^2 d\gamma$ corresponds to

$$\int_{-\infty}^\infty \widehat{\phi}\Big(-\frac{\gamma}{2\pi}\Big)^2 d\gamma = 2\pi \int_{-\infty}^\infty \phi(t)^2 dt = 2\pi \int_0^\infty \Phi(x)^2 dx.$$

Thus we obtain Conjecture 5.2

$$(5.3) \sim c_f 2\pi \int_0^\infty \Phi(x)^2 dx \cdot \frac{\log K}{\pi} \min\Big(\frac{\alpha}{2}, 1\Big) = c_2(f, \Phi) \cdot \log K \min(\alpha, 2).$$

5.2. PROOF OF PROPOSITION 5.3.

Proof. We use the Fourier expansion (5.5) to obtain

$$\int_{G(N)} |S_n(U)|^2 dU = \sum_{m,m'} \widehat{w}(m-n)\overline{\widehat{w}(m'-n)} \int_{G(N)} \text{tr}(U^m)\overline{\text{tr}(U^{m'})}dU.$$

We trivially have $|\text{tr}\,U^m| \leq N$, and since $n \approx N$ and $\widehat{w}$ is rapidly decreasing, only the terms with say $m, m' = n + O(\log N)$ contribute anything non-negligible. Thus

$$\int_{G(N)} |S_n(U)|^2 dU \sim \sum_{m,m'=n+O(\log N)} \widehat{w}(m-n)\overline{\widehat{w}(m'-n)} \int_{G(N)} \text{tr}(U^m)\overline{\text{tr}(U^{m'})}dU.$$

THE UNITARY CASE $G(N) = U(N)$:

We use Dyson's lemma [3]

$$\int_{U(N)} \text{tr}(U^m)\overline{\text{tr}(U^{m'})}dU = \begin{cases} N^2, & m = m' = 0, \\ \delta(m,m')\min(|m|, N), & (m,m') \neq (0,0). \end{cases}$$

In particular, only the diagonal terms contribute. In our case, $m, m' \sim n$ are nonzero, hence we get

$$\int_{U(N)} |S_n(U)|^2 dU \sim \sum_{m=n+O(\log N)} |\widehat{w}(m-n)|^2 \min(|m|, N).$$

Since m varies very little around n, we can replace $\min(|m|, N)$ by $\min(n, N)$ with negligible error to obtain

$$\int_{U(N)} |S_n(U)|^2 dU \sim \min(n, N) \sum_{m=n+O(\log N)} |\widehat{w}(m-n)|^2$$

$$\sim \min(n, N) \sum_{\text{all } m} |\widehat{w}(m)|^2 = \min(n, N) \int_0^1 |w(\gamma)|^2 d\gamma$$

by Plancherel.

THE SYMPLECTIC CASE $G(N) = \mathrm{USp}(2g)$:

The expected values for the symplectic group ($N = 2g$) are [8, Lemma 2]:

(i) If $m = n$ then

$$\int_{\mathrm{USp}(2g)} |\operatorname{tr} U^n|^2 dU = \begin{cases} n + \eta(n), & 1 \le n \le g, \\ n - 1 + \eta(n), & g+1 \le n \le 2g, \\ 2g, & n > 2g. \end{cases}$$

(ii) If $1 \le m < n$ then

$$\int_{\mathrm{USp}(2g)} \operatorname{tr} U^m \operatorname{tr} U^n dU = \begin{cases} \eta(m)\eta(n), & m+n \le 2g, \\ \eta(m)\eta(n) - \eta(m+n), & m < n \le 2g, \ m+n > 2g, \\ -\eta(m+n), & n > 2g, \quad n-m \le 2g, \\ 0, & n-m > 2g, \end{cases}$$

and, in particular, if $m \ne m'$ (and neither is zero) then

$$(5.7) \qquad \int_{\mathrm{USp}(N)} \operatorname{tr}(U^m)\overline{\operatorname{tr}(U^{m'})} dU = O(1)$$

while for $m = m' \ne 0$ we obtain

$$(5.8) \qquad \int_{\mathrm{USp}(N)} |\operatorname{tr}(U^m)|^2 dU = \min(m, N) + O(1)$$

so that

$$\int_{\mathrm{USp}(N)} |S_n(U)|^2 dU \sim \sum_{m=n+O(\log N)} |\widehat{w}(m-n)|^2 \min(m, N)$$

$$+ \sum_{m,m'=n+O(\log N)} \widehat{w}(m-n)\overline{\widehat{w}(m'-n)}O(1).$$

The second term is $O(\log N)$, while the first is as in the unitary case, so that again we recover

$$\int_{\mathrm{USp}(N)} |S_n(U)|^2 dU \sim \min(n, N) \int_0^1 |w(\gamma)|^2 d\gamma.$$

For the orthogonal group $G(N) = \mathrm{SO}(N)$ with N even, we have the same result because (5.7), (5.8) are still valid (see [8, Lemma 2]).   ∎

6. A function field model

6.1. THE GROUP OF SECTORS. Our goal in this section is to formulate and prove an analogue of Conjecture 1.2 and of Conjecture 5.1 in the setting of the ring of polynomials over a finite field of q elements (q odd), in the limit of large q. Using the notation in the Introduction, we denote by[3]

$$\mathbb{S}_k^1 = \{f \in \mathbb{F}_q[S]/(S^k) : f(0) = 1, \ f(-S)f(S) = 1 \bmod S^k\}$$

the elements of unit norm and constant term 1 in $(\mathbb{F}_q[S]/(S^k))^\times$, and by

$$H_k := \{f \in (\mathbb{F}_q[S]/(S^k))^\times : f(-S) = f(S) \bmod S^k\}$$

the subgroup of even polynomials.

LEMMA 6.1 ([7, Lemma 2.1]):   (i) We have a direct product decomposition

$$(\mathbb{F}_q[S]/(S^k))^\times = H_k \times \mathbb{S}_k^1.$$

(ii) The order of $\mathbb{S}_k^1$ is

$$\#\mathbb{S}_k^1 = q^\kappa,$$

where

$$\kappa := k - 1 - \left\lfloor \frac{k-1}{2} \right\rfloor = \left\lfloor \frac{k}{2} \right\rfloor,$$

so that

$$k = \begin{cases} 2\kappa + 1, \\ 2\kappa. \end{cases}$$

---

[3] Katz [7, §2] denotes $B_{\mathrm{even}}^\times = H_k$, and $B_{\mathrm{odd}}^\times = \mathbb{S}_k^1$.

Proof. (i) is stated in [7] for k even, but the proof is valid for arbitrary $k \geq 1$.
　(ii) The order of H_k is

$$\#H_k = (q-1)q^{\lfloor \frac{k-1}{2} \rfloor}$$

since we can write any element of H_k as

$$h = \sum_{0 \leq 2j < k} h_j S^{2j} = \sum_{j=0}^{\lfloor \frac{k-1}{2} \rfloor} h_j S^{2j} \in H_k, \quad h_0 \neq 0$$

and the number of such elements is clearly $(q-1)q^{\lfloor \frac{k-1}{2} \rfloor}$. Since the order of $(\mathbb{F}_q[S]/(S^k))^\times$ is $(q-1)q^{k-1}$, we obtain that the order of $\mathbb{S}_k^1$ is

$$\#\mathbb{S}_k^1 = q^{k-1-\lfloor \frac{k-1}{2} \rfloor} = q^\kappa,$$

as claimed. ∎

　　We put an absolute value

$$|f| = q^{-\operatorname{ord}(f)}$$

on $\mathbb{F}_q[[S]]$, where $\operatorname{ord}(f) = \max(j : S^j \mid f)$. We then divide $\mathbb{S}^1$ into "sectors"

$$\operatorname{Sect}(u; k) = \{v \in \mathbb{S}^1 : |v - u| \leq q^{-k}\},$$

so that by definition, for $u, v \in \mathbb{S}^1 \subset \mathbb{F}_q[[S]]$

(6.1) $$v \in \operatorname{Sect}(u; k) \Leftrightarrow u = v \bmod S^k.$$

Consequently, the sectors $\operatorname{Sect}(u; k)$ are in bijection with the group $\mathbb{S}_k^1$, and their number is

$$K := \#\mathbb{S}_k^1 = q^\kappa.$$

Expanding in $\mathbb{F}_q[[S]]$:

$$u = \sum_{j=0}^{\infty} u_j S^j, \quad u_0 = 1,$$

and likewise for v, we see that $v \in \operatorname{Sect}(u; k)$ is equivalent to

$$v_j = u_j, \quad j = 1, \ldots, k-1.$$

　　We have a modular version of the homomorphism U from (1.4)

$$U_k : (\mathbb{F}_q[S]/(S^k))^\times \to \mathbb{S}_k^1, \quad f \mapsto \sqrt{f/\sigma(f)} \bmod S^k$$

whose kernel is H_k. Note that $f/\sigma(f) \in \mathbb{S}_k^1$ as it has unit norm and constant term 1, and in $\mathbb{S}_k^1$ the square root is well defined since $\mathbb{S}_k^1 = q^\kappa$ has odd order.

LEMMA 6.2: *The homomorphism $U_k : (\mathbb{F}_q[S]/(S^k))^\times \to \mathbb{S}_k^1$ is surjective.*

Proof. The kernel of $U_k : (\mathbb{F}_q[S]/(S^k))^\times \to \mathbb{S}_k^1$ is H_k because the kernel of $f \mapsto f/\sigma(f)$ is, by definition, H_k, and the square root map is an automorphism of $\mathbb{S}_k^1$. According to Lemma 6.1(i), the map is therefore onto. ∎

6.2. SUPER-EVEN CHARACTERS AND THEIR L-FUNCTIONS. A super-even character modulo S^k is a Dirichlet character

$$\Xi : (\mathbb{F}_q[S]/(S^k))^\times \to \mathbb{C}^\times$$

which is trivial on H_k. In particular, Ξ is even (trivial on the scalars $\mathbb{F}_q^\times$). These are the analogues of Hecke characters in §4.1. The group of super-even characters mod S^k is the character group of $(\mathbb{F}_q[S]/(S^k))^\times/H_k \simeq \mathbb{S}_k^1$. Hence by general orthogonality relations for characters of a finite Abelian group, the super-even characters separate the cosets of H_k, that is the elements of $\mathbb{S}_k^1$.

PROPOSITION 6.3: *For $f \in (\mathbb{F}_q[S]/(S^k))^\times$, and $u \in \mathbb{S}_k^1$, the following are equivalent:*

   (i) $U_k(f) \in \text{Sect}(u; k)$,
   (ii) $U_k(f) = U_k(u)$,
   (iii) $f \cdot H_k = u \cdot H_k$,
   (iv) $\Xi(f) = \Xi(u)$ *for all super-even characters mod S^k.*

Proof. For $u \in \mathbb{S}^1$ we have $U_k(u) = \sqrt{u/\sigma(u)} = \sqrt{u^2} = u \bmod S^k$, and so combining with (6.1) we find that $U_k(f) = U_k(u)$ is equivalent to $U_k(f) \in \text{Sect}(u; k)$.

According to Lemma 6.2, the map U_k is onto. Therefore, since the kernel of $U_k(u)$ is H_k, we obtain that $U_k(f) = U_k(u)$ is equivalent to $f \cdot H_k = u \cdot H_k$ in $(\mathbb{F}_q[S]/(S^k))^\times$.

Using the orthogonality relations for characters of $\mathbb{S}_k^1$ (super-even characters) we obtain the final equivalence. ∎

The Swan conductor of an even non-trivial character Ξ mod S^k is the maximal integer $d < k$ such that Ξ is non-trivial on the subgroup

$$\Gamma_d := (1 + (S^d))/(S^k) \subset (\mathbb{F}_q[S]/(S^k))^\times.$$

Then Ξ is a primitive character modulo $S^{d(\Xi)+1}$. For a super-even character, the Swan conductor is necessarily odd, since super-even characters are automatically trivial on Γ_d for d even.

Let Ξ be a non-trivial even character modulo S^k. The L-function associated to Ξ is

$$(6.2) \quad L(z,\Xi) = \sum_{f \text{ monic}} \Xi(f) z^{\deg f} = \prod_{P \text{ prime}} (1 - \Xi(P) z^{\deg P})^{-1}, \quad |z| < 1/q,$$

which for non-trivial even Ξ is a polynomial in z of degree exactly $d(\Xi)$ (the Swan conductor of Ξ), including a trivial zero at $z = 1$. Thus we write for any non-trivial super-even character

$$(6.3) \qquad\qquad L(z,\Xi) = (1 - z) \det(I - zq^{1/2}\Theta_\Xi)$$

for a unitary matrix $\Theta_\Xi \in U(N)$ ($N = d(\Xi) - 1$).

For any non-trivial super-even character mod S^k, let

$$\Psi(\nu;\Xi) := \sum_{\deg f = \nu} \Lambda(f)\Xi(f)$$

be the sum over all monic polynomials of degree ν, with $\Lambda(f)$ being the von Mangoldt function. The Explicit Formula (obtained by comparing the logarithmic derivative of (6.2) and (6.3); see, e.g., [9]) shows that for non-trivial super-even Ξ, the sum over prime powers $\Psi(\nu;\Xi)$ is a sum over zeros of the L-function associated to Ξ:

$$(6.4) \qquad\qquad \Psi(\nu;\Xi) = -q^{\nu/2}\operatorname{tr}\Theta_\Xi^\nu - 1.$$

6.3. A WEIGHTED COUNT. We introduce a weighted count in terms of the von Mangoldt function on $\mathbb{F}_q[S]$, defined as $\Lambda(f) = \deg \mathfrak{p}$ if $f = c\mathfrak{p}^j$ for some prime $\mathfrak{p} \in \mathbb{F}_q[S]$ and $j \geq 1$ and scalar $c \in \mathbb{F}_q^\times$, and $\Lambda(f) = 0$ otherwise. Set

$$\Psi_{k,\nu}(u) = \sum_{U(f)\in\operatorname{Sect}(u;k)} \Lambda(f),$$

the sum over monic $f \in \mathbb{F}_q[S]$ with $\deg f = \nu$ and $f(0) \neq 0$.

We want to average over all directions $u \in \mathbb{S}_k^1$. The mean value is

$$\mathbb{E}(\Psi_{k,\nu}) = \frac{1}{q^\kappa} \sum_{u\in\mathbb{S}_k^1} \Psi_{k,\nu}(u).$$

By definition, the sum is just the sum over all monic $f \in M_\nu$ (with $f(0)\neq 0$), that is

$$\mathbb{E}(\Psi_{k,\nu}) = \frac{1}{q^\kappa} \sum_{\substack{\deg f = \nu \\ f(0)\neq 0}} \Lambda(f) = \frac{1}{q^\kappa}\left(\sum_{\deg f = \nu} \Lambda(f) - 1 \right) = \frac{q^\nu - 1}{q^\kappa}$$

by the Prime Polynomial Theorem in $\mathbb{F}_q[S]$.

We use Proposition 6.3 to pick out prime powers lying in a given sector, and obtain a formula for the sum $\Psi_{k,\nu}(u)$ in terms of super-even characters.

LEMMA 6.4:

$$\Psi_{k,\nu}(u) - \frac{q^\nu - 1}{q^\kappa} = -\frac{q^{\nu/2}}{q^\kappa} \sum_{\Xi \neq \Xi_0} \overline{\Xi(u)} \operatorname{tr} \Theta_\Xi^\nu - \delta(u,1) + \frac{1}{q^\kappa},$$

the sum being over all non-trivial super-even characters mod S^k.

Proof. From Proposition 6.3 and the orthogonality relations we find

$$\frac{1}{q^\kappa} \sum_{\Xi \text{ super-even mod } S^k} \overline{\Xi(u)} \Xi(f) = \begin{cases} 1, & U(f) \in \operatorname{Sect}(u;k), \\ 0, & \text{otherwise,} \end{cases}$$

which gives

$$\Psi_{k,\nu}(u) = \sum_{\substack{\deg f = \nu \\ U_k(f) \in \operatorname{Sect}(u;k)}} \Lambda(f) = \frac{1}{q^\kappa} \sum_{\Xi \text{ super-even mod } S^k} \overline{\Xi(u)} \sum_{\deg f = \nu} \Lambda(f) \Xi(f),$$

with the sum over all monic $f \in \mathbb{F}_q[S]$ of degree ν. Hence

$$(6.5) \qquad \Psi_{k,\nu}(u) = \frac{1}{q^\kappa} \sum_{\Xi \text{ super-even mod } S^k} \overline{\Xi(u)} \Psi(\nu;\Xi).$$

The contribution of the trivial character Ξ_0 is

$$\frac{1}{q^\kappa} \sum_{\substack{\deg f = \nu \\ f(0) \neq 0}} \Lambda(f) = \frac{1}{q^\kappa} \left(\sum_{\deg f = \nu} \Lambda(f) - 1 \right) = \frac{q^\nu - 1}{q^\kappa}.$$

Inserting the Explicit Formula (6.4) gives

$$\Psi_{k,\nu}(u) - \frac{q^\nu - 1}{q^\kappa} = -\frac{1}{q^\kappa} \sum_{\substack{\Xi \text{ super-even mod } S^k \\ \Xi \neq \Xi_0}} \overline{\Xi(u)} (q^{\nu/2} \operatorname{tr} \Theta_\Xi^\nu + 1)$$

$$= -\frac{q^{\nu/2}}{q^\kappa} \sum_{\substack{\Xi \text{ super-even mod } S^k \\ \Xi \neq \Xi_0}} \overline{\Xi(u)} \operatorname{tr} \Theta_\Xi^\nu - \delta(u,1) + \frac{1}{q^\kappa}$$

on using the orthogonality relations in the form

$$\frac{1}{q^\kappa} \sum_{\Xi \neq \Xi_0} \overline{\Xi(u)} = \delta(u,1) - \frac{1}{q^\kappa}. \qquad \blacksquare$$

We use $|\operatorname{tr} \Theta_\Xi^\nu| \leq 2\kappa - 2$ for $\Xi \neq \Xi_0$ to obtain

COROLLARY 6.5: *As $q \to \infty$,*

$$\Psi_{k,\nu}(u) = \frac{q^\nu}{q^\kappa} + O(q^{\nu/2}).$$

Hence for $\kappa < \nu/2$, we obtain an asymptotic formula.

By a standard argument, this implies that $\mathcal{N}_{k,\nu}(u) = N/K + O(q^{\nu/2})$.

Remark 6.6: Note that for $\kappa > \nu/2$, it is no longer necessarily the case that $\Psi_{k,\nu}(u) \sim \frac{q^\nu}{q^\kappa}$, in fact there may not be any polynomials $g \in \mathbb{F}_q[S]$ of degree $\deg g = \nu < 2\kappa$ with direction $U(g) \in \mathrm{Sect}(u; k)$. As an example, assume that $k - 1$ is odd, take

$$u = \frac{1 + S^{k-1}}{1 - S^{k-1}} = 1 + 2S^{k-1} \bmod S^k$$

and suppose that $\deg g = \nu < 2\kappa \le k - 1$ satisfies

$$U(g) \in \mathrm{Sect}(u; k) = \mathrm{Sect}(1 + 2S^{k-1}; k).$$

By Proposition 6.3, this is equivalent to $g \in (1 + 2S^{k-1})H_k$. Reducing modulo S^{k-1} gives $g \in H_{k-1}$, so that $g(-S) = g(S) \bmod S^{k-1}$. But $\deg g < k - 1$ hence $g(-S) = g(S)$, that is g is an even polynomial, hence $U(g) = 1$. But then $U(g) = 1 \notin \mathrm{Sect}(1 + 2S^{k-1}; k)$, a contradiction.

6.4. THE VARIANCE OF $\Psi_{k,\nu}$. The variance of $\Psi_{k,\nu}$ is

$$\mathrm{Var}(\Psi_{k,\nu}) = \frac{1}{q^\kappa} \sum_{u \in \mathbb{S}_k^1} \left| \Psi_{k,\nu}(u) - \frac{q^\nu - 1}{q^\kappa} \right|^2.$$

THEOREM 6.7: *Assume q is odd, and $\kappa \ge 3$, or that $\kappa = 2$ and additionally $5 \nmid q$. Then as $q \to \infty$,*

$$\mathrm{Var}(\Psi_{k,\nu}) \sim q^{\nu - \kappa} \begin{cases} \nu + \eta(\nu), & 1 \le \nu \le \kappa - 1, \\ \nu - 1 + \eta(\nu), & \kappa \le \nu \le 2(\kappa - 1), \\ 2\kappa - 2, & \nu > 2\kappa - 2. \end{cases}$$

In other words, if we denote $X = q^\nu$ the number of all monics of degree ν, then

$$\frac{\mathrm{Var}(\Psi_{k,\nu})}{X/K} \sim \begin{cases} \log_q X - 1 + \eta(\log_q X), & \frac{1}{2} \log_q X + \frac{1}{2} < \log_q K \le \log_q X, \\ 2 \log_q K - 2, & \log_q K \le \frac{1}{2} \log_q X + \frac{1}{2}. \end{cases}$$

This is to be compared with Conjecture 5.1. Note that the range $\nu < \kappa$ is the "trivial regime", where there are more sectors than directions; in that case the result is elementary, but of little interest.

LEMMA 6.8:

$$\mathrm{Var}(\Psi_{k,\nu}) = q^{\nu-\kappa}\left(\frac{1}{q^\kappa}\sum_{\Xi\neq\Xi_0}|\operatorname{tr}\Theta_\Xi^\nu|^2\right)\cdot(1+O(\kappa q^{-\nu/2}))$$

the sum over all non-trivial super-even characters mod S^k.

Proof. Inserting (6.5) we find

$$\mathrm{Var}(\Psi_{k,\nu}) = \frac{1}{q^\kappa}\sum_{u\in\mathbb{S}_k^1}\left|\frac{1}{q^\kappa}\sum_{\substack{\Xi \text{ super-even mod } S^k \\ \Xi\neq\Xi_0}}\overline{\Xi(u)}\Psi(\nu;\Xi)\right|^2$$

$$= \frac{1}{q^{2\kappa}}\sum_{\substack{\Xi_1,\Xi_2 \text{ super-even mod } S^k \\ \Xi_1,\Xi_2\neq\Xi_0}}\Psi(\nu;\Xi_1)\overline{\Psi(\nu;\Xi_2)}\frac{1}{q^\kappa}\sum_{u\in\mathbb{S}_k^1}\overline{\Xi_1(u)}\Xi_2(u).$$

We use the orthogonality relations in the group of super-even characters, which is the character group of $\mathbb{S}_k^1$:

$$\frac{1}{q^\kappa}\sum_{u\in\mathbb{S}_k^1}\overline{\Xi_1(u)}\,\Xi_2(u) = \delta(\Xi_1,\Xi_2).$$

This gives

$$\mathrm{Var}(\Psi_{k,\nu}) = \frac{1}{q^{2\kappa}}\sum_{\substack{\Xi \text{ super-even mod } S^k \\ \Xi\neq\Xi_0}}|\Psi(\nu;\Xi)|^2.$$

Set $c(u) = \delta(u,1) - \frac{1}{q^\kappa}$. From Lemma 6.4 we obtain, on denoting by $\langle\bullet\rangle_{\mathbb{S}^1}$ the average over all $u\in\mathbb{S}_k^1$, that

$$\mathrm{Var}(\Psi_{k,\nu}) = \frac{q^\nu}{q^{2\kappa}}\sum_{\Xi_1\neq\Xi_0}\sum_{\Xi_2\neq\Xi_0}\operatorname{tr}\Theta_{\Xi_1}^\nu\,\overline{\operatorname{tr}\Theta_{\Xi_2}^\nu}\langle\overline{\Xi_1(u)}\,\Xi_2(u)\rangle_{\mathbb{S}^1}$$

$$+ 2\frac{q^{\nu/2}}{q^\kappa}\operatorname{Re}\sum_{\Xi\neq\Xi_0}\operatorname{tr}(\Theta_\Xi^\nu)\langle\overline{\Xi(u)}c(u)\rangle_{\mathbb{S}^1} + \langle c(u)^2\rangle_{\mathbb{S}^1}.$$

Using the orthogonality relations, the averages over $u \in \mathbb{S}^1$ are

$$\langle \overline{\Xi_1(u)} \, \Xi_2(u) \rangle_{\mathbb{S}^1} = \delta(\Xi_1, \Xi_2),$$

$$\langle \overline{\Xi(u)} c(u) \rangle_{\mathbb{S}^1} = \langle \overline{\Xi(u)} \delta(u, 1) \rangle_{\mathbb{S}^1} - \frac{1}{q^\kappa} \langle \overline{\Xi(u)} \rangle_{\mathbb{S}^1}$$

$$= \frac{1}{q^\kappa} \overline{\Xi(1)} - \frac{1}{q^\kappa} \delta(\Xi, \Xi_0) = \frac{1}{q^\kappa},$$

since $\Xi \neq \Xi_0$, and

$$\langle c(u)^2 \rangle_{\mathbb{S}^1} = \frac{1}{q^\kappa} \left(1 - \frac{1}{q^\kappa} \right).$$

Substituting into our formula gives

$$\mathrm{Var}(\Psi_{k,\nu}) = q^{\nu - \kappa} \frac{1}{q^\kappa} \sum_{\Xi \neq \Xi_0} |\operatorname{tr} \Theta_\Xi^\nu|^2$$

$$+ 2 \frac{q^{\nu/2}}{q^{2\kappa}} \operatorname{Re} \sum_{\Xi \neq \Xi_0} \operatorname{tr}(\Theta_\Xi^\nu) + \frac{1}{q^\kappa} \left(1 - \frac{1}{q^\kappa} \right).$$

Finally we use $|\operatorname{tr} \Theta_\Xi^\nu| \leq 2\kappa - 2$ for $\Xi \neq \Xi_0$ to get our claim. ∎

Hence we get an inequality (for all κ and ν)

COROLLARY 6.9:

$$\mathrm{Var}(\Psi_{k,\nu}) \lesssim q^{\nu - \kappa} (2\kappa - 2)^2.$$

This is analogous to Theorem 3.2. To do better, we invoke an equidistribution result for the zeros of these L-functions.

6.5. PROOF OF THEOREM 6.7. We use Lemma 6.8. We separate the characters according to their Swan conductor, which is necessarily an odd integer $d(\Xi) < k$, whose maximal value is $2\kappa - 1$ (recall $k = 2\kappa$ or $2\kappa + 1$). Characters with such maximal conductor make up all primitive super-even characters modulo $S^{2\kappa}$. As in [9], the contribution of characters with smaller Swan conductor $d(\Xi) < 2\kappa - 1$ is negligible, and up to lower order terms one finds

$$(6.6) \qquad \mathrm{Var}(\Psi_{k,\nu}) \sim q^{\nu - \kappa} \frac{1}{\#} \sum_{\substack{\Xi \text{ super-even mod } S^{2\kappa} \\ \text{primitive}}} |\operatorname{tr} \Theta_\Xi^\nu|^2,$$

the average over all primitive super-even characters modulo $S^{2\kappa}$.

Katz [7, Theorem 5.1] showed that for any sequence of odd[4] $q \to \infty$, the Frobenii

$$\{\Theta_\Xi : \Xi \text{ primitive super-even mod } S^{2\kappa}\}$$

become uniformly distributed in the unitary symplectic group $\mathrm{USp}(2\kappa - 2)$ provided $2\kappa - 2 \geq 4$, and that the same holds for $2\kappa - 2 = 2$ if the q are coprime to 10 (i.e., the characteristic of $\mathbb{F}_q$ is not 2 or 5). Katz's equidistribution theorem allows us to replace the average over primitive super-even characters in (6.6) by the corresponding continuous average over the unitary symplectic group $\mathrm{USp}(2\kappa - 2)$, to get

$$\mathrm{Var}(\Psi_{k,\nu}) \sim q^{\nu - \kappa} \int_{\mathrm{USp}(2\kappa-2)} |\operatorname{tr}(U^\nu)|^2 dU.$$

The matrix integral equals, for $\nu > 0$ [8, Lemma 2],

$$\int_{\mathrm{USp}(2\kappa-2)} |\operatorname{tr}(U^\nu)|^2 dU = \begin{cases} \nu + \eta(\nu), & 1 \leq \nu \leq \kappa - 1, \\ \nu - 1 + \eta(\nu), & \kappa \leq \nu \leq 2(\kappa - 1), \\ 2\kappa - 2, & \nu > 2\kappa - 2, \end{cases}$$

where $\eta(\nu) = 1$ for ν even, and equals 0 for ν odd. This proves Theorem 6.7.

6.6. RELATION BETWEEN VARIANCE OF $\mathcal{N}_{k,\nu}$ AND $\Psi_{k,\nu}$. We can now proceed to prove Theorem 1.3, which follows from Theorem 6.7 once we establish the following relation between the variance of $\mathcal{N}_{k,\nu}$ and of $\Psi_{k,\nu}$:

PROPOSITION 6.10: *Under the conditions of Theorem 6.7,*

$$\mathrm{Var}(\mathcal{N}_{k,\nu}) \sim \frac{1}{\nu^2} \mathrm{Var}(\Psi_{k,\nu})$$

as $q \to \infty$.

Let $\mathbf{1}_{\mathrm{Sect}(u;k)}$ be the indicator function of the sector $\mathrm{Sect}(u;k)$. We write

$$\begin{aligned} \Psi_{k,\nu}(u) &= \sum_{\deg f = \nu} \Lambda(f) \mathbf{1}_{\mathrm{Sect}(u;k)}(U(f)) \\ &= \nu \sum_{\substack{\deg P = \nu \\ \text{prime}}} \mathbf{1}_{\mathrm{Sect}(u;k)}(U(P)) + R_{k,\nu}(u) \\ &= \nu \mathcal{N}_{k,\nu}(u) + R_{k,\nu}(u) \end{aligned}$$

---

[4] In [7, Theorem 5.1], q is allowed to be even for $2\kappa - 2 \geq 6$.

with the sums over monic polynomials, where

$$R(u) = R_{k,\nu}(u) = \sum_{\substack{\deg f = \nu \\ f \text{ not prime}}} \Lambda(f) \mathbf{1}_{\text{Sect}(u;k)}(U(f)).$$

We subtract the expected value of Ψ, which is

$$\langle \Psi \rangle = \frac{q^\nu - 1}{q^\kappa},$$

where we write $\langle \bullet \rangle$ for the average over all sectors $u \in \mathbb{S}_k^1$. Compare this with the expected value of $\mathcal{N} = \mathcal{N}_{k,\nu}$, which is

$$\langle \mathcal{N} \rangle = \frac{N}{q^\kappa} = \frac{q^\nu}{\nu q^\kappa} + O\left(\frac{q^{\nu/2}}{\nu q^\kappa} \right)$$

by the Prime Polynomial Theorem. Therefore

(6.7) $$\Psi_{k,\nu}(u) - \langle \Psi \rangle = \nu \cdot (\mathcal{N}(u) - \langle \mathcal{N} \rangle) + R(u) + O\left(\frac{q^{\nu/2}}{q^\kappa} \right).$$

We claim that the mean square of R is bounded by

LEMMA 6.11:

$$\langle R^2 \rangle := \frac{1}{q^\kappa} \sum_{u \in \mathbb{S}_k^1} R(u)^2 \ll q^{\nu - 2\kappa} + q^{\frac{2}{3}\nu - \kappa}.$$

This bound is certainly negligible compared to the variance of $\Psi_{k,\nu}$, which by Theorem 6.7 is of order $q^{\nu - \kappa}$. Using (6.7) gives

$$|\nu^2 \langle |(\mathcal{N} - \langle N \rangle|^2 \rangle - \langle |\Psi - \langle \Psi \rangle|^2 \rangle| \ll \langle R^2 \rangle + O\left(\frac{q^\nu}{q^{2\kappa}} \right),$$

and we obtain

$$\nu^2 \operatorname{Var}(\mathcal{N}) = \operatorname{Var}(\Psi) + O(q^{\nu - \kappa}(q^{-\kappa} + q^{-\nu/3})).$$

Hence by Theorem 6.7

$$\operatorname{Var}(\mathcal{N}) \sim \frac{1}{\nu^2} \operatorname{Var}(\Psi)$$

as $q \to \infty$.

6.7. PROOF OF LEMMA 6.11. To prove Lemma 6.11 we write

$$\langle R^2 \rangle = \sum_{\substack{\deg f, \deg g = \nu \\ \text{not prime}}} \Lambda(f)\Lambda(g)\langle \mathbf{1}_{\text{Sect}(u;k)}(U(f))\mathbf{1}_{\text{Sect}(u;k)}(U(g))\rangle.$$

We compute

$$\langle \mathbf{1}_{\text{Sect}(u;k)}(U(f))\mathbf{1}_{\text{Sect}(u;k)}(U(g))\rangle = \frac{1}{q^\kappa} \sum_{u \in \mathbb{S}^1_k} \mathbf{1}_{\text{Sect}(u;k)}(U(f))\mathbf{1}_{\text{Sect}(u;k)}(U(g))$$

$$= \begin{cases} \frac{1}{q^\kappa}, & U(f) = U(g) \bmod S^k, \\ 0, & \text{otherwise.} \end{cases}$$

By Proposition 6.3, the condition $U(f) = U(g) \bmod S^k$ is equivalent to

$$\Xi(f) = \Xi(g)$$

for all super-even characters modulo S^k, that is

$$\langle \mathbf{1}_{\text{Sect}(u;k)}(U(f))\mathbf{1}_{\text{Sect}(u;k)}(U(g))\rangle = \frac{1}{q^\kappa} \cdot \frac{1}{q^\kappa} \sum_{\Xi \text{ super-even mod } S^k} \overline{\Xi(f)}\,\Xi(g).$$

Therefore

$$\langle R^2 \rangle = \sum_{\substack{\deg f, \deg g = \nu \\ \text{not prime}}} \Lambda(f)\Lambda(g)\frac{1}{q^{2\kappa}} \sum_{\Xi \text{ super-even mod } S^k} \overline{\Xi(f)}\,\Xi(g)$$

$$(6.8) \qquad = \frac{1}{q^{2\kappa}} \sum_{\Xi \text{ super-even mod } S^k} \left| \sum_{\substack{\deg f = \nu \\ \text{not prime}}} \Lambda(f)\Xi(f) \right|^2$$

$$= \frac{1}{q^{2\kappa}} \sum_{\Xi \text{ super-even mod } S^k} |B(\nu, \Xi)|^2,$$

where

$$B(\nu, \Xi) := \sum_{\substack{\deg f = \nu \\ \text{not prime}}} \Lambda(f)\Xi(f).$$

We will show below that if $\Xi = 1$, then

$$(6.9) \qquad\qquad\qquad B(\nu, 1) \ll_\nu q^{\nu/2},$$

and if $\Xi \neq 1$, then

$$(6.10) \qquad\qquad\qquad |B(\nu, \Xi)| \ll_\nu q^{\nu/3}.$$

Assuming (6.9) and (6.10), we use the expansion (6.8) for $\langle R^2 \rangle$, and insert the bounds (6.9) for $\Xi = 1$, and (6.10) for $\Xi \neq 1$ to obtain

$$\langle R^2 \rangle \ll q^{\nu - 2\kappa} + q^{\frac{2}{3}\nu - \kappa}$$

proving Lemma 6.11.

It remains to prove (6.9) and (6.10). We set

$$A(\nu, \Xi) := \sum_{\substack{\deg P = \nu \\ P \text{ prime}}} \nu \, \Xi(P)$$

so that

(6.11)
$$B(\nu, \Xi) = \sum_{\substack{\delta \mid \nu \\ \delta < \nu}} A(\delta, \Xi^{\nu/\delta}).$$

The trivial bound for $A(\nu, \Xi)$ is

$$|A(\nu, \Xi)| \leq A(\nu, 1) = \nu \#\{P \text{ prime, } \deg P = \nu\} \leq q^\nu.$$

This gives (6.9), because

$$B(\nu, 1) = \sum_{\substack{\delta \mid \nu \\ \delta < \nu}} A(\delta, 1) \leq \sum_{\substack{\delta \mid \nu \\ \delta < \nu}} q^\delta \ll_\nu q^{\nu/2}$$

since the largest divisor $\delta \mid \nu$ which is smaller than ν is not larger than $\nu/2$.

If $\Xi \neq 1$ then we have a better bound:

(6.12)
$$|A(\nu, \Xi)| \ll_\nu q^{\nu/2}, \quad \Xi \neq 1.$$

Indeed, write

$$A(\nu, \Xi) = \Psi(\nu, \Xi) - B(\nu, \Xi),$$

and then use the trivial bound (6.9):

$$|B(\nu, \Xi)| \ll q^{\nu/2}$$

and (6.4):

$$|\Psi(\nu, \Xi)| \ll q^{\nu/2},$$

to obtain (6.12).

Next, we use the expansion (6.11) of $B(\nu, \Xi)$ to write

$$|B(\nu, \Xi)| \leq \sum_{\substack{\delta \mid \nu, \ \delta < \nu \\ \Xi^{\nu/\delta} = 1}} A(\delta, 1) + \sum_{\substack{\delta \mid \nu, \ \delta < \nu \\ \Xi^{\nu/\delta} \neq 1}} |A(\delta, \Xi^{\nu/\delta})|.$$

To bound the contribution of divisors δ with $\Xi^{\nu/\delta} = 1$, note that the order of Ξ divides $\#\mathbb{S}^1 = q^\kappa$, so that if $\Xi \neq 1$ but $\Xi^{\nu/\delta} = 1$ then necessarily $p \mid \nu/\delta$, where $q = p^r$ with p an odd prime (since q is odd). Hence using the trivial bound $A(\delta, 1) \leq q^\delta$ gives

$$\sum_{\substack{\delta \mid \nu, \ \delta < \nu \\ \Xi^{\nu/\delta} = 1}} A(\delta, 1) \leq \sum_{\substack{\delta \mid \nu \\ p \mid \frac{\nu}{\delta}}} q^\delta.$$

Now if $p \mid \frac{\nu}{\delta}$, then $\delta \mid \frac{\nu}{p}$ so $\delta \leq \frac{\nu}{p}$, and we obtain

$$\sum_{\substack{\delta \mid \nu, \ \delta < \nu \\ \Xi^{\nu/\delta} = 1}} A(\delta, 1) \ll_\nu q^{\nu/p}.$$

We bound the contribution of divisors δ with $\Xi^{\nu/\delta} \neq 1$, using (6.12), by

$$\sum_{\substack{\delta \mid \nu, \ \delta < \nu \\ \Xi^{\nu/\delta} \neq 1}} |A(\delta, \Xi^{\nu/\delta})| \ll_\nu \sum_{\delta \mid \nu, \ \delta < \nu} q^{\delta/2} \ll q^{\nu/4},$$

again using that the largest divisor $\delta \mid \nu$ which is smaller than ν is not larger than $\nu/2$. Thus we find that for $\Xi \neq 1$,

$$|B(\nu, \Xi)| \ll_\nu q^{\nu/p} + q^{\nu/4}$$

which proves (6.10) since $p \geq 3$.

References

[1] L. Bary-Soroker, Y. Smilansky and A. Wolf, *On the function field analogue of Landau's theorem on sums of squares*, Finite Fields and their Applications **39** (2016), 195–215.

[2] H. M. Bui, J. P. Keating and D. J. Smith, *On the variance of sums of arithmetic functions over primes in short intervals and pair correlation for L-functions in the Selberg class*, Journal fo the London Mathematical Society **94** (2016), 161–185.

[3] F. J. Dyson, *Statistical theory of the energy levels of complex systems, I, II and III*, Journal of Mathematical Physics **3** (1962), 140–175.

[4] G. Harman and P. A. Lewis, *Gaussian primes in narrow sectors*, Mathematika **48** (2001), 119–135.

[5] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen. I*, Mathematische Zeitschrift **1** (1918), 357–376; *II*, Mathematische Zeitschrift **6** (1920), 11–51.

[6] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society Colloquium Publications, Vol. 53, American Mathematical Society, Providence, RI, 2004.

[7] N. M. Katz, *Witt vectors and a question of Rudnick and Waxman*, International Mathematics Research Notices **2017** (2017), 3377–3412.

[8] J. P. Keating and B. E. Odgers, *Symmetry transitions in random matrix theory & L-functions*, Communications in Mathematical Physics **281** (2008), 499–528.

[9] J. Keating and Z. Rudnick, *The variance of the number of prime polynomials in short intervals and in residue classes*, International Mathematics Research Notices **2014** (2014), 259–288.

[10] F. B. Koval'chik, *Density theorems for sectors and progressions*, Lietuvos Matematikos Rinkinys **15** (1975), 133–151.

[11] I. Kubilyus, *The distribution of Gaussian primes in sectors and contours*, Leningradskiĭ Gosudarstvennyĭ Ordena Lenina Universitet imeni A. A. Zhdanova. Uchenye Zapiski. Seriya Matematicheskikh Nauk **137** (1950), 40–52.

[12] J. Kubilius, *On a problem in the n-dimensional analytic theory of numbers*, Vilniaus Valst. Univ. Mokslo Darbai. Mat. Fiz. Chem. Mokslu Ser. **4** (1955), 5–43.

[13] P. Lévy, *Sur la division d'un segment par des points choisis au hasard*, Comptes rendus hebdomadaires des séances de l'Académie des Sciences **208** (1939), 147–149.

[14] M. Maknys, *Zeros of Hecke Z-functions and the distribution of primes of an imaginary quadratic field*, Lithuanian Mathematical Journal **15** (1975), 140–149.

[15] M. Maknys, *Density theorems for Hecke Z functions and the distribution of primes of an imaginary quadratic field*, Lithuanian Mathematical Journal **16** (1976), 105–110.

[16] M. Maknys, *Refinement of the remainder term in the law of the distribution of prime numbers of an imaginary quadratic field in sectors*, Lithuanian Mathematical Journal **17** (1977), 90–93.

[17] O. Parzanchevski and P. Sarnak, *Super-golden-gates for PU(2)*, Advances in Mathematics **327** (2018), 869–901.