ZEROS OF FEKETE POLYNOMIALS

Brian Conrey, Andrew Granville,
Bjorn Poonen and K. Soundararajan

1. Introduction

Dirichlet noted that, from the formula

$$\Gamma(s) = n^s \int_0^\infty x^{s-1} e^{-nx} dx = n^s \int_0^1 (-\log t)^{s-1} t^{n-1} dt,$$

we may obtain the identity

$$\begin{aligned}\Gamma(s)L(s,(\tfrac{\cdot}{p})) = \Gamma(s)\sum_{n\ge 1}\frac{\left(\frac{n}{p}\right)}{n^s} &= \int_0^1 (-\log t)^{s-1}\sum_{n\ge 1}\left(\frac{n}{p}\right)t^{n-1}dt \\ &= \int_0^1 \frac{(-\log t)^{s-1}}{t}\frac{f_p(t)}{1-t^p}dt. \qquad (1.1)\end{aligned}$$

Here $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol and

$$f_p(t) := \sum_{a=0}^{p-1}\left(\frac{a}{p}\right)t^a. \qquad (1.2)$$

Equation (1.1) allowed Dirichlet to define $L(s,(\frac{\cdot}{p}))$ as a regular function for all complex s. Fekete observed that if $f_p(t)$ has no real zeros t with $0 < t < 1$, then $L(s,(\frac{\cdot}{p}))$ has no real zeros $s > 0$; and the $f_p(t)$ are thus now known as *Fekete polynomials*. Indeed, if $L(s,(\frac{\cdot}{p})) = 0$ then by (1.1) and the mean value theorem there is a t in $(0,1)$ with $\frac{(-\log t)^{s-1}}{t}\frac{f_p(t)}{1-t^p} = 0$, and so $f_p(t) = 0$ here.

Among small primes p, there are only a few for which the Fekete polynomial $f_p(t)$ has a real zero t in the range $0 < t < 1$. In fact, we may verify computationally that there are just 23 primes up to 1000 for which f_p has a zero in $(0,1)$. This implies that there are no positive real zeros of $L(s,(\frac{\cdot}{p}))$ for most such primes p, and in particular no *Siegel zeros* (that is, real zeros "especially close to 1"). It is interesting to note that for those primes $p \equiv 3 \mod 4$ for which $f_p(t)$ does have a zero in $(0,1)$, the class number of $Q(\sqrt{-p})$ is surprisingly small (for example $p = 43, 67, 163, \ldots$). Unfortunately this trend does not persist: Indeed Baker and

---

The first three authors are all supported, in part, by grants from the N.S.F. The first and fourth authors are supported by the American Institute of Mathematics. The second author is a Presidential Faculty Fellow. The third author is an Alfred P. Sloan Research Fellow and a Packard Fellow.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Montgomery [1] proved that $f_p(t)$ has a large number of zeros in $(0,1)$ for almost all primes p (that is, the number of such zeros $\to\infty$ as $p\to\infty$, and it seems likely that there are, in fact, $\asymp \log\log p$ such zeros).

In this paper we shall study the complex zeros of $f_p(t)$. Using zero locating software one finds that, for primes p up to 1000, about half of the zeros lie on the unit circle; leading one to expect this to be the general phenomenon. It turns out to be fairly easy to prove that *at least* half of the zeros of $f_p(t)$ are on the unit circle (that is $|t|=1$): First note that

$$F_p(z) := z^{-p/2} f_p(z) = \sum_{a=1}^{(p-1)/2} \left(\frac{a}{p}\right)\left(z^{a-p/2} + \left(\frac{-1}{p}\right) z^{p/2-a}\right)$$

by combining the a and $p-a$ terms[1]. Taking $z=e^{2i\pi t}$ we have

$$F_p\left(e^{2i\pi t}\right) = \begin{cases} 2\sum_{a=1}^{(p-1)/2}\left(\frac{a}{p}\right)\cos((2a-p)\pi t) & \text{if } p\equiv 1 \mod 4 \\ 2i\sum_{a=1}^{(p-1)/2}\left(\frac{a}{p}\right)\sin((2a-p)\pi t) & \text{if } p\equiv 3 \mod 4. \end{cases} \tag{1.3}$$

Define $H_p(t) = F_p(e^{2i\pi t})$ if $p\equiv 1 \pmod 4$, and $H_p(t) = -iF_p(e^{2i\pi t})$ if $p\equiv 3 \pmod 4$. By (1.3) we see that $H_p(t)$ is a periodic, continuous real-valued function when t is real.

Now if $\zeta_p = e^{2i\pi/p}$ then, for all k not divisible by p, $f_p(\zeta_p^k)$ is a *Gauss sum* and has absolute value $\sqrt{p}$ (see section 2 of [2]); therefore $|F_p(\zeta_p^k)| = \sqrt{p}$. Moreover

$$F_p(\zeta_p^k) = (\zeta_p^k)^{-p/2}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_p^{ak} = (-1)^k\left(\frac{k}{p}\right)\sum_{a=1}^{p-1}\left(\frac{ak}{p}\right)\zeta_p^{ak} = (-1)^k\left(\frac{k}{p}\right)F_p(\zeta_p).$$

Therefore if $\left(\frac{k}{p}\right) = \left(\frac{k+1}{p}\right)$ then $H_p(k/p)$ and $H_p((k+1)/p)$ have different signs. Since $H_p(t)$ is real-valued and continuous, it must have a zero in-between k/p and $(k+1)/p$, by the intermediate value theorem. Thus the number of zeros of $H_p(t)$ in $[0,1)$ (and so of $F_p(z)$ on the unit circle) is

$$\geq \#\left\{k : 1\leq k\leq p-2 \text{ and } \left(\frac{k}{p}\right) = \left(\frac{k+1}{p}\right)\right\} = \frac{p-3}{2},$$

as we shall see in Lemma 2.

Other than possible zeros at $z=-1$ and at $z=1$, this accounts for all the zeros on the unit circle for each prime $p<500$. So the question is, is this all, for all p? The answer is "no" and indeed one finds more zeros when $p=661$. In general one has the following:

Theorem 1. *There exists a constant κ_0, $1>\kappa_0>\frac{1}{2}$ such that*

$$\#\{z : |z|=1 \text{ and } f_p(z)=0\} \sim \kappa_0 p \text{ as } p\to\infty.$$

We determine κ_0 in terms of another constant κ_1 defined as follows:

[1]Here $z=e^{2i\pi t}$ with $0\leq t<1$, so that there is no ambiguity in the meaning of $z^{-p/2}$.

Theorem 2. *Let $\mathcal{F}_J$ be the set of rational functions*

$$g(x) = \frac{1}{x} + \frac{1}{1-x} + \sum_{\substack{|j|<J \\ j\neq 0,-1}} \frac{\delta_j}{x+j}$$

where we allow each δ_j to take value $+1$ or -1. There exists a constant κ_1, $\frac{1}{2} > \kappa_1 > 0$, such that

$$\#\{g \in \mathcal{F}_J : g(x) = 0 \text{ for some } x \in (0,1)\} \sim \kappa_1 \#\{g \in \mathcal{F}_J\}$$

as $J \to \infty$.

The constants κ_0 and κ_1 are related as follows:

Theorem $1\frac{1}{2}$. *In fact $\kappa_0 = \frac{1}{2} + \kappa_1$.*

It is still an open question to determine the value of κ_0. It is known that a "random" trigonometric polynomial of degree p has $p/\sqrt{3}$ zeros in $[0,1)$ (see [7]), so one might guess that $\kappa_0 = 1/\sqrt{3} \approx 0.5773\ldots$. However this is not the case. We will show

$$0.500813 > \kappa_0 > 0.500668.$$

While it is theoretically easy to find the value of κ_0, we do not know a good practical way of achieving this.

As well as determining precisely the proportion, κ_0, of the zeros of $f_p(t)$ which lie on the unit circle, we would also like to understand the distribution of the set of zeros in the complex plane. There are several easy remarks to make: By (1.2) we have

$$t^p f_p(1/t) = \left(\frac{-1}{p}\right) f_p(t)$$

and so the zeros of $f_p(t)$, other than $t = 0$, are symmetric about the unit circle (i.e. they come in pairs other than at $t = 0, \pm 1$). We also note that, for $|t| > 1$,

$$|f_p(t)/t^{p-1}| = \left| \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) \frac{1}{t^{p-1-a}} \right| \geq 1 - \sum_{a=0}^{p-2} \frac{1}{|t|^{p-1-a}} > 1 - \frac{1}{|t|-1}.$$

However if $|t| \geq 2$ then $1 - 1/(|t|-1) \geq 0$, and so $f_p(t)$ has no zeros in $|t| \geq 2$. By symmetry it has no zeros in $|t| \leq \frac{1}{2}$ except 0. Thus

Proposition 1. *The zeros of $f_p(t)$, other than at $0, 1$ and -1 come in pairs $\alpha, 1/\alpha$. Moreover, other than 0, they all lie in the annulus $\{r \in \mathbb{C} : \frac{1}{2} < |r| < 2\}$.*

As for the distribution of the arguments of the roots of $f_p(t)$ we can use a beautiful result of Erdős and Turán (Theorem 1 of [3]), which immediately implies that, for any $0 \leq \alpha < \beta < 1$,

$$\#\{\tau \in \mathbb{C} : \; f_p(\tau) = 0, \; \alpha < \arg(\tau)/2\pi < \beta\} = (\beta - \alpha)p + O(\sqrt{p \log p}). \tag{1.4}$$

The arguments above, and those used in proving Theorems 1 and 2, focus on determining which arcs $(\zeta_p^K, \zeta_p^{K+1})$ of the unit circle contain a zero of $f_p(t)$. Evidently (1.4) cannot be used so precisely. However we can show that there are zeros of $f_p(t)$ near to such an arc, so long as $f_p(t)$ gets "small" on that arc.

Theorem 3. *Suppose that $\epsilon > 0$ is a sufficiently small constant. If p is a sufficiently large prime and K an integer such that there exists a value of t on the unit circle in the arc from ζ_p^K to ζ_p^{K+1} with $|f_p(t)| < \epsilon\sqrt{p}$, then there exists $\tau = r\zeta_p^{K+\theta}$ with $f_p(\tau) = 0$ where $0 < \theta < 1$ and $1 - \epsilon^{1/3}/p < r \le 1$.*

Remark. Applying Proposition 1 we also have $f_p((1/r)\zeta_p^{K+\theta}) = 0$.

As we have already discussed, Gauss sums $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right)\zeta_p^{ak}$ (and many generalizations) have the surprising property that they have absolute value exactly equal to $\sqrt{p}$. It is, we think, of interest to ask what happens when we replace the primitive pth root of unity ζ_p^k in the expression for a Gauss sum above, by some primitive $2p$th root of unity. These may be written as $\zeta_p^{k+1/2}$ or ζ_{2p}^{2k+1}, or $-\zeta_p^k$; so we must consider the values of $f_p(-\zeta_p^k)$. Do these all take on the same absolute value ? The answer we now see is "no", as we evaluate the distribution of these absolute values:

Theorem 4. *For any fixed real number ρ*

$$\#\left\{k : 1 \le k \le p \text{ such that } H_p\left(\frac{k+1/2}{p}\right) < \rho\sqrt{p}\right\} \sim c_\rho p$$

as $p \to \infty$ where

$$c_\rho = \frac{1}{2} + \frac{1}{\pi}\int_{x=0}^{\infty} \sin(\rho\pi x) \prod_{\substack{n\ge 1\\ n \text{ odd}}} \cos^2\left(\frac{2x}{n}\right)\frac{dx}{x}.$$

Moreover $c_{-\rho}$ and $1 - c_\rho = \exp(-\exp(\pi\rho/2 + O(1)))$ for positive ρ.

After proving this in section 6, we indicate how our proof may be modified to establish several related results. First, to show that $\max_{|z|=1}|f_p(z)| \gg \sqrt{p}\log\log p$, so re-establishing a result of Montgomery [5]. Second to understand the distribution of the values of the Fekete polynomial at $(p-1)$st roots of unity.

Acknowledgements: *We thank Jeff Lagarias for facilitating this joint endeavour, Peter Borwein, Neil Dummigan, Hugh Montgomery, Pieter Moree, Mike Mossinghoff, Bob Vaughan and Trevor Wooley for some helpful remarks, and the referee for a very careful reading of the paper.*

2. First results

Let χ be any character $\pmod p$ and let k be an integer not divisible by p. Note that

$$\sum_{a=1}^{p-1}\chi(a)\zeta_p^{ak} = \bar\chi(k)\sum_{a=1}^{p-1}\chi(ak)\zeta_p^{ak} = \bar\chi(k)\sum_{b=1}^{p-1}\chi(b)\zeta_p^{b}. \tag{2.1}$$

In particular we see that $f_p(\zeta_p^k) = \left(\frac{k}{p}\right)f_p(\zeta_p)$, whereas in contrast $f_p(1) = 0$. Recall that for a non-principal character $\chi \pmod p$, the Gauss sum $\tau(\chi)$ is $\sum_{a=1}^{p-1}\chi(a)\zeta_p^a$. Thus $f_p(\zeta_p)$ is the Gauss sum $\tau(\left(\frac{\cdot}{p}\right))$. It is easy to determine the magnitude of

$|f_p(\zeta_p)|$: Note that

$$\begin{aligned}(p-1)f_p(\zeta_p)^2 &= \sum_{k=0}^{p-1} f_p(\zeta_p^k)^2 = \sum_{k=0}^{p-1}\sum_{a,b=0}^{p-1}\left(\frac{ab}{p}\right)\zeta_p^{(a+b)k} \\ &= \sum_{a,b=1}^{p-1}\left(\frac{ab}{p}\right)\sum_{k=0}^{p-1}\zeta_p^{(a+b)k} = p\sum_{\substack{a=1\\ b=p-a}}^{p-1}\left(\frac{ab}{p}\right) = p\left(\frac{-1}{p}\right)(p-1).\end{aligned}$$

Hence we have $f_p(\zeta_p)^2 = \left(\frac{-1}{p}\right)p$, and so $|f_p(\zeta_p)| = \sqrt{p}$. Gauss showed more and determined that

$$f_p(\zeta_p) = \begin{cases} \sqrt{p} & \text{if } p \equiv 1 \pmod 4, \\ i\sqrt{p} & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Since $f_p(\zeta_p^k) = \left(\frac{k}{p}\right)f_p(\zeta_p)$, for $1 \le k \le p-1$, and $f_p(1) = 0$, we get by Lagrangian interpolation

$$f_p(z) = \sum_{k=0}^{p-1} f_p(\zeta_p^k)\prod_{\substack{j=0\\ j\neq k}}^{p-1}\left(\frac{z-\zeta_p^j}{\zeta_p^k-\zeta_p^j}\right).$$

Note that

$$\prod_{\substack{j=0\\ j\neq k}}^{p-1}(z-\zeta_p^j) = \frac{z^p-1}{z-\zeta_p^k}, \qquad \text{and that} \qquad \prod_{\substack{j=0\\ j\neq k}}^{p-1}(\zeta_p^k-\zeta_p^j) = \zeta_p^{k(p-1)}\prod_{j=1}^{p-1}(1-\zeta_p^j) = p\zeta_p^{-k}.$$

Hence

$$\frac{p}{f_p(\zeta_p)}\frac{f_p(z)}{z^p-1} = \frac{p}{f_p(\zeta_p)}\frac{z^{-\frac{p}{2}}f_p(z)}{z^{\frac{p}{2}}-z^{-\frac{p}{2}}} = \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\frac{\zeta_p^k}{z-\zeta_p^k}. \tag{2.2}$$

If $|z| = 1$ then note that $z^{\frac{p}{2}} - z^{-\frac{p}{2}} \in i\mathbb{R}$, and from (1.3) and $f_p(\zeta_p)^2 = \left(\frac{-1}{p}\right)p$ we have $z^{-\frac{p}{2}}f_p(z)/f_p(\zeta_p) \in \mathbb{R}$. Thus the right side of (2.2) $\in i\mathbb{R}$ for all $|z| = 1$. To facilitate studying $f_p(z)$ as z goes around the unit circle from ζ_p^K to ζ_p^{K+1}, we write $z = \zeta_p^{K+x} = \zeta_p^K e^{2i\pi x/p}$ and then let

(2.3)

$$g_{p,K}(x) := i\left(\frac{K}{p}\right)\frac{p}{f_p(\zeta_p)}\frac{f_p(z)}{z^p-1}\bigg|_{z=\zeta_p^{K+x}} = i\left(\frac{K}{p}\right)\sum_{k=K-(\frac{p-1}{2})}^{K+(\frac{p-1}{2})}\left(\frac{k}{p}\right)\frac{1}{\zeta_p^{K-k+x}-1}.$$

Thus $g_{p,K}(x)$ is a real valued function of $x \in [0,1]$.

Proposition 2. *If $0 \le K \le p-1$ is an integer with $\left(\frac{K}{p}\right) = \left(\frac{K+1}{p}\right)$ then $g_{p,K}(x)$ has exactly one zero in $(0,1)$. Equivalently, $f_p(z)$ has exactly one zero on the arc of the unit circle from ζ_p^K to ζ_p^{K+1}. If $\left(\frac{K}{p}\right) = -\left(\frac{K+1}{p}\right)$ then $g_{p,K}$ has either no zeros, or exactly two zeros in $(0,1)$. Equivalently, $f_p(z)$ has exactly 0 or 2 zeros on the arc from ζ_p^K to ζ_p^{K+1}.*

Remark. In the above Proposition, and henceforth, we count zeros with multiplicity.

Before proving the Proposition, we evaluate $\sum_{k=1}^{p-1}\frac{1}{\sin^2(\frac{\pi k}{p})}$.

Lemma 1. *For all integers $p \geq 2$,*

$$\sum_{k=1}^{p-1} \frac{1}{\sin^2(\frac{\pi k}{p})} = \frac{p^2-1}{3}.$$

Proof. Put $A(z) = \prod_{k=1}^{p-1}(z-\zeta_p^k)$. Logarithmic differentiation shows that

$$\left\{ z\left(\frac{A'(z)}{A(z)}\right)' + \frac{A'(z)}{A(z)} \right\} \Bigg|_{z=1} = -\sum_{k=1}^{p-1} \frac{\zeta_p^k}{(1-\zeta_p^k)^2} = \frac{1}{4}\sum_{k=1}^{p-1} \frac{1}{\sin^2(\frac{\pi k}{p})}.$$

However, $A(z) = \frac{z^p-1}{z-1} = z^{p-1} + z^{p-2} + \ldots + 1$ and using this to evaluate the left side above, we get the lemma.

Proof of Proposition 2. Note that with $g = g_{p,K}$, we have $\lim_{x\to 0^+} g(x) = \infty$, and $\lim_{x\to 1^-} g(x) = -\left(\frac{K}{p}\right)\left(\frac{K+1}{p}\right)\infty$. Further observe that

$$\begin{aligned} g'(x) &= \frac{2\pi}{p}\left(\frac{K}{p}\right) \sum_{|k-K|<\frac{p}{2}} \left(\frac{k}{p}\right) \frac{\zeta_p^{K-k+x}}{(\zeta_p^{K-k+x}-1)^2} \\ &= -\frac{\pi}{2p}\left(\frac{K}{p}\right) \sum_{|k-K|<\frac{p}{2}} \left(\frac{k}{p}\right) \frac{1}{\sin^2(\frac{\pi}{p}(K-k+x))}. \end{aligned}$$

If $\left(\frac{K}{p}\right) = \left(\frac{K+1}{p}\right)$ then, by Lemma 1,

$$|g'(x)| \geq \frac{\pi}{2p}\left(\frac{1}{\sin^2(\frac{\pi}{p}x)} + \frac{1}{\sin^2(\frac{\pi}{p}(1-x))} - \sum_{\substack{j\neq 0,1 \\ |j|<p/2}} \frac{1}{\sin^2(\frac{\pi}{p}(x-j))} \right)$$

$$\geq \frac{\pi}{2p}\left(\frac{2}{\sin^2(\frac{\pi}{2p})} - \frac{p^2-1}{3} \right) > 0, \tag{2.4}$$

since the sum of the first two terms is minimized when $x = \frac{1}{2}$. Hence $g'(x) \neq 0$ for all $x \in (0,1)$, so that g is monotone decreasing in $[0,1]$ going from ∞ to $-\infty$. Thus g has exactly one zero in this interval.

Moreover

$$g''(x) = \frac{\pi^2}{p^2}\left(\frac{K}{p}\right) \sum_{|k-K|<p/2} \left(\frac{k}{p}\right) \frac{\cos(\frac{\pi}{p}(K-k+x))}{\sin^3(\frac{\pi}{p}(K-k+x))}.$$

Now if $\left(\frac{K}{p}\right) = -\left(\frac{K+1}{p}\right)$ then

$$g''(x) \geq \frac{\pi^2}{p^2}\left(\frac{\cos(\frac{\pi}{p}x)}{\sin^3(\frac{\pi}{p}x)} + \frac{\cos(\frac{\pi}{p}(1-x))}{\sin^3(\frac{\pi}{p}(1-x))} - \sum_{\substack{|j|<p/2 \\ j\neq 0,1}} \frac{\cos(\frac{\pi}{p}(j-x))}{|\sin(\frac{\pi}{p}(j-x))|^3} \right).$$

Let μ be the minimum of $\cot(\frac{\pi}{p}t)$ over $t = x,\, 1-x$. Since $\cot t$ decreases rapidly as t goes from 0 to $\frac{\pi}{2}$ we see that the above is

$$\geq \frac{\pi^2}{p^2}\mu\left(\frac{1}{\sin^2(\frac{\pi}{p}x)} + \frac{1}{\sin^2(\frac{\pi}{p}(1-x))} - \sum_{\substack{j\neq 0,1\\ |j|<p/2}} \frac{1}{\sin^2(\frac{\pi}{p}(x-j))}\right) > 0,$$

as in (2.4). Thus $g'(x)$ is monotone increasing in $(0,1)$ going from $-\infty$ to $+\infty$. Thus there is a unique x_0 in $(0,1)$ with $g'(x_0)=0$, and the minimum value of $g(x)$ is attained at x_0. Plainly g has 0 or 2 zeros depending on whether $g(x_0)>0$, or $g(x_0)\leq 0$. This proves the proposition.

From Proposition 2 we know that $f_p(z)$ has at least as many zeros on $|z|=1$, as there are values $1\leq K\leq p-1$ with $(\frac{K}{p}) = (\frac{K+1}{p})$. We next determine the number of such values K.

Lemma 2 (Gauss). *For any non-principal character $\chi \pmod p$, we have*

$$\sum_{b=1}^{p-1}\chi(b)\bar{\chi}(b+k) = \begin{cases} p-1 & \text{if } p|k \\ -1 & \text{if } p\nmid k. \end{cases} \tag{2.5}$$

Hence

$$\#\left\{b \pmod p : \left(\frac{b}{p}\right) = \left(\frac{b+1}{p}\right)\right\} = \frac{p-3}{2},$$

and

$$\#\left\{b \pmod p : \left(\frac{b}{p}\right) = -\left(\frac{b+1}{p}\right)\right\} = \frac{p-1}{2}.$$

Proof. If $p|k$ then the right side of (2.5) is $\sum_{b=1}^{p-1}|\chi(b)|^2 = p-1$. Suppose now that $p\nmid k$, and let $c=(b+k)/b = 1+k/b$. As b runs over the non-zero residue classes $\pmod q$, note that c runs over all residue classes except the residue class 1 $\pmod p$. Hence the right side of (2.5) is

$$\sum_{\substack{c \pmod p\\ c\not\equiv 1 \pmod p}} \bar{\chi}(c) = -1,$$

as desired.

If $(\frac{K}{p}) = -(\frac{K+1}{p})$ then we need to determine (in the notation of the proof of Proposition 2) whether $g(x_0)>0$ or ≤ 0. This depends heavily on the values of $(\frac{k}{p})$ for k neighbouring K. The following Lemma shows that these neighbouring values behave like independent random variables.

Lemma 3 (Weil). *Fix integer J, and then the numbers $\delta_j\in\{-1,1\}$ for each j with $|j|<J$. We have, uniformly,*

$$\#\left\{x \pmod p : \left(\frac{x-j}{p}\right) = \delta_j \text{ for all } |j|<J\right\} = \frac{p}{2^{2J-1}} + O(J\sqrt{p}).$$

Proof. The above equals

$$\sum_{x=1}^{p}\frac{1}{2^{2J-1}}\prod_{|j|<J}\left(1+\delta_j\left(\frac{x-j}{p}\right)\right)+O(J)$$
$$=\frac{p}{2^{2J-1}}+O\biggl(\frac{1}{2^{2J-1}}\sum_{\substack{S\subseteq\{|j|<J\}\\ S\neq\emptyset}}\sum_{x=1}^{p}\left(\frac{\prod_{j\in S}(x-j)}{p}\right)+J\biggr).$$

By Weil's Theorem [8], if $f(x)$ is a squarefree polynomial $\pmod p$ then

$$\left|\sum_{x=1}^{p}\left(\frac{f(x)}{p}\right)\right|\ll(\text{degree } f)\sqrt{p}.$$

Hence the above is

$$=\frac{p}{2^{2J-1}}+O\left(\frac{\sqrt{p}}{2^{2J-1}}\sum_{m=1}^{2J-1}\binom{2J-1}{m}m+J\right),$$

and the result follows.

We conclude this section by determining the order of the zeros of $f_p(z)$ at ±1. In fact we shall determine the number of zeros of $f_p(z)$ on the arcs $\zeta_p^{\frac{p-1}{2}}$ to $\zeta_p^{\frac{p+1}{2}}$ (which contains -1), and ζ_p^{-1} to ζ_p (which contains 1).

Lemma 4. *If $p\equiv 1 \pmod 4$ then $f_p(z)$ has only a simple zero at $z=-1$, on the arc from $\zeta_p^{\frac{p-1}{2}}$ to $\zeta_p^{\frac{p+1}{2}}$, and $f_p(z)$ has only a double zero at $z=1$, on the arc from ζ_p^{-1} to ζ_p. If $p\equiv 3 \pmod 4$ then there are no zeros of $f_p(z)$ on the arc from $\zeta_p^{\frac{p-1}{2}}$ to $\zeta_p^{\frac{p+1}{2}}$, and $f_p(z)$ has only a simple zero at $z=1$ on the arc from ζ_p^{-1} to ζ_p.*

Proof. We make free use of the fact that $\left(\frac{-1}{p}\right)=1$, or -1 depending on whether $p\equiv 1 \pmod 4$, or $3 \pmod 4$. Let's begin with the arc from $\zeta_p^{\frac{p-1}{2}}$ to $\zeta_p^{\frac{p+1}{2}}$. We take $K=\frac{p-1}{2}$ in Proposition 2. Note that $\left(\frac{K}{p}\right)=\left(\frac{K+1}{p}\right)$ if $p\equiv 1 \pmod 4$, and $\left(\frac{K}{p}\right)=-\left(\frac{K+1}{p}\right)$ if $p\equiv 3 \pmod 4$. In the first case, Proposition 2 tells us that there's exactly one (simple) zero on this arc. Since $f_p(-1)=\sum_{a=1}^{p-1}(-1)^a\left(\frac{a}{p}\right)=\frac{1}{2}\sum_{a=1}^{p-1}(-1)^a\left(\left(\frac{a}{p}\right)-\left(\frac{p-a}{p}\right)\right)=0$ for $p\equiv 1 \pmod 4$, this simple zero is at -1. Now suppose $p\equiv 3 \pmod 4$. By Proposition 2, we know that there are 0 or 2 zeros on this arc, depending on whether $\min_x g_{p,K}(x)>0$ or not. We now show that this minimum is attained at $x=\frac{1}{2}$, and the minimum value is positive. Putting $j=K-k$ in (2.3) we have

$$g_{p,K}(x)=i\left(\frac{K}{p}\right)\sum_{|j|\le\frac{p-1}{2}}\left(\frac{K-j}{p}\right)\frac{1}{\zeta_p^{j+x}-1}$$
$$=i\left(\frac{K}{p}\right)\sum_{j=0}^{\frac{p-1}{2}}\left(\frac{K-j}{p}\right)\left(\frac{1}{\zeta_p^{j+x}-1}-\frac{1}{\zeta_p^{-j-1+x}-1}\right),$$

since $K+j+1 \equiv -(K-j) \pmod p$. Evidently $g_{p,K}(1-x) = \overline{g_{p,K}(x)}$, so $g_{p,K}(1-x) = g_{p,K}(x)$ since $g_{p,K}(x)$ is real-valued. However we see that the minimum of $g_{p,K}(x)$ is obtained at a unique point in $(0,1)$, so that must be at $x = \frac{1}{2}$. Now

$$f_p(-1) = \sum_{a=1}^{p-1} (-1)^a \left(\frac{a}{p}\right) = \sum_{\substack{a=1 \\ a \text{ even}}}^{p-1} \left(\frac{a}{p}\right) - \sum_{\substack{b=1 \\ b \text{ even}}}^{p-1} \left(\frac{p-b}{p}\right)$$

where $a = p-b$ is odd in the second sum,

$$= 2\sum_{d=1}^{(p-1)/2} \left(\frac{2d}{p}\right) = 2\left(\frac{2}{p}\right)\sum_{d=1}^{(p-1)/2} \left(\frac{d}{p}\right) = 2\left(2\left(\frac{2}{p}\right) - 1\right) h(-p),$$

where $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$ (see section 2 of [2]). By (2.3), and since $f_p(\zeta_p) = i\sqrt{p}$ by Gauss, we have

$$\begin{aligned} g_{p,K}(\tfrac{1}{2}) &= -\left(\frac{K}{p}\right)\frac{\sqrt{p}}{2} f_p(-1) = \sqrt{p}\left(-2\left(\frac{2K}{p}\right) + \left(\frac{K}{p}\right)\right) h(-p) \\ &= \sqrt{p}\left(2 + \left(\frac{K}{p}\right)\right) h(-p) > 0. \end{aligned}$$

This shows that $f_p(z)$ has no zeros on the arc from $\zeta_p^{\frac{p-1}{2}}$ to $\zeta_p^{\frac{p+1}{2}}$ when $p \equiv 3 \pmod 4$.

Now let's consider the arc from ζ_p^{-1} to ζ_p. Take $K = p-1$, and consider $g_{p,K}(x)$ as defined in (2.3). Usually $g_{p,K}(x)$ would have a discontinuity at 1, but here since $\left(\frac{K+1}{p}\right) = \left(\frac{0}{p}\right) = 0$ we do not have this problem. Thus $g_{p,K}$ is a continuous function on $(0,2)$, and we may study $f_p(z)$ on the arc from ζ_p^{-1} to ζ_p by studying $g_{p,K}(x)$ on $(0,2)$. Note that for any p, $f_p(1) = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) = 0$, so that there is at least a simple zero at $z = 1$. Also $f_p'(1) = -i(-1/p) f_p(\zeta_p) g_{p,p-1}(1)$ by (2.3). Since $f_p(z) = (-1/p) z^p f_p(\overline{z})$, we deduce that $g_{p,p-1}(x) = -(-1/p) g_{p,p-1}(2-x)$.

If $p \equiv 1 \pmod 4$ then $g_{p,p-1}(1) = 0$ and so $f_p'(1) = 0$. Now, as in the proof of (2.4), the first part of the proof of Proposition 2, we have $|g_{p,K}'(x)| > 0$ for all $x \in (0,2)$. Therefore g has only a simple zero at $x = 1$, and thus f_p has a double zero at 1.

If $p \equiv 3 \pmod 4$ then, as in the second part of the proof of Proposition 2, $|g_{p,K}''(x)| > 0$ for $x \in (0,2)$. Thus there is a unique minimum of $g_{p,K}(x)$ on $(0,2)$, but since $g_{p,p-1}(x) = g_{p,p-1}(2-x)$ this must be attained at $x = 1$. However, by (2.3), and as $f_p(\zeta_p) = i\sqrt{p}$ by Gauss,

$$g_{p,K}(1) = -\frac{f_p'(1)}{\sqrt{p}} = -\frac{1}{\sqrt{p}} \sum_{a=1}^{p-1} a\left(\frac{a}{p}\right) = \sqrt{p}\, h(-p) > 0,$$

(see [2], section 2), and so $g_{p,K}(x) > 0$ and thus has no zeros in $(0,2)$. Therefore f_p has only a simple zero at $z = 1$ on this arc.

3. Functions with random coefficients

If $g \in \mathcal{F}_J$ then, for any $x \in (0,1)$, we have

$$\frac{1}{2}g''(x) = \frac{1}{x^3} + \frac{1}{(1-x)^3} + \sum_{\substack{|j|<J \\ j\neq 0,-1}} \frac{\delta_j}{(x+j)^3}$$

$$\geq \frac{1}{x^3} + \frac{1}{(1-x)^3} - \sum_{\substack{|j|<J \\ j\neq 0,-1}} \frac{1}{(x+j)^3} > 2\frac{1}{(\frac{1}{2})^3} - 2\zeta(3) > 0. \tag{3.1}$$

Since $\lim_{t\to 0^+} g'(t) = -\infty$ and $\lim_{t\to 1^-} g'(t) = \infty$ we deduce that $g'(x)$ has exactly one zero in $(0,1)$, call it x_0. Note that $g(x)$ attains its minimum value at x_0. If $0 \leq t < \frac{1}{\pi}$ then

$$-g'(t) \geq \frac{1}{t^2} - 2\left(\frac{1}{(1/2)^2} + \frac{1}{(3/2)^2} + \frac{1}{(5/2)^2} + \dots\right) = \frac{1}{t^2} - \pi^2 > 0.$$

Similarly if $1 - \frac{1}{\pi} < t \leq 1$ then $g'(t) > 0$. Thus

$$x_0 \in [\tfrac{1}{\pi}, 1 - \tfrac{1}{\pi}]. \tag{3.2}$$

We now show that few g are small in absolute value, at their minimum x_0.

Proposition 3. *We have $|g(x_0)| > J^{-\frac{1}{4}}$ for almost all $g \in \mathcal{F}_J$, where $g'(x_0) = 0$, uniformly as $J \to \infty$.*

Proof. Consider the subset S of $\mathcal{F}_J$ with all the δ_j fixed given values, except when $j \in [I, I + I^{\frac{1}{2}}]$ where $I = J^{\frac{1}{4}}$. Let $f \in S$ with $\delta_j = -1$ for all $j \in [I, I + I^{\frac{1}{2}}]$. Suppose that $f'(x_1) = 0$ and let

$$\gamma = \sum_{\substack{|j|<J \\ j\notin[I, I+I^{\frac{1}{2}}]}} \frac{\delta_j}{x_1 + j}$$

where $\delta_0 = 1$, $\delta_{-1} = -1$. Let g be any element of S with $g'(x_0) = 0$.

By (3.1) note that

$$|x_1 - x_0| \ll \left|\int_{x_0}^{x_1} f''(t)dt\right| = |f'(x_0) - f'(x_1)| = |f'(x_0)|$$

$$= |f'(x_0) - g'(x_0)| \leq 2 \sum_{j\in[I, I+I^{\frac{1}{2}}]} \frac{1}{(x_0+j)^2} \ll \frac{1}{I}. \tag{3.3}$$

Hence, keeping in mind x_0, $x_1 \in [\frac{1}{\pi}, 1 - \frac{1}{\pi}]$,

$$g(x_0) - \gamma = \sum_{j\in[I, I+I^{\frac{1}{2}}]} \frac{\delta_j}{x_0 + j} + O\Bigg(\sum_{\substack{|j|<J \\ j\notin[I, I+I^{\frac{1}{2}}]}} \left|\frac{1}{x_0+j} - \frac{1}{x_1+j}\right|\Bigg)$$

$$= \frac{1}{I}\sum_{j\in[I, I+I^{\frac{1}{2}}]} \delta_j + O\Bigg(\sum_{j\in[I, I+I^{\frac{1}{2}}]} \left|\frac{1}{I} - \frac{1}{x_0+j}\right| + |x_1 - x_0|\Bigg)$$

$$= \frac{1}{I}\sum_{j\in[I, I+I^{\frac{1}{2}}]} \delta_j + O\Big(\frac{1}{I}\Big),$$

since each $|1/I - 1/(x_0+j)| \ll 1/I^{\frac{3}{2}}$ and there are $I^{\frac{1}{2}}$ such terms. Therefore if $|g(x_0)| \le \frac{1}{I}$ then

$$\sum_{j\in[I,I+I^{\frac{1}{2}}]} \delta_j = -\gamma I + O(1). \tag{3.4}$$

Now, the δ_j are independent binomial random variables, so the distribution of their sum tends towards the normal distribution. Therefore the maximum probability for (3.4) to occur happens when $\gamma = 0$; and so (3.4) holds with probability $O(I^{-\frac{1}{4}})$, for any γ, implying Proposition 3.

4. Proof of Theorem 2

Suppose that $g \in \mathcal{F}_J$ and $f \in \mathcal{F}_K$, with $J < K$, such that the δ_j are the same in each for $|j| < J$. Select $x_0, x_1 \in (0,1)$ so that $g'(x_0) = 0$ and $f'(x_1) = 0$. Now

$$|f(x_1) - f(x_0)| \le \sum_{|j|<K} \left| \frac{1}{x_1+j} - \frac{1}{x_0+j} \right| \ll \sum_{|j|<K} \frac{|x_1-x_0|}{j^2+1} \ll |x_1 - x_0|,$$

since x_0, $x_1 \in [1/\pi, 1-1/\pi]$. Arguing exactly as in (3.3), we see that $|x_0 - x_1| \ll \frac{1}{J}$, and so we have

$$|f(x_1) - f(x_0)| \ll \frac{1}{J}. \tag{4.1}$$

We next consider the mean-square of

$$|f(x_0) - g(x_0)| = \left| \sum_{J\le|j|<K} \frac{\delta_j}{x_0+j} \right|.$$

To do so we will need to sum over all $\delta = \{\delta_j\}_{J\le|j|<K} \in \Delta_{J,K}$, that is the set of all possibilities with each $\delta_j = -1$ or 1 (note that there are 2 possible values for each δ_j so the set $\Delta_{J,K}$ has 2^{2K-2J} elements). With this notation, the mean square is

$$\begin{aligned} &\frac{1}{2^{2K-2J}} \sum_{\delta\in\Delta_{J,K}} \left| \sum_{J\le|j|<K} \frac{\delta_j}{x_0+j} \right|^2 \\ &\qquad = \sum_{J\le|j_1|,|j_2|<K} \frac{1}{(x_0+j_1)(x_0+j_2)} \frac{1}{2^{2K-2J}} \sum_{\delta\in\Delta_{J,K}} \delta_{j_1}\delta_{j_2} \\ &\qquad = \sum_{J\le|j|<K} \frac{1}{(x_0+j)^2} \asymp \frac{1}{J}. \end{aligned}$$

Thus if $\psi_J \to \infty$ as $J \to \infty$ then

$$\left| \sum_{J\le|j|<K} \frac{\delta_j}{x_0+j} \right| < \frac{\psi_J}{J^{\frac{1}{2}}}, \tag{4.2}$$

for almost all choices of the δ_j.

Combining (4.1) and (4.2), we see that for almost all choices of δ_j $(J \le |j| < K)$ we have

$$|f(x_1) - g(x_0)| \le |f(x_1) - f(x_0)| + |f(x_0) - g(x_0)| < \frac{2\psi_J}{J^{\frac{1}{2}}}. \tag{4.3}$$

Taking $\Psi_J = J^{\frac{1}{4}}/2$, and combining this with Proposition 3 we see that for almost all $g \in \mathcal{F}_J$, and almost all extensions f of g to $\mathcal{F}_K$, $f(x_1)$ has the same sign as $g(x_0)$. Summing up over all $g \in \mathcal{F}_J$ we deduce that $\omega_K = \omega_J + o(1)$, where

$$\omega_J := \frac{\#\{g \in \mathcal{F}_J : g(x) = 0 \text{ for some } x \in (0,1)\}}{\#\{g \in \mathcal{F}_J\}},$$

and the "$o(1)$" term depends only on J. Therefore $\lim_{J\to\infty} \omega_J$ exists, and equals κ_1 say.

Strong bounds on κ_1, which imply those in the statement of Theorem 2, are given in Proposition 6 in section 8.

Theorem 2 follows.

5. Proofs of Theorems 1 and $1\frac{1}{2}$

Let $1 \le K \le p-1$ be an integer. If $\left(\frac{K}{p}\right) = \left(\frac{K+1}{p}\right)$ then by Proposition 2 there is exactly one zero of $f_p(z)$ on the arc from ζ_p^K to ζ_p^{K+1}; by Lemma 2 this happens for $\sim \frac{p}{2}$ values of K. Suppose now that $\left(\frac{K}{p}\right) = -\left(\frac{K+1}{p}\right)$ so that $f_p(z)$ has either 0 or 2 zeros on the arc from ζ_p^K to ζ_p^{K+1} depending on whether $\min_{x\in(0,1)} g_{p,K}(x)$ is positive or not. To decide this question we need the following proposition:

Proposition 4. *Suppose $J \le \sqrt{p}$, and $J \to \infty$ as $p \to \infty$. For almost all $1 \le K \le p-1$ we have*

$$g_{p,K}(x) = \frac{p}{2\pi}\left(\frac{K}{p}\right) \sum_{|j|<J} \left(\frac{K-j}{p}\right) \frac{1}{j+x} + O\left(\frac{p}{J^{\frac{1}{3}}}\right),$$

uniformly for all $x \in (0,1)$.

Proof. Note that for $J \le |j| < \frac{p}{2}$,

$$\left| \frac{1}{\zeta_p^{j+x} - 1} - \frac{1}{\zeta_p^{j} - 1} \right| = \left| \frac{\zeta_p^x - 1}{(\zeta_p^{j+x} - 1)(\zeta_p^{j} - 1)} \right| \asymp \frac{px}{j(j+x)} \ll \frac{p}{j^2},$$

and, for $|j| < J$,

$$\frac{1}{\zeta_p^{j+x} - 1} = \frac{p}{2i\pi} \frac{1}{(j+x)} + O(1).$$

Hence, putting $j = K - k$ in (2.3), we have

$$\begin{aligned} g_{p,K}(x) &= i\left(\frac{K}{p}\right) \sum_{|j|<\frac{p}{2}} \left(\frac{K-j}{p}\right) \frac{1}{\zeta_p^{j+x} - 1} \\ &= \frac{p}{2\pi}\left(\frac{K}{p}\right) \sum_{|j|<J} \left(\frac{K-j}{p}\right) \frac{1}{j+x} + i\left(\frac{K}{p}\right) \sum_{J\le|j|<\frac{p}{2}} \left(\frac{K-j}{p}\right) \frac{1}{\zeta_p^{j} - 1} + O\left(J + \frac{p}{J}\right). \end{aligned}$$

We now show that the mean-square of the second term above is small, which proves the Proposition. By Lemma 2,

$$\begin{aligned}
&\sum_{K=1}^{p}\Bigg|\sum_{J\le|j|<\frac{p}{2}}\left(\frac{K-j}{p}\right)\frac{1}{\zeta_p^j-1}\Bigg|^2\\
&\qquad= \sum_{J\le|j_1|,\ |j_2|<\frac{p}{2}} \frac{1}{(\zeta_p^{j_1}-1)(\zeta_p^{-j_2}-1)}\sum_{K=1}^{p}\left(\frac{K-j_1}{p}\right)\left(\frac{K-j_2}{p}\right)\\
&\qquad= p\sum_{J\le|j|<\frac{p}{2}}\frac{1}{|\zeta_p^j-1|^2}-\Bigg|\sum_{J\le|j|<\frac{p}{2}}\frac{1}{\zeta_p^j-1}\Bigg|^2\\
&\qquad\ll p\sum_{J\le|j|<p/2}\left(\frac{p}{j}\right)^2+\Bigg(\sum_{J\le|j|<p/2}\frac{p}{j}\Bigg)^2\ll\frac{p^3}{J}+p^2\log^2 p.
\end{aligned}$$

This proves the Proposition.

By Proposition 4 we know that for almost all K with $\left(\frac{K}{p}\right)=-\left(\frac{K+1}{p}\right)$ the minimum value of $\frac{2\pi}{p}g_{p,K}(x)$ equals the minimum of $\left(\frac{K}{p}\right)\sum_{|j|<J}\left(\frac{K-j}{p}\right)\frac{1}{j+x}+O(J^{-\frac{1}{3}})$. For such K the minimum value of $g_{p,K}(x)$ is non-positive if and only if the minimum of $\left(\frac{K}{p}\right)\sum_{|j|<J}\left(\frac{K-j}{p}\right)\frac{1}{j+x}$ is non-positive, unless

$$\left(\frac{K}{p}\right)\sum_{|j|<J}\left(\frac{K-j}{p}\right)\frac{1}{j+x}\ll\frac{1}{J^{\frac{1}{3}}}. \tag{5.1}$$

Now choose $J=[\frac{\log p}{10}]$. Given any choice of $\delta_j\in\{-1,1\}$, $0<|j|<J$ with $\delta_0=1$, and $\delta_{-1}=-1$, by Lemma 3 there are $\sim p/2^{2J-2}$ values of K with $\left(\frac{K}{p}\right)\left(\frac{K-j}{p}\right)=\delta_j$ for each j. Therefore (5.1) fails, for almost all K, by Proposition 3. Appealing now to Theorem 2 we have proved that for $\sim\kappa_1 p/2$ values of K with $\left(\frac{K}{p}\right)=-\left(\frac{K+1}{p}\right)$, the minimum of $g_{p,K}(x)$ is <0. For such K, $f_p(z)$ has two zeros on the arc from ζ_p^K to ζ_p^{K+1}, so that the total number of such zeros is $\sim\kappa_1 p$. Theorems 1 and $1\frac{1}{2}$ follow.

6. Pseudo-Gauss Sums: Proof of the first part of Theorem 4

In this section, we wish to study the distribution of $f_p(\zeta_p^{K+\frac{1}{2}})$. By (2.3) and Proposition 4 we have (if $(\sqrt{p}>)J\to\infty$ as $p\to\infty$) for almost all $1\le K\le p-1$,

$$\begin{aligned}
f_p(\zeta_p^{K+\frac{1}{2}})&=\frac{if_p(\zeta_p)}{\pi}\Bigg(\sum_{|j|<J}\left(\frac{K-j}{p}\right)\frac{1}{j+\frac{1}{2}}+O\left(\frac{1}{J^{\frac{1}{3}}}\right)\Bigg)\\
&=\eta\frac{\sqrt{p}}{\pi}\Bigg(\sum_{|j|<J}\left(\frac{K-j}{p}\right)\frac{1}{j+\frac{1}{2}}+O\left(\frac{1}{J^{\frac{1}{3}}}\right)\Bigg),
\end{aligned} \tag{6.1}$$

where $\eta=\pm1$ or $\pm i$ is fixed. Thus, by Lemma 3, we have that for any fixed real number ρ

$$\lim_{p\to\infty}\frac{1}{p}\#\left\{K:1\le K\le p\text{ and }H_p\left(\frac{K+\frac{1}{2}}{p}\right)<\rho\sqrt{p}\right\}$$

exists and equals

$$\lim_{J\to\infty} \operatorname{Prob}\biggl(\sum_{|j|<J} \frac{\delta_j}{j+\frac{1}{2}} < \pi\rho : \ \delta \in \Delta_{0,J}\biggr). \tag{6.2}$$

(using the notation $\Delta_{J,K}$ of section 4). One may obtain an expression for this probability as follows: Recall that $\int_0^\infty \frac{\sin y}{y}dy = \frac{\pi}{2}$, and so for any $k \neq 0$

$$\frac{2}{\pi}\int_0^\infty \frac{\sin(kx)}{x}dx = \operatorname{sgn}(k)\frac{2}{\pi}\int_0^\infty \frac{\sin(|k|x)}{x}dx = \operatorname{sgn}(k)\frac{2}{\pi}\int_0^\infty \frac{\sin y}{y}dy = \operatorname{sgn}(k),$$

where $\operatorname{sgn}(k)$ is the sign of k ($=1$ if $k>0$ and -1 if $k<0$). Hence the probability (6.2) equals

$$\begin{aligned}
&\frac{1}{2^{2J-1}}\sum_{\delta\in\Delta_{0,J}}\left(\frac{1}{2}-\frac{1}{\pi}\int_0^\infty \sin\biggl(\biggl(\sum_{|j|<J}\frac{\delta_j}{j+\frac{1}{2}}-\pi\rho\biggr)x\biggr)\frac{dx}{x}\right)\\
&\quad= \frac{1}{2}-\frac{1}{\pi}\int_0^\infty \frac{1}{2^{2J-1}}\sum_{\delta\in\Delta_{0,J}}\left(\frac{e^{ix\left(\sum_{|j|<J}\frac{\delta_j}{j+1/2}-\pi\rho\right)}-e^{-ix\left(\sum_{|j|<J}\frac{\delta_j}{j+1/2}-\pi\rho\right)}}{2i}\right)\frac{dx}{x}\\
&\quad= \frac{1}{2}-\frac{1}{\pi}\int_0^\infty \prod_{|j|<J}\left(\frac{e^{\frac{ix}{j+1/2}}+e^{-\frac{ix}{j+1/2}}}{2}\right)\left(\frac{e^{-ix\pi\rho}-e^{ix\pi\rho}}{2i}\right)\frac{dx}{x}\\
&\quad= \frac{1}{2}+\frac{1}{\pi}\int_{x=0}^\infty \sin(\rho\pi x)\prod_{|j|<J}\cos\left(\frac{2x}{2j+1}\right)\frac{dx}{x}.
\end{aligned}$$

Letting $J\to\infty$, we get

$$c_\rho = \frac{1}{2}+\frac{1}{\pi}\int_0^\infty \sin(\rho\pi x)C(x)\frac{dx}{x} \qquad \text{where} \qquad C(x) := \prod_{\substack{n\geq 1\\ n \text{ odd}}}\cos^2\left(\frac{2x}{n}\right),$$

and thus Theorem 4 is proved. Note that this integral does converge: For any $x>0$ we have

$$C(x) \ll \frac{1}{2^{\frac{3x}{\pi}}}$$

since this estimate is trivial for $x \leq 1$, and otherwise we note that $|\cos(\frac{2x}{n})| < \frac{1}{2}$ if $3x/\pi < n < 6x/\pi$. Thus the part of the integral with $x \geq 1$ is easily bounded. Since $\sin(\rho\pi x) \ll \rho\pi x$, the portion of the integral from 0 to 1 is also easily bounded.

Remark 1. We use the above to study the multiplicative average size of $f_p(\zeta_p^{k+\frac{1}{2}})$. Due to the symmetry of c_ρ we have that

$$\frac{1}{p-1}\log\biggl(\prod_{k=1}^{p-1}\frac{f_p(\zeta_p^{k+\frac{1}{2}})}{\sqrt{p}}\biggr) = 2\int_0^\infty \log\rho \ \mathrm{d}(c_\rho - \tfrac{1}{2}).$$

Using our expression for c_ρ one can show that this is

$$= \gamma + \log\pi - \int_0^1 \frac{C(x)-1}{x}\,dx \ - \int_1^\infty \frac{C(x)}{x}\,dx.$$

All of these integrals converge, though we do not know their exact values.

Remark 2. The expansion given in (6.1) for f_p, and the general technique involved, is very similar to that used by Montgomery [5] in showing that,

i) $|f_p(z)| \ll \sqrt{p}\log p$ for all $|z|=1$.
ii) If p is sufficiently large then there exists some value of z with $|z|=1$ for which $|f_p(z)| > \frac{2}{\pi}\sqrt{p}\log\log p$.

Indeed to prove a result like that in (ii) we note that we may select each δ_j equal to the sign of j for $|j| < J = \varepsilon \log p$. By Lemma 3 there are many such K and we proceed as before with the expansion in (6.1), but now taking a little more care over the set of excluded K.

Remark 3. Fix $t \in (0,1)$. By the argument above, we have, for any fixed real number ρ,

$$\begin{aligned} c_{\rho,t} := & \lim_{p\to\infty} \frac{1}{p}\#\left\{K : 1 \le K \le p \text{ and } H_p\left(\frac{K+t}{p}\right) < \rho\sqrt{p}\right\} \\ = & \lim_{J\to\infty} \text{ Prob}\left(\delta \in \Delta_{0,J} : \sum_{|j|<J} \frac{\delta_j}{j+t} < \frac{\pi\rho}{\sin(\pi t)}\right) \\ = & \frac{1}{2} + \frac{1}{\pi}\int_{x=0}^{\infty} \sin\left(\frac{\rho\pi x}{\sin(\pi t)}\right)\prod_{j\in\mathbb{Z}}\cos\left(\frac{x}{j+t}\right)\frac{dx}{x}. \end{aligned}$$

Remark 4. We can also use these techniques to investigate the distribution of values of $H_p(t)$ at $t = a/(p-1)$ for $1 \le a \le p-1$. We note that if $K \sim \alpha p$ then $\zeta_{p-1}^K = \zeta_p^{K+\alpha}\{1+o(\frac{1}{p})\}$. Therefore we can get an expression similar to (6.1) for almost all $F_p(\zeta_{p-1}^K)$, but now with $\sum_{|j|<J}\left(\frac{K-j}{p}\right)\frac{1}{j+\alpha}$ replacing the sum in (6.1), and multiplying the whole expression through by $\sin(\alpha\pi)$. Thus the density of those K, for which $H_p(K/(p-1)) \le \rho\sqrt{p}$, is

$$\frac{1}{2} + \frac{1}{\pi}\int_{\alpha=0}^{1}\int_{x=0}^{\infty} \sin\left(\frac{\rho\pi x}{\sin(\alpha\pi)}\right)\prod_{m\in\mathbb{Z}}\cos\left(\frac{x}{m+\alpha}\right)\frac{dx}{x}d\alpha.$$

We cannot see how to obtain a simpler expression.

It is not hard to modify this technique to determine the distribution of values of the Fekete polynomial (or, in fact, $H_p(t)$) at any "reasonably" distributed set of values.

7. The distribution of $g(\frac{1}{2})$ for $g \in \mathcal{F}_J$ as $J \to \infty$.

We now look at the limiting distribution of $g(\frac{1}{2}) - 4$ for $g \in \mathcal{F}_J$ as $J \to \infty$. Define, for $N \ge 1$,

$$S_N(\underline{\delta}) = \sum_{|j+\frac{1}{2}|>N} \frac{\delta_j}{j+\frac{1}{2}},$$

where each $\delta_j = 1$ or -1 with probability $\frac{1}{2}$. We will prove that the distribution function of $S_1(\underline{\delta})$ decays *double exponentially*.

Theorem 5. *As $x \to \infty$, we have Prob*$(|S_1(\underline{\delta})| > x) = \exp(-e^{\frac{x}{2}+O(1)})$.

Proof of second part of Theorem 4. Note that $\mathrm{Prob}(S_1(\underline{\delta}) > x) = \mathrm{Prob}(S_1(\underline{\delta}) < -x) = \exp(-e^{\frac{x}{2}+O(1)})$, by symmetry. Taking $x = \pi\rho$, the result follows from (6.2).

To prove Theorem 5 we study the $2k$-th moment of $S_N(\underline{\delta})$, call it $M_N(k)$, that is, the expectation of $S_N(\underline{\delta})^{2k}$. For example

$$M_N(1) = \sum_{|j+\frac{1}{2}|>N} \frac{1}{(j+\frac{1}{2})^2}.$$

Our aim is to determine the asymptotic behaviour of $M_1(k)$ for large k.

Proposition 5. *For large k,*

$$M_1(k) = (2\log k - 2\log\log k + O(1))^{2k}.$$

Proof. To establish the lower bound, consider $\underline{\delta}$ such that $\delta_j = 1$ for all $1 \le |j + \frac{1}{2}| \le k/\log k$; and such that $S_{k/\log k}(\underline{\delta}) > 0$. The probability of this happening is $\asymp 1/2^{2k/\log k}$, and $S_1(\underline{\delta}) \ge 2\log k - 2\log\log k + O(1)$ for such $\underline{\delta}$. Hence

$$M_1(k) \gg \frac{1}{2^{2k/\log k}}(2\log k - 2\log\log k + O(1))^{2k} = (2\log k - 2\log\log k + O(1))^{2k}.$$

Now

$$M_N(k) = \sum_{j_1,j_2,\dots j_{2k}} \mathbb{E}\left(\frac{\delta_{j_1}}{j_1+\frac{1}{2}}\frac{\delta_{j_2}}{j_2+\frac{1}{2}}\cdots\frac{\delta_{j_{2k}}}{j_{2k}+\frac{1}{2}}\right),$$

where $\mathbb{E}$ stands for the expectation. Observe that a summand above is non-zero only if each value of j appears an even number of times amongst $j_1, j_2, \dots j_{2k}$. In particular $j_\ell = j_1$ for some $\ell > 1$, and then $\mathbb{E}(\prod_{1\le i\le 2k}\delta_{j_i}) = \mathbb{E}(\prod_{1\le i\le 2k,\ i\ne 1,\ell}\delta_{j_i})$. Summing over all $2k-1$ possibilities for ℓ in the above, we deduce that

$$M_N(k) \le (2k-1)\sum_{|j+\frac{1}{2}|>N}\frac{1}{(j+\frac{1}{2})^2}M_N(k-1), \tag{7.1}$$

for all $k \ge 1$ and all $N \ge 1$. Iterating this inequality, we obtain

$$\begin{aligned} M_N(k) &\le (2k-1)\cdot(2k-3)\cdots 3\cdot 1\cdot\left(\sum_{|j+\frac{1}{2}|>N}\frac{1}{(j+\frac{1}{2})^2}\right)^k \\ &\le \frac{(2k)!}{k!2^k}\left(\frac{2}{N-\frac{1}{2}}\right)^k = \frac{(2k)!}{k!(N-\frac{1}{2})^k}. \end{aligned} \tag{7.2}$$

Now

$$|S_1(\underline{\delta}) - S_N(\underline{\delta})| \le 2\lambda_N, \quad \text{where} \quad \lambda_N := \sum_{N\ge j+\frac{1}{2}\ge 1}\frac{1}{j+\frac{1}{2}} = \log N + O(1).$$

Evidently the odd moments of $S_N(\underline{\delta})$ are zero. Therefore, by the binomial theorem and (7.2),

$$\begin{aligned} M_1(k) &= \sum_{j=0}^{k} \binom{2k}{2j} \; M_N(j) \; \mathbb{E}(|S_1(\underline{\delta}) - S_N(\underline{\delta})|^{2k-2j}) \\ &\leq \sum_{j=0}^{k} \binom{2k}{2j} \frac{(2j)!}{j!(N-\frac{1}{2})^j} \; (2\lambda_N)^{2k-2j} \\ &\leq (2\lambda_N)^{2k} \sum_{j=0}^{k} \frac{1}{j!} \left(\frac{k^2}{(N-\frac{1}{2})\lambda_N^2} \right)^j \leq (2\lambda_N)^{2k} \exp\left(\frac{k^2}{(N-\frac{1}{2})\lambda_N^2} \right). \end{aligned}$$

Taking $N = k/\log k$ we obtain the upper bound of the Proposition.

Proof of Theorem 5. Take $k = c_1 x e^{x/2} + O(1)$ for some $c_1 > 0$, and then $\text{Prob}(|S_1(\underline{\delta})| > x) \leq x^{-2k} M_1(k) \ll \exp(-c_2 e^{x/2})$ for some constant $c_2 > 0$, if c_1 is sufficiently small, by Proposition 5.

The lower bound is more involved. Select integer k so that $2\log k - 2\log\log k$ is as close as possible to x. The contribution to $M_1(k)$ of those $\underline{\delta}$ with $|S_1(\underline{\delta})| < x - c_3$ is $\leq (x-c_3)^{2k} \leq M_1(k)/4$ if c_3 is sufficiently large. The contribution to $M_1(k)$ of those $\underline{\delta}$ with $|S_1(\underline{\delta})| > x + c_3$ is $\leq \int_{t>x+c_3} \text{Prob}(|S_1(\underline{\delta})| > t) t^{2k} dt \ll \int_{t>x+c_3} \exp(-c_2 e^{t/2}) t^{2k} dt \leq M_1(k)/4$ if c_3 is sufficiently large, using the upper bound from the paragraph above. Thus $M_1(k)/2 \leq \text{Prob}(x - c_3 \leq |S_1(\underline{\delta})| \leq x + c_3)(x+c_3)^k$ which implies that $\text{Prob}(|S_1(\underline{\delta})| \geq x - c_3) \geq M_1(k)/2(x+c_3)^k \gg \exp(-c_4 e^{x/2})$ for some constant $c_4 > 0$, by Proposition 5. Replacing $x - c_3$ by x gives the lower bound and thus our result.

Remark. We follow up on remark 3 of section 6. The arguments above (Theorem 5 and Proposition 5) hold just as well with "1/2" replaced by any fixed $t \in (0,1)$. Thus $1 - c_{\rho,t}$ and $c_{-\rho,t} = \exp(-\exp(\pi\rho/2\sin(\pi t) + O(1)))$ for $\rho > 0$.

8. Bounds on κ_1

Applying the method of section 6, we note that for any real λ,

$$\begin{aligned} \pi_\lambda := & \lim_{J\to\infty} \text{Prob}\{g \in \mathcal{F}_J : g(1/2) < 4\lambda\} \\ = & \frac{1}{2} - \frac{1}{\pi} \int_0^\infty \sin((1-\lambda)x) \prod_{\substack{n\geq 3 \\ n \text{ odd}}} \cos^2\left(\frac{x}{2n}\right) \frac{dx}{x}. \end{aligned} \tag{8.1}$$

We can use this to obtain numerical bounds on κ_1 using the following result.

Proposition 6. *We have* $\pi_{.013496...} \geq \kappa_1 \geq \pi_0$.

Using Simpson's rule to compute the integrals in (8.1) we obtain $.000813 > \pi_{.013496...} \geq \kappa_1 \geq \pi_0 > .000668$, from which we deduce the bounds on κ_0 in the introduction.

Proof. Again selecting x_0 so that $g(x_0)$ is minimal, we have, by definition, that

$$\kappa_1 = \lim_{J\to\infty} \text{Prob}\{g \in \mathcal{F}_J : g(x_0) \leq 0\}.$$

Since $g(x_0) \le g(1/2)$ we deduce the lower bound on κ_1 above.

To get the upper bound, write $x_0 = \frac{1}{2} + \nu$ so that $|\nu| < \frac{1}{2}$. If $g(x_0) \le 0$ then

$$\begin{aligned} g(\tfrac{1}{2}) \le g(\tfrac{1}{2}) - g(x_0) &= 4 - \frac{1}{x_0} - \frac{1}{1-x_0} + \sum_{\substack{|j|<J \\ j\ne 0,-1}} \frac{\delta_j (x_0 - \frac{1}{2})}{(j+\frac{1}{2})(j+x_0)} \\ &\le -\frac{4\nu^2}{\frac{1}{4}-\nu^2} + \sum_{j=1}^{\infty} \frac{|\nu|}{(j+\frac{1}{2})(j+\frac{1}{2}+\nu)} + \sum_{j=-\infty}^{-2} \frac{|\nu|}{(j+\frac{1}{2})(j+\frac{1}{2}+\nu)} \\ &= -\frac{4\nu^2}{\frac{1}{4}-\nu^2} + \sum_{j=1}^{\infty} \frac{2|\nu|}{(j+\frac{1}{2})^2-\nu^2} = -\frac{(2|\nu|+4\nu^2)}{\frac{1}{4}-\nu^2} + \pi\tan(\pi|\nu|). \end{aligned}$$

Using Maple to compute the $\max_\nu$, we obtain

$$g(\tfrac{1}{2}) \le \max_{|\nu|\le\frac{1}{2}} \left(\pi \tan(\pi|\nu|) - \frac{(2|\nu|+4\nu^2)}{\frac{1}{4}-\nu^2} \right) = 0.053986\ldots,$$

the maximum being attained at $\nu = \pm.057052\ldots$.

Remark. One can refine the above to get better bounds for κ_1. First note that $g(x) = 1/x + 1/(1-x)$ is the only element in $\mathcal{F}_1$, and in this case $x_0 = 1/2$; thus "1/2" appears in the definition of π_λ. More generally, let J be some positive integer. For each $\gamma \in \mathcal{F}_J$ select χ_0 so that $\gamma(\chi_0)$ is minimal. We again have $g(x_0) \le g(\chi_0)$, so if $g(\chi_0) \le 0$ then $g(x_0) \le 0$. On the other hand, if $g(x_0) \le 0$ then we can again get an explicit upper bound on $g(\chi_0)$ and proceed as above. This can be used to give another proof that κ_1 exists.

9. Zeros off the unit circle

Proof of Theorem 3. Theorem 3 holds trivially if there is a zero of $f_p(t)$ on the unit circle in the arc from ζ_p^K to ζ_p^{K+1}. Thus we shall henceforth assume that there is no such zero. Let $h(x) := H_p((K+x)/p)/H_p(K/p)$, so that $|h(x)| = |f_p(\zeta_p^{K+x})/\sqrt{p}|$, and $h(x)$ is a continuous real-valued function. Now the hypothesis implies that $h(y) < \epsilon$ for some $y \in (0,1)$ (in fact, $t = \zeta_p^{K+y}$), while our assumption above implies that $h(x) \ne 0$ for all $x \in (0,1)$. By (2.3) we have, uniformly for $|x| \le 2/3$,

$$\begin{aligned} h(x) &= \frac{\sin(\pi x)}{p} \left(\frac{1}{\sin(\pi x/p)} + \left(\frac{K}{p}\right) \sum_{1\le|K-k|<p/2} \frac{(k/p)}{\sin(\pi(x+K-k)/p)} \right) \\ &= 1 - (C + O(1))x, \quad \text{where } C := -\left(\frac{K}{p}\right) \sum_{1\le|K-k|<p/2} \frac{(k/p)}{K-k}. \end{aligned} \tag{9.1}$$

So if $h(y) < \epsilon$ for some sufficiently small y then $h(2y) = 2h(y) - 1 + O(y) < 0$, contradicting our assumption. Therefore we may assume that $y \gg 1$, and also $1 - y \gg 1$ by the symmetric argument. Thus $g_{p,K}(y) \ll \sqrt{p}|f_p(t)|/\sin(\pi y) \ll \epsilon p$ by (2.3), so that

$$g_{p,K}(x_0) \le g_{p,K}(y) \ll \epsilon p$$

where x_0 is defined as in section 3.

Let $x_1 = x_0 - \epsilon^{1/2}$, and $x_2 = x_0 + \epsilon^{1/2}$, and then $\alpha_j = \zeta_p^{x_j}$ for $j = 1, 2$. Let $R = 1 - \epsilon^{\frac{1}{3}}/p$. We shall consider the variation in argument of

$$G(z) := i\left(\frac{K}{p}\right)\frac{p}{f_p(\zeta_p)}\frac{f_p(z)}{z^p-1} = i\left(\frac{K}{p}\right)\sum_{|K-k|<\frac{p}{2}}\left(\frac{k}{p}\right)\frac{1}{z\zeta_p^{-k}-1},$$

as z goes around (in the anti-clockwise direction) the box bounded by the four curves, $\mathcal{C}_1$, the arc of the unit circle from α_1 to α_2, then $\mathcal{C}_2$, the straight line segment from α_2 to $R\alpha_2$, then $\mathcal{C}_3$, the arc of the circle of radius R, from $R\alpha_2$ to $R\alpha_1$, then finally $\mathcal{C}_4$, the straight line segment from $R\alpha_1$ back to α_1.

We know that $G(z)$ is real valued and positive on the arc $\mathcal{C}_1$. We shall show that $G(z)$ has positive imaginary part on $\mathcal{C}_2$, that $G(z)$ has negative real part on $\mathcal{C}_3$, and that $G(z)$ has negative imaginary part on $\mathcal{C}_4$, This shows that the change in argument of $G(z)$ is 2π as we go around our box, so that there is exactly one zero in our box. This implies a little more than Theorem 3.

To estimate $H(r,x) := G(r\zeta_p^{(K+x)/p})$ when $R \le r \le 1$, for a value of $x \in [x_1, x_2]$, we calculate the Taylor series expansion around $r = 1$, which is

$$H(r,x) = g_{p,K}(x) - \frac{(1-r)^2}{2r}\left(\frac{p}{2\pi}\right)^2 g''_{p,K}(x) + i\frac{1-r^2}{2r}\frac{p}{2\pi}g'_{p,K}(x) + O\left(\frac{(1-r)^3}{r}p^4\right).$$

From the proof of Proposition 2 we have, since x is bounded away from 0 and 1,

$$g_{p,K}(x) = g_{p,K}(x_0) + O((x-x_0)^2 p), \quad g'_{p,K}(x) \asymp (x-x_0)p, \quad \text{and} \quad g''_{p,K}(x) \asymp p.$$

Therefore

$$\begin{aligned}
\operatorname{Im}(G(z)) = \operatorname{Im}(H(r,x)) &\asymp \epsilon^{\frac{1}{2}}p^2(1-r) + O((1-r)\epsilon^{\frac{2}{3}}p^2) > 0 \quad \text{on } \mathcal{C}_2,\\
\operatorname{Im}(G(z)) = \operatorname{Im}(H(r,x)) &\asymp -\epsilon^{\frac{1}{2}}p^2(1-r) + O((1-r)\epsilon^{\frac{2}{3}}p^2) < 0 \quad \text{on } \mathcal{C}_4,\\
\operatorname{Re}(G(z)) = \operatorname{Re}(H(r,x)) &\asymp -\epsilon^{\frac{2}{3}}p + O(\epsilon p) < 0 \quad \text{on } \mathcal{C}_3,
\end{aligned}$$

as required.

Remark. By (9.1) we see that

$$\max_{|z|=1} |f_p(z)| \asymp \sqrt{p}\max_{K\in\mathbb{Z}}\sum_{j\neq 0}\frac{1}{j}\left(\frac{K+j}{p}\right).$$

This again allows us to recover the results of Montgomery [5], as in remark 2 of section 6.

References

1. R.C. Baker and H.L. Montgomery, *Oscillations of Quadratic L-functions*, Analytic Number Theory (ed. B.C. Berndt et.al.), Birkhäuser, Boston, 1990, p. 23–40.
2. H. Davenport, *Multiplicative Number Theory* (2nd ed.), Springer-Verlag, New York, 1980.
3. P. Erdős and P. Turán, *On the distribution of roots of polynomials*, Ann. of Math. **51** (1950), 105–119.

4. M. Fekete and G. Pólya, *Über ein Problem von Laguerre*, Rend. Circ. Mat. Palermo **34** (1912), 89–120.
5. H.L. Montgomery, *An exponential polynomial formed with the Legendre symbol*, Acta Arithmetica **37** (1980), 375–380.
6. G. Pólya, *Verschiedene Bemerkung zur Zahlentheorie*, Jber. deutsch Math. Verein **28** (1919), 31–40.
7. M. Sambandham and V. Thangaraj, *On the average number of real zeros of a random trigonometric polynomial*, J. Indian Math. Soc **47** (1983), 139–150.
8. A. Weil, *Sur les fonctions algébriques à corps de constantes fini*, C.R. Acad. Sci., Paris **210** (1940), 592–594.

(Conrey) American Institute of Mathematics. 360 Portage Ave, Palo Alto, California 94306, USA

E-mail address: `conrey@aimath.org`

(Conrey) Department of Mathematics, Oklahoma State University, Stillwater, Oklahoma 74078, USA

E-mail address: `conrey@hardy.math.okstate.edu`

(Granville) Department of Mathematics, The University of Georgia, Athens, Georgia 30602-7403, USA

E-mail address: `andrew@sophie.math.uga.edu`

(Poonen) Department of Mathematics, The University of California, Berkeley, California 94720-3840, USA

E-mail address: `poonen@math.berkeley.edu`

(Soundararajan) Department of Mathematics, Princeton University, Princeton, New Jersey 08544, USA

E-mail address: `skannan@math.princeton.edu`