Compositio Math. 144 (2008) 1351–1374
doi:10.1112/S0010437X08003631

Chebyshev's bias in function fields

Byungchul Cha

Abstract

We study a function field analog of Chebyshev's bias. Our results, as well as their proofs, are similar to those of Rubinstein and Sarnak in the case of the rational number field. Following Rubinstein and Sarnak, we introduce the grand simplicity hypothesis (GSH), a certain hypothesis on the inverse zeros of Dirichlet L-series of a polynomial ring over a finite field. Under this hypothesis, we investigate how primes, that is, irreducible monic polynomials in a polynomial ring over a finite field, are distributed in a given set of residue classes modulo a fixed monic polynomial. In particular, we prove under the GSH that, like the number field case, primes are biased toward quadratic nonresidues. Unlike the number field case, the GSH can be proved to hold in some cases and can be violated in some other cases. Also, under the GSH, we give the necessary and sufficient conditions for which primes are unbiased and describe certain central limit behaviors as the degree of modulus under consideration tends to infinity, all of which have been established in the number field case by Rubinstein and Sarnak.

1. Introduction

Chebyshev's bias is a term referring to the phenomenon, first observed by Chebyshev [Che53] in 1853, that the prime quadratic nonresidues of a given modulus predominate over the prime quadratic residues, in other words, primes are biased toward quadratic nonresidues. This and its various generalizations have been extensively studied by many authors. In 1994, Rubinstein and Sarnak in [RS94] made many important contributions to this area. Among other results, they were able to justify, under certain very plausible hypotheses, the existence of the bias, and assign numerical values to it. For more details and other related results, the readers are referred to the original paper of Rubinstein and Sarnak and to an excellent survey paper [GM06] of Granville and Martin.

In this article, we study the analog of Chebyshev's bias in a rational function field setting. Our results exhibit a strong resemblance to those in [RS94], and our proofs are obtained by closely following the strategies in [RS94]. To describe our results in more details, we fix a prime $p > 2$ and a finite field $\mathbb{F}$ with q elements, where q is a power of p. Let m be a monic polynomial in the polynomial ring $\mathbb{F}[T]$ over $\mathbb{F}$. For any positive integer N and an element a in $\mathbb{F}[T]$ prime to m, we let $\pi(N)$ and $\pi(a, m, N)$ be the prime counting functions defined by

$$\pi(N) := \#\{P \mid \deg(P) = N\},$$

and

$$\pi(a, m, N) := \#\{P \mid P \equiv a \mod m, \deg(P) = N\},$$

where the letter P denotes an irreducible and monic polynomial in $\mathbb{F}[T]$. Define $E_{m;a}(X)$, for a

Received 6 March 2008, accepted in final form 16 April 2008, published online 26 September 2008.
2000 Mathematics Subject Classification 11N05.
Keywords: Chebyshev's bias, prime number race.

positive integer X, by

$$E_{m;a}(X) := \frac{X}{q^{X/2}} \sum_{N=1}^{X} (\Phi(m)\pi(a, m, N) - \pi(N)),$$

where $\Phi(m) := \#(\mathbb{F}[T]/m)^*$ is the Euler phi function. The function $E_{m;a}(X)$ can be thought as describing how much more (or less) primes there are in the residue class of a than its fair share. The explicit formula of $E_{m;a}(X)$ is obtained by analyzing the coefficients of the power series of the logarithmic derivative of a Dirichlet L-function $L(s, \chi)$ for all Dirichlet characters modulo m. In the function field case, if $\chi \neq \chi_0$, the principal Dirichlet character, then $L(s, \chi)$ is a polynomial in q^{-s} and we denote its degree by $d(\chi)$. So, we can write

$$L(s, \chi) = \prod_{\nu=1}^{d(\chi)} (1 - \alpha(\chi, \nu)q^{-s}),$$

for some complex numbers $\alpha(\chi, \nu)$, which we call *inverse zeros* associated to χ. The absolute values of inverse zeros are either 1 or $\sqrt{q}$ by a result of Weil, the function field version of the Riemann hypothesis for curves. If we denote by $\gamma_\chi = \sqrt{q}e^{i\theta(\chi)}$ any inverse zero whose absolute value is $\sqrt{q}$, then the explicit formula of $E_{m;a}(X)$ is given by

$$E_{m;a}(X) = -c(m, a)\mathcal{B}_q(X) - \sum_{\chi \neq \chi_0} \bar{\chi}(a) \sum_{\gamma_\chi} e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1} + o(1), \tag{1}$$

as $X \to \infty$. (See Theorem 2.5.) Here, the number $c(m, a)$ is defined, as in [RS94], by

$$c(m, a) := -1 + \sum_{\substack{b^2 \equiv a \bmod m \\ b \in (\mathbb{F}[T]/m)^*}} 1,$$

and the function $\mathcal{B}_q(X)$ is defined by

$$\mathcal{B}_q(X) := \begin{cases} \sqrt{q}/(q-1) & \text{if } X \text{ is odd,} \\ q/(q-1) & \text{if } X \text{ is even.} \end{cases}$$

The term $-c(m, a)\mathcal{B}_q(X)$ in the formula (1) is the source of the bias. The similarity between the formula (1) and its number field counterpart (2.5) in [RS94] is the reason why we can prove the function field versions of many results in [RS94] by adapting the arguments of Rubinstein and Sarnak appropriately. From (1), we prove in Theorem 3.2 the existence of a certain limiting distribution μ that is constructed from $E_{m;a_1}(X), \ldots, E_{m;a_r}(X)$, for $a_1, \ldots, a_r$ in $\mathbb{F}[T]$ representing distinct classes in $(\mathbb{F}[T]/m)^*$. Understanding the measure μ, as in [RS94], holds the key to analyzing the bias.

We define a function field version of *grand simplicity hypothesis* (GSH). To do so, we first fix a set $\mathcal{I}$ of non-principal Dirichlet characters modulo m which is closed under complex conjugation. In this paper, $\mathcal{I}$ will be always either the set of all non-principal characters or, when m is irreducible, the singleton consisting of the non-principal real quadratic character modulo m. We say that the GSH is satisfied for $\mathcal{I}$ if the set

$$\{\theta(\chi) \mid \gamma_\chi = \sqrt{q}e^{i\theta(\chi)} \text{ is an inverse zero for some } \chi \in \mathcal{I}, 0 \leqslant \theta(\chi) \leqslant \pi\} \cup \{2\pi\}$$

is linearly independent over $\mathbb{Q}$. As in the work of Rubinstein and Sarnak, under the GSH for all non-principal characters, we find a product formula (Theorem 3.4) of the Fourier transformation of μ. From this, we can deduce that, if we define $P_{m;a_1,\ldots,a_r}$ to be the set of all positive integers X with

$$\sum_{N=1}^{X} \pi(a_1, m, N) > \sum_{N=1}^{X} \pi(a_2, m, N) > \cdots > \sum_{N=1}^{X} \pi(a_r, m, N),$$

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

then the limit

$$\delta(P_{m;a_1,\dots,a_r}) := \lim_{X\to\infty} \frac{\#(P_{m;a_1,\dots,a_r} \cap \{1,2,\dots,X\})}{X}$$

is equal to $\mu(\{x_1 > \cdots > x_r\} \subset \mathbb{R}^r)$, hence always exists. Note that the use of logarithmic density in [RS94] is now replaced by the use of the natural density in the function field setting.

In § 4, we focus on the non-principal real quadratic character χ_{quad} modulo an irreducible m. From this, we obtain an asymptotic formula (Theorem 4.3) for a function counting the number of prime quadratic residues minus that of prime quadratic nonresidues, similar to (1). This formula is proved using a slightly different method to that of (1). Define $a(N)$ and $b(N)$ to be the number of prime quadratic residues of degree N, and the number of prime quadratic nonresidues of degree N, respectively. Let $P_{m;\mathrm{R,N}}$ be the set of all positive integers X with

$$\sum_{N=1}^{X} a(N) > \sum_{N=1}^{X} b(N).$$

Under the GSH for the set $\{\chi_{\text{quad}}\}$, we establish the fact that

$$\delta(P_{m;\mathrm{R,N}}) := \lim_{X\to\infty} \frac{\#(P_{m;\mathrm{R,N}} \cap \{1,2,\dots,X\})}{X}$$

exists and $\delta(P_{m;\mathrm{R,N}}) < 1/2$. As an easy application of this, we also prove that more primes of an affine line split on a double covering of an irreducible plane curve than remain inert.

Unlike the number field case, there are some examples where the GSH does not hold. We give three examples in § 5 where the GSH is violated and the bias is toward quadratic residues, toward nonresidues, and nonexistent. Also, it is possible to confirm the GSH in certain cases, thanks to a recent result [Cal06] of Calcut. The verification of GSH is considered to be difficult for number fields. When $\deg(m) \leqslant 4$ and when GSH is confirmed to hold, our example indicates how we can calculate $\delta(P_{m;\mathrm{R,N}})$ from the inverse zeros associated to χ_{quad}.

The last section § 6 is devoted to proving, under the GSH, the analogs of Theorems 1.4, 1.6 and 1.5 of [RS94]. The first analog is Theorem 6.1 in the present paper, which gives the necessary and sufficient conditions for the density function of μ to remain unchanged under permutations of $(x_1,\dots,x_r)$. The second and third describe certain central limit behaviors. When m is irreducible, we show in Theorem 6.2 that

$$\delta(P_{m;\mathrm{R,N}}) \to \tfrac{1}{2}$$

as the degree of m goes to infinity, that is, the bias toward nonsquares disappears. Finally, we prove Theorem 6.5, which asserts that, now allowing m to be an arbitrary monic element in $\mathbb{F}[T]$,

$$\max_{a_1,\dots,a_r \in (\mathbb{F}[T]/m)^*} \left| \delta(P_{m;a_1,\dots,a_r}) - \frac{1}{r!} \right| \to 0,$$

as the degree of m tends to infinity. The proofs of all three theorems in this section are either similar to the corresponding proofs in [RS94], or different but easier. We give most of the details on how one can adapt the arguments of Rubinstein and Sarnak to the function field setting.

2. The asymptotic formula

We fix the following data:

- p, a prime number > 2;
- $\mathbb{F} = \mathbb{F}_q$, the finite field with q elements where q is a p-power;
- m, a monic polynomial in $\mathbb{F}[T]$ whose degree is at least two;

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

- M, the degree of m;
- $\Phi(m)$, the number $\#(\mathbb{F}[T]/m)^*$ of nonzero residue classes modulo m;
- a, an element of $\mathbb{F}[T]$ prime to m.

Throughout this paper, the letter P will always denote an irreducible monic polynomial in $\mathbb{F}[T]$. For any positive integer N, we define $\pi(N)$ and $\pi(a, m, N)$ by

$$\pi(N) := \#\{P \mid \deg(P) = N\}$$

and

$$\pi(a, m, N) := \#\{P \mid P \equiv a \mod m, \deg(P) = N\}.$$

It is known [Ros02] that

$$\pi(N) = \frac{q^N}{N} + O(q^{N/2}/N), \tag{2}$$

and

$$\pi(a, m, N) = \frac{1}{\Phi(m)} \cdot \frac{q^N}{N} + O(q^{N/2}/N). \tag{3}$$

For a positive integer X, we define $E_{m;a}(X)$ by

$$E_{m;a}(X) := \frac{X}{q^{X/2}} \sum_{N=1}^{X} (\Phi(m)\pi(a, m, N) - \pi(N)). \tag{4}$$

The purpose of this section is to find an asymptotic formula of $E_{m;a}(X)$ as $X \to \infty$.

For a Dirichlet character χ modulo m, the Dirichlet L-series is defined by

$$L(s, \chi) = \sum_{\substack{f \in \mathbb{F}[T] \\ f \text{ monic}}} \frac{\chi(f)}{|f|^s}. \tag{5}$$

Recall, by definition, $|f| := q^{\deg(f)}$. It is convenient to introduce the change of variable $u := q^{-s}$. We write $\mathcal{L}(u, \chi) := L(s, \chi)$.

We will estimate $\Phi(m)\pi(a, m, N) - \pi(N)$ in Proposition 2.1 by calculating the coefficients of the power series of $\sum_\chi \bar{\chi}(a) u(d/du) \log \mathcal{L}(u, \chi)$ for all Dirichlet characters χ modulo m, as outlined in [Ros02]. For each character χ, define the numbers $c_N(\chi)$ by the equation

$$u \frac{d}{du} \log \mathcal{L}(u, \chi) = \sum_{N=1}^{\infty} c_N(\chi) u^N.$$

From the Euler product $L(s, \chi) = \prod_{P \nmid m} (1 - \chi(P)|P|^{-s})^{-1}$, we have

$$\mathcal{L}(u, \chi) = \prod_{d=1}^{\infty} \prod_{\substack{P \nmid m \\ \deg(P) = d}} (1 - \chi(P) u^d)^{-1}. \tag{6}$$

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

Hence,

$$u\frac{d}{du}\log\mathcal{L}(u,\chi) = u\frac{d}{du}\sum_{d=1}^{\infty}\sum_{\substack{P\nmid m\\ \deg(P)=d}}\log(1-\chi(P)u^d)^{-1}$$
$$=\sum_{d=1}^{\infty}\sum_{k=1}^{\infty}\sum_{\substack{P\nmid m\\ \deg(P)=d}} d\chi(P^k)u^{dk}$$
$$=\sum_{N=1}^{\infty}\Bigg(\sum_{d\mid N} d\sum_{\substack{P\nmid m\\ \deg(P)=d}}\chi(P^{N/d})\Bigg)u^N.$$

From this, we obtain

$$c_N(\chi) = \sum_{d\mid N} d\sum_{\substack{P\nmid m\\ \deg(P)=d}}\chi(P^{N/d}). \tag{7}$$

By summing over all Dirichlet characters χ modulo m,

$$\sum_{\chi}\bar{\chi}(a)c_N(\chi) = \sum_{d\mid N} d\sum_{\substack{P\nmid m\\ \deg(P)=d}}\sum_{\chi}\bar{\chi}(a)\chi(P^{N/d}). \tag{8}$$

To simplify this summation, we introduce another notation $\pi(a,m,d,k)$, which is defined as

$$\pi(a,m,d,k) := \#\{P \mid P^k \equiv a \mod m, \deg(P)=d\},$$

for any positive integers k and d. From this definition it immediately follows that

$$\pi(a,m,d,1) = \pi(a,m,d). \tag{9}$$

To simplify $\pi(a,m,d,2)$, following [RS94], we define

$$c(m,a) := -1 + \sum_{\substack{b^2\equiv a \bmod m\\ b\in(\mathbb{F}[T]/m)^*}} 1. \tag{10}$$

If m is irreducible, then $c(m,a)$ is just the non-principal real quadratic character mod m. In general, $c(m,a)+1$ is the number of square roots of a in $(\mathbb{F}[T]/m)^*$. So, from (3),

$$\pi(a,m,d,2) = \frac{c(m,a)+1}{\Phi(m)}\cdot\frac{q^d}{d} + O(q^{d/2}/d). \tag{11}$$

For an arbitrary k, we have the estimation

$$\pi(a,m,d,k) \leqslant \pi(d) = O(q^d/d) \tag{12}$$

from (2).

Now we continue to estimate the summation in (8) using (9), (11), and (12), as well as the orthogonality of Dirichlet characters (see, for example, [Ros02, Proposition 4.2]). By the definition of $\pi(a,m,d,k)$ and the orthogonality, we have

$$\sum_{\chi}\bar{\chi}(a)c_N(\chi) = \sum_{d\mid N} d\sum_{\substack{P\nmid m\\ \deg(P)=d}}\sum_{\chi}\bar{\chi}(a)\chi(P^{N/d})$$
$$= \sum_{d\mid N} d\Phi(m)\pi(a,m,d,N/d).$$

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

We separate out the terms for $d = N$ and $d = N/2$ (which exists only when N is even) from above. By (9), the term for $d = N$ is $N\Phi(m)\pi(a, m, N)$. In addition, (11) implies that the term for $d = N/2$ is equal to

$$\frac{N}{2}\Phi(m)\left(\frac{c(m,a)+1}{\Phi(m)}\cdot\frac{q^{N/2}}{N/2}+O(q^{N/4}/N)\right)=(c(m,a)+1)q^{N/2}+O(q^{N/4}),$$

provided that N is even. If N is odd, then the $d = N/2$ term is zero. The sum of the terms with $d < N/2$ is $O(q^{N/3})$ from (12). Therefore, we proved that, for even N,

$$\sum_{\chi}\bar{\chi}(a)c_N(\chi)=N\Phi(m)\pi(a,m,N)+(c(m,a)+1)q^{N/2}+O(q^{N/3}) \tag{13}$$

and, if N is odd,

$$\sum_{\chi}\bar{\chi}(a)c_N(\chi)=N\Phi(m)\pi(a,m,N)+O(q^{N/3}). \tag{14}$$

Now, we give another estimate of $\sum_{\chi}\bar{\chi}(a)c_N(\chi)$. First, assume that χ is a non-principal Dirichlet character mod m, and let $d(\chi)$ be the degree of $\mathcal{L}(u, \chi)$ as a polynomial in u. Then we can write

$$\mathcal{L}(u,\chi)=\prod_{\nu=1}^{d(\chi)}(1-\alpha(\chi,\nu)u) \tag{15}$$

for some complex numbers $\alpha(\chi, \nu)$ whose absolute values are either $\sqrt{q}$ or 1 (see Proposition 6.4). We call $\alpha(\chi, \nu)$ an *inverse zero* of $\mathcal{L}(u, \chi)$. It is straightforward to apply $u(d/du)\log$ to (15) to obtain

$$u\frac{d}{du}\log\mathcal{L}(u,\chi)=-\sum_{N=1}^{\infty}\sum_{\nu=1}^{d(\chi)}\alpha(\chi,\nu)^N u^N.$$

So, for a non-principal character χ, we obtain

$$c_N(\chi)=-\sum_{\nu=1}^{d(\chi)}\alpha(\chi,\nu)^N. \tag{16}$$

Let χ_0 be the principal Dirichlet character modulo m. It is not hard to show that (see [Ros02, § 4])

$$\mathcal{L}(u,\chi_0)=\frac{\prod_{P|m}(1-u^{\deg(P)})}{1-qu},$$

from which we can deduce

$$c_N(\chi_0)=q^N+O(1). \tag{17}$$

It is possible to calculate the $O(1)$-term explicitly. For example, if m is irreducible, then this term is $-M$ or 0, if M divides N or not, respectively. For our purpose, though, it is sufficient to say that it is bounded. Summing up, we have proved

$$\sum_{\chi}\bar{\chi}(a)c_N(\chi)=-\sum_{\chi\neq\chi_0}\bar{\chi}(a)\sum_{\nu=1}^{d(\chi)}\alpha(\chi,\nu)^N+q^N+O(1). \tag{18}$$

Proposition 2.1. *Define* $\mathcal{B}(a, m, N)$ *by*

$$\mathcal{B}(a,m,N):=\begin{cases}0 & \text{if } N \text{ is odd},\\ c(m,a) & \text{if } N \text{ is even}.\end{cases}$$

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

Then, we have

$$N(\Phi(m)\pi(a,m,N)-\pi(N)) = -\mathcal{B}(a,m,N)q^{N/2} - \sum_{\chi\neq\chi_0}\bar{\chi}(a)\sum_{\nu=1}^{d(\chi)}\alpha(\chi,\nu)^N + O(q^{N/3}).$$

Proof. From a formula [Ros02, p. 13],

$$\pi(N) = \frac{1}{N}\sum_{d|N} q^{N/d}\mu(d),$$

where $\mu(d)$ is the Möbius function. As we will need all terms to be of size $q^{N/2}$ or larger, we write this as

$$\pi(N) = \begin{cases} (q^N - q^{N/2})/N + O(q^{N/3}/N) & \text{if } N \text{ is even,} \\ q^N/N + O(q^{N/3}/N) & \text{if } N \text{ is odd.} \end{cases} \tag{19}$$

If N is odd, we use (14), (18) and (19) to obtain

$$\begin{aligned} N(\Phi(m)\pi(a,m,N)-\pi(N)) &= \sum_{\chi}\bar{\chi}(a)c_N(\chi) - q^N + O(q^{N/3}) \\ &= -\sum_{\chi\neq\chi_0}\bar{\chi}(a)\sum_{\nu=1}^{d(\chi)}\alpha(\chi,\nu)^N + O(q^{N/3}). \end{aligned}$$

The case for even N is similar, except that there will be a $q^{N/2}$-term. An easy calculation, using (13), (18) and (19), verifies that the $q^{N/2}$-term in $N(\Phi(m)\pi(a,m,N)-\pi(N))$ is $-c(m,a)q^{N/2}$. This finishes the proof. □

LEMMA 2.2. *For any complex number β with $|\beta|>1$,*

$$\lim_{n\to\infty}\frac{n}{\beta^n}\left(\sum_{i=1}^{n}\frac{\beta^i}{i}\right) = \frac{\beta}{\beta-1}.$$

Proof. Let $h(n) := \beta^n$ and $f(x) := 1/x$. Also, let $H(x) := \sum_{n\leqslant x} h(n)$. Then, clearly,

$$H(x) = \beta\cdot\frac{\beta^{[x]}-1}{\beta-1}.$$

To calculate $\sum_{i=1}^{n}\beta^i/i$ we apply Abel's identity (see [Apo76, Theorem 4.2]), which gives

$$\sum_{n\leqslant x} h(n)f(n) = H(x)f(x) - \int_1^x H(t)f'(t)\,dt.$$

Therefore,

$$\frac{N}{\beta^N}\sum_{n=1}^{N}\frac{\beta^n}{n} = \frac{\beta-\beta^{1-N}}{\beta-1} + \frac{N}{\beta^N}\cdot\beta\cdot\int_1^N\frac{\beta^{[t]}-1}{\beta-1}\frac{1}{t^2}\,dt,$$

and it remains to show that the second term on the right-hand side above tends to zero as $N\to\infty$. Since $\int_1^\infty(1/t^2)\,dt<\infty$ and $|\beta^{[t]}|\leqslant|\beta|^t$, it is sufficient to prove that

$$\frac{N}{\beta^N}\int_1^N\frac{|\beta|^t}{t^2}\,dt\to 0$$

as $N\to\infty$. Using integration by parts,

$$\frac{N}{\beta^N}\int_1^N\frac{|\beta|^t}{t^2}\,dt = \frac{N}{\beta^N}\frac{1}{\log|\beta|}\left(\frac{|\beta|^N}{N^2}-\frac{|\beta|}{1^2}\right) - \frac{N}{\beta^N}\frac{1}{\log|\beta|}\int_1^N(-2)\frac{|\beta|^t}{t^3}\,dt.$$

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

The first term is easily seen to tend to zero as $N \to \infty$, and, again, we only need to show

$$\frac{N}{\beta^N} \int_1^N \frac{|\beta|^t}{t^3}\, dt \to 0.$$

To do so,

$$\begin{aligned}\int_1^N \frac{|\beta|^t}{t^3}\, dt &= \int_1^{N/2} \frac{|\beta|^t}{t^3}\, dt + \int_{N/2}^N \frac{|\beta|^t}{t^3}\, dt \\ &\leqslant \int_1^{N/2} \frac{|\beta|^{N/2}}{t^3}\, dt + \int_{N/2}^N \frac{|\beta|^N}{t^3}\, dt \\ &\leqslant k \cdot |\beta|^{N/2} + |\beta|^N \cdot \left(\frac{-2}{N^2} - \frac{(-2)}{(N/2)^2}\right)\end{aligned}$$

for a constant k. We multiply N/β^N on both sides of this inequality, and this completes the proof. □

Corollary 2.3. *Define $\mathcal{B}(N)$ by*

$$\mathcal{B}(N) = \begin{cases} 0 & \text{if } N \text{ is odd,} \\ 1 & \text{if } N \text{ is even.} \end{cases}$$

Then

$$\frac{X}{q^{X/2}} \sum_{N=1}^{X} \mathcal{B}(N) \frac{q^{N/2}}{N} = \begin{cases} \sqrt{q}/(q-1) + o(1) & \text{if } X \text{ is odd,} \\ q/(q-1) + o(1) & \text{if } X \text{ is even.} \end{cases}$$

Proof. Suppose that X is even, $X = 2X'$. Since $\mathcal{B}(N)$ is zero for all odd N we have that

$$\begin{aligned}\frac{X}{q^{X/2}} \sum_{N=1}^{X} \mathcal{B}(N) \frac{q^{N/2}}{N} &= \frac{2X'}{q^{X'}} \sum_{n=1}^{X'} \frac{q^n}{2n} \\ &= \frac{q}{q-1} + o(1),\end{aligned}$$

where the last equality is from Lemma 2.2. This proves the even X case.

For an odd $X = 2X' + 1$, we proceed similarly:

$$\begin{aligned}\frac{X}{q^{X/2}} \sum_{N=1}^{X} \mathcal{B}(N) \frac{q^{N/2}}{N} &= \frac{1}{\sqrt{q}} \frac{2X'+1}{q^{X'}} \sum_{n=1}^{X'} \frac{q^n}{2n} \\ &= \frac{\sqrt{q}}{q-1} + o(1),\end{aligned}$$

again, by Lemma 2.2. □

Corollary 2.4. *Let γ be a complex number with absolute value $\sqrt{q}$ and argument θ, that is, $\gamma = \sqrt{q}e^{i\theta}$. Then*

$$\frac{X}{q^{X/2}} \sum_{N=1}^{X} \frac{\gamma^N}{N} = e^{i\theta X} \frac{\gamma}{\gamma - 1} + o(1).$$

Proof. The is straightforward from Lemma 2.2, because

$$\frac{X}{q^{X/2}} \sum_{N=1}^{X} \frac{\gamma^N}{N} = e^{i\theta X} \frac{X}{\gamma^X} \sum_{N=1}^{X} \frac{\gamma^N}{N} = e^{i\theta X} \frac{\gamma}{\gamma - 1} + o(1).$$

□

We need to make a few notational conventions which will be used throughout this paper. When χ is a non-principal Dirichlet character, the letter γ_χ will denote an inverse zero of $\mathcal{L}(u, \chi)$ whose absolute value is $\sqrt{q}$. Also, $\theta(\gamma_\chi)$ is defined to be the argument of γ_χ, so that $\gamma_\chi = \sqrt{q}\, e^{i\theta(\gamma_\chi)}$.

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

THEOREM 2.5. *Define*

$$\mathcal{B}_q(X) := \begin{cases} \sqrt{q}/(q-1) & \text{if } X \text{ is odd,} \\ q/(q-1) & \text{if } X \text{ is even.} \end{cases}$$

Then

$$E_{m;a}(X) = -c(m,a)\mathcal{B}_q(X) - \sum_{\chi \neq \chi_0} \bar{\chi}(a) \sum_{\gamma_\chi} e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1} + o(1).$$

Proof. In view of Proposition 2.1, it will be sufficient to estimate the following three sums:

$$\frac{X}{q^{X/2}} \sum_{N=1}^{X} \mathcal{B}(a,m,N) \frac{q^{N/2}}{N}, \quad \frac{X}{q^{X/2}} \sum_{N=1}^{X} \frac{\bar{\chi}(a)\alpha(\chi,\nu)^N}{N}, \quad \frac{X}{q^{X/2}} \sum_{N=1}^{X} \frac{O(q^{N/3})}{N}. \tag{20}$$

The third is $o(1)$ because

$$\frac{X}{q^{X/2}} \sum_{N=1}^{X} \frac{O(q^{N/3})}{N} = \frac{X}{q^{X/2}} O(Xq^{X/3}) = o(1).$$

Corollary 2.3 says that the first sum above is equal to $-c(m,a)\mathcal{B}_q(X) + o(1)$. Finally, it remains to estimate the second sum in (20). When $|\alpha(\chi,\nu)| = 1$, the second sum in (20) is clearly $o(1)$. If $|\alpha(\chi,\nu)| = \sqrt{q}$, then we write $\alpha(\chi,\nu) = \gamma_\chi = \sqrt{q}\, e^{i\theta(\gamma_\chi)}$. From Corollary 2.4, we obtain

$$\frac{X}{q^{X/2}} \sum_{N=1}^{X} \frac{\bar{\chi}(a)\alpha(\chi,\nu)^N}{N} = \frac{X}{q^{X/2}} \sum_{N=1}^{X} \frac{\bar{\chi}(a)\gamma_\chi^N}{N} = \bar{\chi}(a) e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1} + o(1).$$

Combining all of the above, the theorem is proved. □

3. Limiting distribution and the GSH

Let $a_1, \ldots, a_r$ be elements of $\mathbb{F}[T]$ prime to m, representing distinct residue classes modulo m. Define the vector-valued function

$$E_{m;a_1,\ldots,a_r}(X) := (E_{m;\,a_1}(X), \ldots, E_{m;a_r}(X)).$$

Owing to the similarity between our function $E_{m;a}(X)$ (Theorem 2.5) and that of Rubinstein and Sarnak in (2.5) of [RS94], we can closely follow the argument in [RS94] to prove the existence of a limiting distribution defined by $E_{m;a_1,\ldots,a_r}(X)$, which is the main goal of this section. The fact that there are only finitely many inverse zeros of the L-series makes our proof simpler than Rubinstein and Sarnak's.

Define

$$E^{(T)}(X) := (E_1^{(T)}(X), \ldots, E_r^{(T)}(X))$$

where

$$E_l^{(T)}(X) := -c(m,a_l)\mathcal{B}_q(X) - \sum_{\chi \neq \chi_0} \bar{\chi}(a_l) \sum_{\gamma_\chi} e^{i\theta(\gamma_\chi)X} \frac{\gamma_\chi}{\gamma_\chi - 1} \tag{21}$$

for $l = 1, \ldots, r$, and $\epsilon_*(X) := (E_{m;a_1}(X) - E_1^{(T)}(X), \ldots, E_{m;a_r}(X) - E_r^{(T)}(X))$. By Theorem 2.5, $|\epsilon_*(X)| = o(1)$.

LEMMA 3.1. *For any continuous bounded function f on $\mathbb{R}^r$, the limit*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{X=1}^{N} f(E^{(T)}(X))$$

exists.

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

Proof. During the proof of this lemma, we let k be the number of all of the inverse zeros $\{\gamma_\chi\}_{\chi\neq\chi_0}$ with $\Im(\gamma_\chi)\geqslant 0$. We enumerate all such inverse zeros as $\gamma_1,\dots,\gamma_k$, and the corresponding arguments as $\theta_1,\dots,\theta_k$. After this enumeration, we let χ_j denote the character to which γ_j belongs for each $j=1,\dots,k$.

Define $b_0,b_1,\dots,b_k\in\mathbb{C}^r$ by

$$b_0 := -(c(m,a_1),\dots,c(m,a_r)),$$

and

$$b_j := -\left(\bar{\chi}_j(a_1)\frac{\gamma_j}{\gamma_j-1},\dots,\bar{\chi}_j(a_r)\frac{\gamma_j}{\gamma_j-1}\right),$$

for $j=1,\dots,k$. Also, define a function g on $\mathbb{R}^{k+1}$ by

$$g(\mathbf{x})=g(x_0,x_1,\dots,x_k) := f\left(b_0\frac{q^{(3+\cos(2\pi x_0))/4}}{q-1}+2\sum_{j=1}^{k}\Re(b_je^{2\pi i x_j})\right).$$

Then g gives rise to a continuous function on $\mathbb{R}^{k+1}/\mathbb{Z}^{k+1}$ and clearly

$$f(E^{(T)}(X))=g\left(\frac{X}{2},\frac{\theta_1X}{2\pi},\dots,\frac{\theta_kX}{2\pi}\right).$$

Let

$$\Gamma := \left\{\left(\frac{X}{2},\frac{\theta_1X}{2\pi},\dots,\frac{\theta_kX}{2\pi}\right)\in\mathbb{R}^{k+1}/\mathbb{Z}^{k+1}\;\middle|\;X=1,2,3,\dots\right\}. \tag{22}$$

Then, by Kronecker–Weyl theorem, Γ is equidistributed in its topological closure $\bar{\Gamma}$, and we have

$$\lim_{N\to\infty}\frac{1}{N}\sum_{X=1}^{N}f(E^{(T)}(X))=\int_{\bar{\Gamma}}g(\mathbf{x})\,d\mathbf{x}, \tag{23}$$

where $d\mathbf{x}$ is the normalized Haar measure on $\bar{\Gamma}$. □

Theorem 3.2. *There exists a probability measure $\mu=\mu_{m;a_1,\dots,a_r}$ on Borel sets in $\mathbb{R}^r$ such that*

$$\mu(f)=\lim_{N\to\infty}\frac{1}{N}\sum_{X=1}^{N}f(E_{m;a_1,\dots,a_r}(X)),$$

for all bounded continuous function f on $\mathbb{R}^r$.

Proof. During the proof of this theorem, we abbreviate $E_{m;a_1,\dots,a_r}(X)$ to $E(X)$. Let m_N be the probability measure on the set $\{1,\dots,N\}$ with $m_N(\{1\})=\cdots=m_N(\{N\})=1/N$, and ν_N be the probability measure on $\mathbb{R}^r$ given by

$$\nu_N := m_N{E^{(T)}}^{-1}.$$

Then we have

$$\nu_N(f)=\int_{\mathbb{R}^r}f\,d\nu_N=\frac{1}{N}\sum_{X=1}^{N}f(E^{(T)}(X))$$

for any function f on $\mathbb{R}^r$. Note that $E^{(T)}(X)$ is bounded. Therefore, the probability measures $\{\nu_N\}$ are tight. From [Bil86, Theorem 25.10], there exists a sequence $\{N_j\}$ and a probability measure μ_* such that $\nu_{N_j}\Longrightarrow\mu_*$ (that is, ν_{N_j} converges weakly to μ_*) as $j\to\infty$. Let f be a continuous bounded function. Then, from [Bil86, Theorem 25.8] and Lemma 3.1, we obtain

$$\int_{\mathbb{R}^r}f\,d\mu_*=\lim_{j\to\infty}\int_{\mathbb{R}^r}f\,d\nu_{N_j}=\lim_{N\to\infty}\int_{\mathbb{R}^r}f\,d\nu_N.$$

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

From [Bil86, Theorem 25.8] again, we conclude that $\nu_N \Longrightarrow \mu_*$ as $N \to \infty$.

Suppose, further, that $f : \mathbb{R}^r \longrightarrow \mathbb{R}$ is a continuous function satisfying a Lipschitz estimate

$$|f(\mathbf{x}) - f(\mathbf{y})| \leqslant c_f |\mathbf{x} - \mathbf{y}|.$$

Then, by the definition of $\epsilon_*(X)$,

$$f(E(X)) \leqslant f(E^{(T)}(X)) + c_f|\epsilon_*(X)| \quad \text{and} \quad f(E^{(T)}(X)) \leqslant f(E(X)) + c_f|\epsilon_*(X)| \tag{24}$$

for any X. Let $\epsilon > 0$ be given. Since $\epsilon_*(X) = o(1)$, we have

$$\frac{1}{N}\sum_{X=1}^{N} |\epsilon_*(X)| < \epsilon \tag{25}$$

for all sufficiently large N. From Lemma 3.1, (24) and (25),

$$\begin{aligned}
\mu_*(f) - \epsilon \cdot c_f &= \lim_{N\to\infty} \frac{1}{N}\sum_{X=1}^{N} f(E^{(T)}(X)) - \epsilon \cdot c_f \\
&\leqslant \limsup_{N\to\infty} \frac{1}{N}\sum_{X=1}^{N} f(E(X)) \\
&\leqslant \lim_{N\to\infty} \frac{1}{N}\sum_{X=1}^{N} f(E^{(T)}(X)) + \epsilon \cdot c_f \\
&= \mu_*(f) + \epsilon \cdot c_f.
\end{aligned}$$

Therefore, we conclude that

$$\mu_*(f) = \lim_{N\to\infty} \frac{1}{N}\sum_{X=1}^{N} f(E(X)) \tag{26}$$

for any Lipschitz f.

Let $\mu_N := m_N E^{-1}$. We have

$$\mu_N(f) = \int_{\mathbb{R}^r} f \, d\mu_N = \frac{1}{N}\sum_{X=1}^{N} f(E(X))$$

for any function f. Let μ be a (weak) limit of any subsequence of $\{\mu_N\}$, and let f be a Lipschitz function. Then

$$\mu_*(f) = \lim_{N\to\infty} \frac{1}{N}\sum_{X=1}^{N} f(E(X)) = \lim_{j\to\infty} \int_{\mathbb{R}^r} f \, d\mu_{N_j} = \mu(f).$$

This implies that $\mu_* = \mu$. From the corollary to Theorem 25.10 in [Bil86], we conclude that $\nu_N \Longrightarrow \mu$ as $N \to \infty$. Theorem 25.8 in [Bil86] now finishes the proof. □

DEFINITION 3.3 (Grand Simplicity Hypothesis). Consider a set $\mathcal{I} = \{\chi \neq \chi_0\}$ of non-principal Dirichlet characters modulo m, which is closed under complex conjugation. Then we say that $\mathcal{I}$ satisfies the GSH if the set

$$\{\theta \mid \gamma = \sqrt{q}e^{i\theta} \text{ is an inverse zero of } \mathcal{L}(u,\chi) \text{ for some } \chi \in \mathcal{I} \text{ with } 0 \leqslant \theta \leqslant \pi\} \cup \{2\pi\}$$

is linearly independent over $\mathbb{Q}$.

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

Theorem 3.4. *Assume that the set of all non-principal Dirichlet characters mod m satisfies the GSH. Then, the Fourier transform $\hat{\mu}$ of the measure μ in Theorem 3.2 is given by*

$$\hat{\mu}(\xi) = \mathcal{B}_{m;a_1,\dots,a_r}(\xi) \prod_{\chi\neq\chi_0} \prod_{\Im(\gamma_\chi)>0} J_0\left(\left|\frac{2\gamma_\chi}{\gamma_\chi - 1}\right|\left|\sum_{l=1}^{r} \chi(a_l)\xi_l\right|\right),$$

where

$$J_0(z) = \sum_{n=0}^{\infty} \frac{(-1)^n (z/2)^{2n}}{(n!)^2}$$

is the Bessel function of the first kind, and

$$\mathcal{B}_{m;a_1,\dots,a_r}(\xi) := \frac{1}{2}\left(\exp\left(i\frac{\sqrt{q}}{q-1}\sum_{l=1}^{r} c(m,a_l)\xi_l\right) + \exp\left(i\frac{q}{q-1}\sum_{l=1}^{r} c(m,a_l)\xi_l\right)\right).$$

Proof. We use the enumerations of inverse zeros and characters used in the proof of Lemma 3.1. The main consequence of the GSH for us is that the $\bar{\Gamma}$ in (22) is the union of two copies of a k-torus, more precisely,

$$\begin{aligned}\bar{\Gamma} = {} & \{(0, x_1, \dots, x_k) \in \mathbb{R}^{k+1}/\mathbb{Z}^{k+1} \mid (x_1, \dots, x_k) \in \mathbb{R}^k/\mathbb{Z}^k\} \\ & \cup \{(1/2, x_1, \dots, x_k) \in \mathbb{R}^{k+1}/\mathbb{Z}^{k+1} \mid (x_1, \dots, x_k) \in \mathbb{R}^k/\mathbb{Z}^k\}.\end{aligned}$$

Also, the normalized Haar measure $d\mathbf{x}$ on $\bar{\Gamma}$ is simply half of the usual Lebesgue measure on each k-torus.

Now, as in (3.1) in [RS94], using Theorem 3.2, (26) and (23)

$$\hat{\mu}(\xi) = \int_{\mathbb{R}^r} e^{i\xi x}\, d\mu(x) = \mathcal{B}_{m;a_1,\dots,a_r}(\xi) \prod_{j=1}^{k} \hat{\mu}_j(\xi) \tag{27}$$

where μ_j is the distribution of a typical term

$$-\left(\bar{\chi}_j(a_1)e^{i\theta_j X}\frac{\gamma_j}{\gamma_j - 1} + \chi_j(a_1)e^{-i\theta_j X}\frac{\bar{\gamma}_j}{\bar{\gamma}_j - 1}, \dots, \bar{\chi}_j(a_r)e^{i\theta_j X}\frac{\gamma_j}{\gamma_j - 1} + \chi_j(a_r)e^{-i\theta_j X}\frac{\bar{\gamma}_j}{\bar{\gamma}_j - 1}\right)$$

in (21). Writing $\chi_j(a_l) = u_{j,l} + iv_{j,l}$, we obtain

$$-2\left|\frac{\gamma_j}{\gamma_j - 1}\right|(u_{j,1}\cos(\theta_j X + \omega_j) + v_{j,1}\sin(\theta_j X + \omega_j), \dots, u_{j,r}\cos(\theta_j X + \omega_j) + v_{j,r}\sin(\theta_j X + \omega_j)),$$

where ω_j is the argument of $\gamma_j/(\gamma_j - 1)$. Further, let

$$R_j := \left|\frac{2\gamma_j}{\gamma_j - 1}\right|, \quad U_j := \sum_{l=1}^{r} \xi_l u_{j,l}, \quad V_j := \sum_{l=1}^{r} \xi_l v_{j,l}.$$

Then, as in [RS94, § 3.1],

$$\begin{aligned}\hat{\mu}_j(\xi) &= \frac{1}{2}\int_{-1}^{1} \exp\left(iR_j \sum_{l=1}^{r} \xi_l(u_{j,l}\sqrt{1-t^2} + v_{j,l}t)\right)\frac{dt}{\pi\sqrt{1-t^2}} \\ &\quad + \frac{1}{2}\int_{-1}^{1} \exp\left(iR_j \sum_{l=1}^{r} \xi_l(-u_{j,l}\sqrt{1-t^2} + v_{j,l}t)\right)\frac{dt}{\pi\sqrt{1-t^2}} \\ &= \frac{1}{\pi}\int_{-1}^{1} \exp(iR_jV_jt)\cos(R_jU_j\sqrt{1-t^2})\frac{dt}{\sqrt{1-t^2}} \\ &= J_0(R_j\sqrt{{U_j}^2 + {V_j}^2}).\end{aligned}$$

□

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

Remark 3.5. The term $\mathcal{B}_{m;a_1,\dots,a_r}(\xi)$ comes from $c(m,a)\mathcal{B}_q(X)$ in Theorem 2.5, and causes the bias. This is the analog of the factor $\exp(i\sum_{j=1}^{r} c(q,a_j)\xi_j)$ in (3.3) of [RS94].

4. The quadratic character and its applications

In this section, we assume that m is irreducible. We obtain an asymptotic formula (Theorem 4.3) for a counting function measuring the number of prime quadratic residues minus prime quadratic nonresidues. Although it may be possible to obtain Theorem 4.3 from Theorem 2.5, we give a separate proof, noting its similarity with the proof of the non-vanishing of the L-series associated to the non-principal real quadratic character (see [Ros02, § 2]).

Let χ_{quad} be the non-principal real quadratic character modulo m, that is,

$$\chi_{\text{quad}}(f) = \begin{cases} 1 & \text{if } f \text{ is square modulo } m, \\ -1 & \text{if } f \text{ is a nonsquare modulo } m, \\ 0 & \text{if } m \text{ divides } f. \end{cases}$$

We abbreviate $L(s,\chi_{\text{quad}})$ as $L(s)$ and $\mathcal{L}(u,\chi_{\text{quad}})$ as $\mathcal{L}(u)$. Then, $\mathcal{L}(u)$ is a polynomial in u of degree $M-1$ (see Proposition 6.4). We let $\{\alpha(\chi_{\text{quad}},\nu)\}_{\nu=1}^{M-1}$ denote its inverse zeros.

Define $a(N)$ and $b(N)$ by

$$a(N) := \#\{P \in \mathbb{F}[T] \mid \chi_{\text{quad}}(P) = 1, \deg(P) = N\}, \tag{28}$$

and

$$b(N) := \#\{P \in \mathbb{F}[T] \mid \chi_{\text{quad}}(P) = -1, \deg(P) = N\}. \tag{29}$$

Also, define

$$E_{m;\text{R,N}}(X) := \frac{X}{q^{X/2}} \sum_{N=1}^{X} (a(N) - b(N)). \tag{30}$$

To find an asymptotic formula for $E_{m;\text{R,N}}(X)$, we define a function $G(s)$ (cf. [Ros02, § 4])

$$G(s) := \frac{L(s,\chi_0)L(s)}{L(2s,\chi_0)},$$

where χ_0 is the principal character modulo m. Equivalently,

$$\mathcal{G}(u) := \frac{\mathcal{L}(u,\chi_0)\mathcal{L}(u)}{\mathcal{L}(u^2,\chi_0)}.$$

Let $c_G(N)$ be the Nth coefficient of the power series of $u(d/du)\log\mathcal{G}(u)$, that is,

$$u\frac{d}{du}\log\mathcal{G}(u) = \sum_{N=1}^{\infty} c_G(N)u^N.$$

Using (17) and (16) (with $\chi = \chi_{\text{quad}}$), it is straightforward to derive the equation

$$c_G(N) = -\sum_{\nu=1}^{M-1} \alpha(\chi_{\text{quad}},\nu)^N + q^N - 2\mathcal{B}(N)q^{N/2} + O(1). \tag{31}$$

Here, $\mathcal{B}(N)$ is, as before, defined to be one if N is even and zero if N is odd.

The Euler product of $G(s)$ gives another expression of $c_G(N)$. As in [Ros02, § 4], we have

$$G(s) = \prod \frac{1+|P|^{-s}}{1-|P|^{-s}},$$

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

where the product runs over all primes P that are quadratic residues modulo m. Hence,

$$\mathcal{G}(u) = \prod_{d=1}^{\infty} \left(\frac{1+u^d}{1-u^d} \right)^{a(d)}.$$

We take logarithmic derivative and collect the Nth terms to obtain

$$c_G(N) = \sum_{d|N} d\, a(d)(1-(-1)^{N/d}). \tag{32}$$

Now, the next step is to solve for $a(N)$ from (31) and (32). To do so, we need to recall some properties of Dirichlet multiplication (see, for example, [Apo76, § 2]). Suppose that $f(n)$ and $g(n)$ are functions on the set of positive integers. *Dirichlet multiplication* $f * g$ is the function h defined by

$$h(n) = \sum_{d|n} f(d)g(n/d).$$

Dirichlet multiplication is commutative and associative. Define $I(n)$ by $I(n) = 0$ for all $n > 1$ and $I(1) = 1$. If $f(1) \neq 0$, then there is a unique function f^{-1}, called the *Dirichlet inverse of* f, such that $f * f^{-1} = I$ (see [Apo76, Theorem 2.8]), and f^{-1} is given recursively by

$$f^{-1}(1) = 1/f(1), \quad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f(n/d) f^{-1}$$

for all $n > 1$.

Let $\mu(n)$ be the Möbius function. From [Apo76, Theorem 2.1],

$$\sum_{d|n} \mu(d) = I(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases} \tag{33}$$

Define $\nu(n) := 1$ for all $n \geqslant 1$. Then (33) can be rewritten as $\mu = \nu^{-1}$, or, equivalently, $\nu = \mu^{-1}$. We also define the functions $\mu^\circ(n)$ and $\nu^\circ(n)$ by

$$\mu^\circ(n) = \begin{cases} \mu(n) & n \text{ odd}, \\ 0 & n \text{ even}, \end{cases} \quad \text{and} \quad \nu^\circ(n) = \begin{cases} \nu(n) = 1 & n \text{ odd}, \\ 0 & n \text{ even}. \end{cases}$$

Lemma 4.1. *We have* $(\nu^\circ)^{-1} = \mu^\circ$ *and* $(\mu^\circ)^{-1} = \nu^\circ$.

Proof. We need to show that $\sum_{d|n} \mu^\circ(n/d)\nu^\circ(d) = I(n)$ for $n \geqslant 1$. This is clear for $n = 1$, so assume $n > 1$. First, note that

$$\sum_{d|n} \mu^\circ(n/d)\nu^\circ(d) = \sum_{\substack{d|n \\ d \text{ odd}}} \mu^\circ(n/d).$$

If n is even, then n/d is even for any odd d, so $\mu^\circ(n/d) = 0$ by the definition of μ°. Hence, the above sum is zero. If n is odd, then n/d is always odd, hence the above sum is equal to $\sum_{d|n} \mu(n/d)$. This sum is zero by (33). □

Proposition 4.2. *As* $N \to \infty$,

$$N(a(N) - b(N)) = -\sum_{\nu=1}^{M-1} \alpha(\chi_{\text{quad}}, \nu)^N - \mathcal{B}(N) q^{N/2} + O(q^{N/3}),$$

where $\mathcal{B}(N)$ *is defined to be one if* N *is even and zero if* N *is odd.*

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

Proof. In this proof, let $A(N) := N\,a(N)$ and $B(N) := N\,b(N)$. Note that $(-1)^n = 1 - 2\nu^\circ(n)$ for $n \geqslant 1$. From (31), (32) and Lemma 4.1, we have that

$$2A(N) = \sum_{d|N}\left(-\sum_{\nu=1}^{M-1}\alpha(\chi_{\mathrm{quad}},\nu)^d + q^d - 2\mathcal{B}(d)q^{d/2} + O(1)\right)\mu^\circ(N/d).$$

If N is odd, we can simplify the equation as

$$2A(N) = -\sum_{\nu=1}^{M-1}\alpha(\chi_{\mathrm{quad}},\nu)^N + q^N + O(q^{N/3}),$$

because all of the terms with $d < N$ can be grouped into the $O(q^{N/3})$. When N is even, we obtain

$$2A(N) = -\sum_{\nu=1}^{M-1}\alpha(\chi_{\mathrm{quad}},\nu)^N + q^N - 2q^{N/2} + O(q^{N/3}).$$

Note that the term $d = N/2$ here vanishes because $\mu^\circ(2) = 0$. Also, clearly,

$$A(N) + B(N) = N\pi(N),$$

if $N \neq M$. Therefore, $A(N) - B(N) = 2A(N) - N\pi(N)$ and the proof follows from this and (19). □

We enumerate, among all of the inverse zeros $\{\alpha(\chi_{\mathrm{quad}},\nu)\}_{\nu=1}^{M-1}$ of $\mathcal{L}(u)$, those whose absolute values are $\sqrt{q}$ as $\gamma_1, \bar{\gamma}_1, \ldots, \gamma_k, \bar{\gamma}_k$. From Proposition 6.4, we see that $k = [(M-1)/2]$, the greatest integer not exceeding $(M-1)/2$.

With this enumeration, we can now give an asymptotic formula for $E_{m;\mathrm{R,N}}(X)$.

THEOREM 4.3. *Let $\mathcal{B}_q(X)$ be defined by*

$$\mathcal{B}_q(X) = \begin{cases} \sqrt{q}/(q-1) & \text{if } X \text{ is odd,} \\ q/(q-1) & \text{if } X \text{ is even.} \end{cases}$$

Then we have

$$E_{m;\mathrm{R,N}}(X) = -\mathcal{B}_q(X) - 2\sum_{j=1}^{k}\Re\left(e^{i\theta_j X}\frac{\gamma_j}{\gamma_j - 1}\right) + o(1).$$

The proof is immediate from Proposition 4.2, and is similar to that of Theorem 2.5, so we omit it.

An easy corollary from this theorem is that, if $M = \deg(m) = 2$, then the prime nonresidues always (without assuming the GSH) predominate over prime residues, because the L-series has no inverse zeros with absolute values equal to $\sqrt{q}$.

COROLLARY 4.4. *Suppose that $M = \deg(m) = 2$. Then $E_{m;\mathrm{R,N}}(X) < 0$ for almost all X.*

As in Theorem 3.2, the function $E_{m,\mathrm{R,N}}(X)$ gives rise to a probability measure $\mu_{m;\mathrm{R,N}}$ on all Borel sets in $\mathbb{R}$, satisfying

$$\mu_{m;\mathrm{R,N}}(f) = \lim_{N\to\infty}\frac{1}{N}\sum_{X=1}^{N} f(E_{m;\mathrm{R,N}}(X)), \tag{34}$$

for all bounded continuous function f on $\mathbb{R}$. The proof is, again, similar to that of Theorem 3.2. Further, under the GSH on $\{\chi_{\mathrm{quad}}\}$, the Fourier transform $\hat{\mu}_{m;\mathrm{R,N}}$ of $\mu_{m;\mathrm{R,N}}$ can be given explicitly, so that we can compute the bias numerically, which we state as a theorem without proof.

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

Theorem 4.5. *Assume that the set* $\{\chi_{\text{quad}}\}$ *satisfies the GSH. Then the Fourier transform* $\hat{\mu}_{m;\text{R,N}}$ *of* $\mu_{m;\text{R,N}}$ *is given by*

$$\hat{\mu}_{m;\text{R,N}}(\xi) = \mathcal{B}_{m;\text{R,N}}(\xi) \prod_{j=1}^{k} J_0\left(\left|\frac{2\gamma_j}{\gamma_j - 1}\right|\xi\right),$$

where

$$J_0(z) = \sum_{n=0}^{\infty} \frac{(-1)^n (z/2)^{2n}}{(n!)^2}$$

is the Bessel function of the first kind, and

$$\mathcal{B}_{m;\text{R,N}}(\xi) := \frac{1}{2}\left(\exp\left(i\frac{\sqrt{q}}{q-1}\xi\right) + \exp\left(i\frac{q}{q-1}\xi\right)\right).$$

A direct consequence of the above theorem is that, under the GSH on $\{\chi_{\text{quad}}\}$, we have

$$\mu_{m;\text{R,N}}(-\infty, 0] > \tfrac{1}{2}.$$

In other words, the primes are biased toward quadratic nonresidues, if we assume that the GSH holds on $\{\chi_{\text{quad}}\}$.

As an application of Theorem 4.3, we consider the double covering $C \longrightarrow \mathbb{A}^1_{\mathbb{F}}$ where C is an affine plane curve defined by the equation $y^2 = m$ for a fixed irreducible monic $m \in \mathbb{F}[T]$ and $\mathbb{A}^1_{\mathbb{F}}$ is the affine line over $\mathbb{F}$. Define

$$a'(N) := \#\{P \in \mathbb{F}[T] \mid (m/P) = 1, \deg(P) = N\},$$
$$b'(N) := \#\{P \in \mathbb{F}[T] \mid (m/P) = -1, \deg(P) = N\},$$

and

$$E_{m;\text{S,I}}(X) := \frac{X}{q^{X/2}} \sum_{N=1}^{X} (a'(N) - b'(N))$$

(cf. (28), (29), and (30)). The function $E_{m;\text{S,I}}(X)$ counts the number of primes of $\mathbb{A}^1_{\mathbb{F}}$ splitting in C minus that of primes remaining inert in C, whose degrees are up to N. Now, the quadratic reciprocity law in function fields [Ros02, Theorem 3.3] says

$$\left(\frac{m}{P}\right) = (-1)^{M \deg(P)\cdot(q-1)/2}\left(\frac{P}{m}\right). \tag{35}$$

Therefore, if either M is even or $q \equiv 1 \mod 4$, then $(m/P) = (P/m)$ for all P, and $E_{m;\text{S,I}}(X) = E_{m;\text{R,N}}(X)$. So, the prime number race between splitting primes versus inert primes is the same as prime residues versus nonresidues. Assume now that M is odd and $q \equiv 3 \mod 4$. Then,

$$\left(\frac{m}{P}\right) = (-1)^{\deg(P)}\left(\frac{P}{m}\right),$$

which implies

$$a'(N) - b'(N) = (-1)^N (a(N) - b(N)).$$

Then, from Proposition 4.2, Theorem 4.3, and the definition of $\mathcal{B}(N)$, we obtain

$$E_{m;\text{S,I}}(X) = -\mathcal{B}_q(X) - 2\sum_{j=1}^{k} \Re\left(e^{i(\pi-\theta_j)X}\frac{\gamma_j}{\gamma_j - 1}\right) + o(1). \tag{36}$$

Here, as before, $\{\gamma_j, \bar{\gamma}_j\}_{j=1}^{k}$ enumerates the inverse zeros of the L-series $\mathcal{L}(u)$ associated with $\{\chi_{\text{quad}}\}$. Hence, under the GSH on $\{\chi_{\text{quad}}\}$, we see that the splitting primes outnumber the inert primes.

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

5. Violation of the GSH and examples

In this section, we continue to assume that m is irreducible. When the degree of m is small, it is possible to calculate $L(s, \chi_{\text{quad}})$ explicitly. In particular, in the first three examples below, we illustrate that the GSH can be violated, and the bias can be any of the following: toward squares, nonsquares, or nonexistent. This contrasts with the number field case.

Example 5.1. Let $p = 3$ and $m = T^3 + 2T + 1$. Then, we have

$$\mathcal{L}(u) = 3u^2 - 3u + 1 = \left(1 - \frac{3+\sqrt{3}i}{2}u\right)\left(1 - \frac{3-\sqrt{3}i}{2}u\right).$$

Therefore, the only inverse zero (with argument between 0 and π) is

$$\gamma_1 = \frac{3+\sqrt{3}i}{2} = \sqrt{3}e^{i\pi/6}.$$

In particular, the GSH is violated. We now compute $E_{m;\mathrm{R,N}}(X)$ using Theorem 4.3. It is easy to verify the following.

$X \bmod 12$	$E_{m;\mathrm{R,N}}(X) \pmod{o(1)}$
0 or 2	$-9/2$
1	$-5\sqrt{3}/2$
3 or 11	$-3\sqrt{3}/2$
4 or 10	$-3/2$
5 or 9	$\sqrt{3}/2$
6 or 8	$3/2$
7	$3\sqrt{3}/2$

This shows that $E_{m;\mathrm{R,N}}(X)$ is negative for $7/12 \approx 58.3\%$ of all (large enough) positive integers X. The bias is therefore toward nonsquares. Also, the measure $\mu_{m;\mathrm{R,N}}$ defined in (34) is concentrated at the seven points, more precisely,

$$\mu_{m;\mathrm{R,N}}(\{P\}) = \begin{cases} 1/12 & \text{if } P = -5\sqrt{3}/2 \text{ or } 3\sqrt{3}/2 \\ 2/12 & \text{if } P = -9/2, -3\sqrt{3}/2, -3/2, \sqrt{3}/2, \text{ or } 3/2, \end{cases}$$

and $\mu_{m;\mathrm{R,N}}(A) = 0$ for all A not containing the above points.

Example 5.2. Take $p = 5$ and $m = T^4 + 4T^3 + 4T^2 + 4T + 1$. Then

$$\mathcal{L}(u) = -5u^3 + 5u^2 - u + 1 = (1-u)(1+5u^2),$$

and

$$\gamma_1 = \sqrt{5}i = \sqrt{5}e^{i\pi/2}.$$

The results are as follows.

$X \bmod 4$	$E_{m;\mathrm{R,N}}(X) \pmod{o(1)}$
0	$-35/12$
1	$-7\sqrt{5}/12$
2	$5/12$
3	$\sqrt{5}/12$

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

In this case, the measure μ is concentrated evenly at $-35/12, -7\sqrt{5}/12, 5/12$ and $\sqrt{5}/12$. There is no bias in this example.

Example 5.3. This is an example where the bias is toward squares. Take $p = 5$ and $m = T^5 + 3T^4 + 4T^3 + 2T + 2$. Then

$$\begin{aligned}\mathcal{L}(u) &= 25u^4 - 25u^3 + 15u^2 - 5u + 1\\ &= \left(1 + \frac{5+\sqrt{5}}{2}u + 5u^2\right)\left(1 - \frac{5-\sqrt{5}}{2}u + 5u^2\right)\\ &= (1 - 2\sqrt{5}\cos(4\pi/5)u + 5u^2)(1 - 2\sqrt{5}\cos(2\pi/5)u + 5u^2).\end{aligned}$$

We have

$$\gamma_1 = \sqrt{5}e^{i2\pi/5} \quad \text{and} \quad \gamma_2 = \sqrt{5}e^{i4\pi/5}.$$

Using these, we can verify the following.

X mod 10	(Approximate value of) $E_{m;\mathrm{R,N}}(X)$ (mod $o(1)$)
0	−5.795 454 5455
1	−4.827 874 0423
2	−2.159 090 9091
3	1.270 493 1690
4	0.568 181 8182
5	0.254 098 6338
6	0.113 636 3636
7	2.286 887 7043
8	1.022 727 2727
9	−1.778 690 4366

In other words, for the 60% of X values, $E_{m;\mathrm{R,N}}(X)$ is positive, and the bias is toward squares.

We now give an example where we can confirm the GSH. Note that the GSH in the number field case is much more difficult to verify (see [RS94, §§ 1 and 5]). If an inverse zero γ_j is explicitly expressed using radicals, its argument is given as a value of arc tangent function at such radicals. To confirm the GSH, one must investigate a possible $\mathbb{Q}$-linear relation modulo π among them. In [Cal06], Calcut discusses the irrational nature of the values of the tangent function. In particular, Calcut gives a complete list of quadratic irrational numbers that can arise as values of the tangent function at rational multiples of π. Therefore, if $\mathcal{L}(u)$ is of degree three or less, we can always verify whether or not the GSH holds for this $\mathcal{L}(u)$, using Calcut's list. Also, in this example, we explain how to estimate the bias when the degree of $\mathcal{L}(u)$ is three or less.

Example 5.4. Take $q = 3$ and $m = T^4 + 2T^3 + 2T^2 + T + 2$. Then

$$\mathcal{L}(u) = -3u^3 + 5u^2 - 3u + 1,$$

and

$$\gamma_1 = 1 + i\sqrt{2} = \sqrt{3}e^{i\theta}$$

where $\theta = \tan^{-1}\sqrt{2}$. Since $\sqrt{2}$ does not appear in Calcut's list, we conclude that $(\tan^{-1}\sqrt{2})/\pi$ is irrational. Therefore, the GSH is satisfied for this example.

We illustrate how to compute $\mu_{m;\mathrm{R,N}}(-\infty, 0]$ for the case $k = 1$. See [RS94, § 3] for a similar computation in the number field case. Let $\tilde{\mu}$ be a measure whose Fourier transform is $J_0(2r\xi)$, with

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

$r := |\gamma_1/(\gamma_1 - 1)|$. Then the density of $\tilde{\mu}$ is given by

$$\begin{cases} \dfrac{1}{2r}\dfrac{1}{\sqrt{1-(t/2r)^2}}\Big/\pi & \text{if } -2r < t < 2r, \\ 0 & \text{otherwise.} \end{cases}$$

Let μ_1 and μ_2 be the shifts of $\tilde{\mu}$ by $-q/(q-1)$ and $-\sqrt{q}/(q-1)$, respectively. Then,

$$\mu_1(-\infty, 0] = \left(\sin^{-1}\left(\frac{q}{q-1}\frac{1}{2r}\right) + \frac{\pi}{2}\right)\Big/\pi \approx 0.709\,785,$$
$$\mu_2(-\infty, 0] = \left(\sin^{-1}\left(\frac{\sqrt{q}}{q-1}\frac{1}{2r}\right) + \frac{\pi}{2}\right)\Big/\pi \approx 0.615\,027.$$

Hence,

$$\mu_{m;\mathrm{R,N}}(-\infty, 0] = \frac{\mu_1(-\infty, 0] + \mu_2(-\infty, 0]}{2} \approx 0.662\,406.$$

In other words, for approximately 66% of positive integers $E_{m;\mathrm{R,N}}(X)$ is negative.

6. Symmetry and central limit behaviors

The purpose of this section is to give three theorems (Theorems 6.1, 6.2 and 6.5) describing the symmetry of the measure $\mu_{m;a_1,\dots,a_r}$ and central limit behaviors as the degree of the modulus m tends to infinity. These theorems are analogs of Theorems 1.4, 1.5 and 1.6 in [RS94], and the proofs are also modeled after those of Rubinstein and Sarnak.

THEOREM 6.1. *Assume that the set of all non-principal Dirichlet characters mod m satisfies the GSH. The density function of $\mu_{m;a_1,\dots,a_r}$ is symmetric in $(x_1, \dots, x_r)$ if and only if either:*

(i) *$r = 2$ and $c(m, a_1) = c(m, a_2)$; or*

(ii) *$r = 3$ and there exists $\rho \neq 1$ satisfying these congruences modulo m:*

$$\rho^3 \equiv 1, \quad a_2 \equiv a_1\rho, \quad \text{and} \quad a_3 \equiv a_1\rho^2.$$

The proof of this theorem is almost identical to that of Proposition 3.1 and Lemma 3.2 in [RS94], the only change being the expression $\sqrt{\frac{1}{4} + \gamma^2}$ in [RS94] to be replaced by $|\gamma/(\gamma - 1)|$ at appropriate places. We omit the details.

THEOREM 6.2. *Suppose that m is irreducible of degree M. Assume that the GSH holds for $\{\chi_{\mathrm{quad}}\}$. Let $\tilde{\mu}_{m;\mathrm{R,N}}$ be the limiting distribution of*

$$\sqrt{\frac{q-1}{q}}\frac{E_{m;\mathrm{R,N}}(X)}{\sqrt{M}}.$$

Then $\tilde{\mu}_{m;\mathrm{R,N}}$ converges in measure to the Gaussian $(2\pi)^{-1/2}e^{-X^2/2}dX$ as $M \to \infty$.

To prove Theorem 6.2, we fix an irreducible m whose degree is M. Recall that, if we enumerate the inverse zeros (whose absolute values are $\sqrt{q}$) of $\mathcal{L}(u, \chi_{\mathrm{quad}})$ as $\{\gamma_1, \bar{\gamma}_1, \dots, \gamma_k, \bar{\gamma}_k\}$, then $k = [(M-1)/2]$, the greatest integer not exceeding $(M-1)/2$. We will abbreviate $\hat{\mu} := \hat{\mu}_{m;\mathrm{R,N}}$ during the proof of Theorem 6.2. We have

$$\log \hat{\mu}_{m;\mathrm{R,N}}\left(\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{M}}\right) = \log \mathcal{B}_{m;\mathrm{R,N}}\left(\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{M}}\right) + \sum_{j=1}^{k} \log J_0\left(\left|\frac{2\gamma_j}{\gamma_j - 1}\right|\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{M}}\right) \quad (37)$$

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

from Theorem 4.5. Fix a large constant A. Then, for $|\xi| \leqslant A$, it is not difficult to show that

$$\log \mathcal{B}_{m;\mathrm{R,N}}\left(\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{M}}\right) = O(A/\sqrt{M}), \tag{38}$$

as $M \to \infty$, directly from the definition of $\mathcal{B}_{m;\mathrm{R,N}}(\xi)$ in Theorem 4.5. Also, from the power series expansion of $J_0(z) = 1 - \frac{1}{4}z^2 + \cdots$, we see that

$$\sum_{j=1}^{k} \log J_0\left(\left|\frac{2\gamma_j}{\gamma_j - 1}\right|\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{M}}\right) = -\sum_{j=1}^{k}\left|\frac{\gamma_j}{\gamma_j - 1}\right|^2 \frac{q-1}{q}\frac{\xi^2}{M} + \cdots. \tag{39}$$

For all $|\xi| \leqslant A$, it can be shown that the higher term is $O(A^4/M)$. To estimate the first term, let

$$I := \sum_{j=1}^{k}\left|\frac{\gamma_j}{\gamma_j - 1}\right|^2. \tag{40}$$

We define

$$\tilde{\mathcal{L}}(u) = \tilde{\mathcal{L}}(u, \chi_{\mathrm{quad}}) := \prod_{j=1}^{k}(1 - \gamma_j u)(1 - \bar{\gamma}_j u). \tag{41}$$

Then $\tilde{\mathcal{L}}(u) = \mathcal{L}(u, \chi_{\mathrm{quad}})$ if M is odd, and $\tilde{\mathcal{L}}(u)(1-u) = \mathcal{L}(u, \chi_{\mathrm{quad}})$ if M is even (see Proposition 6.4). By taking logarithmic derivative of $\tilde{\mathcal{L}}(u)$ and then evaluating at $u = 1$, we obtain

$$-\frac{\tilde{\mathcal{L}}'}{\tilde{\mathcal{L}}}(1) = \sum_{j=1}^{k}\frac{\gamma_j + \bar{\gamma}_j}{|\gamma_j - 1|^2} - 2I.$$

Also, we can easily prove

$$k + \sum_{j=1}^{k}\frac{\gamma_j + \bar{\gamma}_j}{|\gamma_j - 1|^2} = \frac{1+q}{q}I.$$

Therefore, from these two equalities, we deduce

$$I = \frac{q}{q-1}\left(\frac{\tilde{\mathcal{L}}'}{\tilde{\mathcal{L}}}(1) - k\right). \tag{42}$$

We can estimate $(\tilde{\mathcal{L}}'/\tilde{\mathcal{L}})(1)$ using the functional equation

$$\tilde{\mathcal{L}}(u, \chi_{\mathrm{quad}}) = \epsilon(\chi_{\mathrm{quad}})q^k u^{2k}\tilde{\mathcal{L}}(1/qu, \chi_{\mathrm{quad}}) \tag{43}$$

for some constant $\epsilon(\chi_{\mathrm{quad}})$ of absolute value 1. This functional equation is readily deduced from (41). We take the logarithmic derivative of (43). Taking into account the fact that $\tilde{\mathcal{L}}(u) = \mathcal{L}(u, \chi_{\mathrm{quad}})$ if M is odd, and $\tilde{\mathcal{L}}(u)(1-u) = \mathcal{L}(u, \chi_{\mathrm{quad}})$ if M is even, it follows that

$$\frac{\tilde{\mathcal{L}}'}{\tilde{\mathcal{L}}}(1) = 2k - \frac{1}{q}\frac{\mathcal{L}'}{\mathcal{L}}(1/q) - C$$

where

$$C := \begin{cases} 0 & \text{for an odd } M, \\ 1/(q-1) & \text{for an even } M. \end{cases}$$

Now we switch back to the variable s using $u = q^{-s}$. Then, from (42),

$$I = \frac{q}{q-1}\left(k + \frac{1}{\log q}\frac{L'}{L}(1, \chi_{\mathrm{quad}}) + C\right) = \frac{q}{q-1}\frac{M}{2} + O(\log M), \tag{44}$$

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

where we use Lemma 6.3 for the last equality. Combining (37), (38), (39), (40), and (44), we obtain

$$\log \hat{\mu}\left(\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{M}}\right) = -\frac{\xi^2}{2} + O\left(\frac{A}{\sqrt{M}} + \frac{A^2 \log M}{M} + \frac{A^4}{M}\right), \tag{45}$$

for all $|\xi| \leqslant A$. (cf. [RS94, p. 135].) By Levy's theorem, as in [RS94], this proves that the measures $\tilde{\mu}_{m;\mathrm{R,N}}$ in Theorem 6.2 converge in measure to the standard Gaussian. This concludes the proof of Theorem 6.2, once we prove the following lemma.

LEMMA 6.3. *Let χ be a non-principal Dirichlet character modulo m with $M = \deg(m)$. Then*

$$\frac{L'}{L}(1,\chi) = O(\log M)$$

as $M \to \infty$.

The number-theoretic counterpart of this lemma is $(L'/L)(1,\chi) = O(\log\log q)$, where χ here is a non-principal Dirichlet character modulo q. Rubinstein and Sarnak in [RS94] refer to a paper of Littlewood [Lit28] for its proof. Our proof of Lemma 6.3 will closely follow Littlewood's argument as well, highlighting the necessary modification. The author is grateful to Dr. Rubinstein for explaining the details of Littlewood's proof.

Proof. The core of the proof for this lemma is to establish the following estimation: for any y with $0 < y \leqslant 1$, we have

$$\left| -\frac{L'}{L}(1,\chi) - \sum_{\substack{f\in\mathbb{F}[T]\\ f \text{ monic}}} \frac{\Lambda(f)\chi(f)}{|f|}\exp(-q^{\deg(f)}y)\right| < A_1 y^{1/4} M, \tag{46}$$

for some constant A_1. Here, $\Lambda(f)$ is the function-field version of von Mangoldt's function and is defined to be $|P|$ if $f = P^j$ for some positive integer j and zero otherwise. The estimation (46) is a function-field counterpart of [Lit28, Lemma 6], and its proof is obtained by mimicking Littlewood's proof (and by setting the constants $\epsilon = 1/4$ and $\sigma = 1$ in his lemma). To be more specific, we start with

$$\exp(-q^{\deg(f)}y) = \frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} (q^{\deg(f)}y)^{-z}\Gamma(z)\,dz \quad (\Re y > 0).$$

This yields

$$\sum_{\substack{f\in\mathbb{F}[T]\\ f \text{ monic}}} \frac{\Lambda(f)\chi(f)}{|f|}\exp(-q^{\deg(f)}y) = -\frac{1}{2\pi i}\int_{2-i\infty}^{2+i\infty} \frac{L'(1+z,\chi)}{L(1+z,\chi)} y^{-z}\Gamma(z)\,dz.$$

Now, we can directly apply the remaining part of Littlewood's argument to the above equation in order to finish the proof of (46), with the only change being the estimation of $(L'/L)(s,\chi)$ given by, for any s with $3/4 < \sigma \leqslant 2$,

$$\left|\frac{L'}{L}(s,\chi)\right| < A_2 M$$

for a constant A_2. This is the counterpart of [Lit28, Lemma 5], and is easily proved using the fact that $L(s,\chi)$ is a polynomial in q^{-s} of degree $\leqslant M-1$, together with [Lit28, Lemma 4]. This finishes the proof of (46).

By taking $y = 1/M^4$ in (46), we see that, in order to finish proving Lemma 6.3, it is now sufficient to establish

$$\sum_{\substack{f\in\mathbb{F}[T]\\ f \text{ monic}}} \frac{\Lambda(f)\chi(f)}{|f|}\exp(-q^{\deg(f)}y) = O(\log(1/y)), \tag{47}$$

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

as $y \to 0$. To do so, we first note the equality

$$\sum_{\deg(f)=d} \Lambda(f) = q^d \log q.$$

One can prove this by considering the coefficients of the power series in q^{-s} of $\zeta'(s)/\zeta(s)$ (see [Ros02, ch. 2]). Now, the sum in the left-hand side of (47) is essentially bounded by $\sum_{d=0}^{\infty} \exp(-q^d y)$. Take d_0 to be the largest integer with $q^{d_0} y < 1$. Then

$$\sum_{d=0}^{\infty} \exp(-q^d y) \leqslant \sum_{d \leqslant d_0} 1 + \sum_{d > d_0} \exp(-(d - d_0)) = O(\log(1/y)) + O(1) = O(\log(1/y)).$$

This concludes the proof of Lemma 6.3. □

We examine more closely the number of inverse zeros of $\mathcal{L}(u, \chi)$ for a given Dirichlet character χ. Consider the cyclotomic function field extension K of $\mathbb{F}(T)$ obtained by adjoining the m-torsion points of the Carlitz module, which gives rise to the identification $\mathrm{Gal}(K/\mathbb{F}(T)) \simeq (\mathbb{F}[T]/m)^*$. Recall that χ is called *even* if χ is trivial on the subgroup $\mathbb{F}^*$ of $\mathrm{Gal}(K/\mathbb{F}(T))$ via the above identification. The next proposition summarizes the structures of $\mathcal{L}(u, \chi)$ we need later.

Proposition 6.4. *Let χ^* be the primitive Dirichlet character modulo a polynomial $m(\chi^*)$ which induces a non-principal Dirichlet character χ modulo m. Also, let $M(\chi^*)$ be the degree of $m(\chi^*)$. Then we have:*

(a)
$$\mathcal{L}(u, \chi) = \mathcal{L}(u, \chi^*) \prod_{\substack{P \mid m \\ P \nmid m(\chi^*)}} (1 - u^{\deg(P)});$$

(b) *$\mathcal{L}(u, \chi^*)$ is a polynomial in u of degree $M(\chi^*) - 1$;*

(c) *if χ^* is even,*
$$\mathcal{L}(u, \chi^*) = (1 - u) \prod_{i=1}^{M(\chi^*)-2} (1 - \gamma_i u),$$
and, otherwise,
$$\mathcal{L}(u, \chi^*) = \prod_{i=1}^{M(\chi^*)-1} (1 - \gamma_i u)$$
for some complex numbers γ_i with $|\gamma_i| = \sqrt{q}$;

(d) *if m is irreducible, then*
$$\mathcal{L}(u, \chi_{\mathrm{quad}}) = (1 - u) \prod_{i=1}^{(M-2)/2} (1 - \gamma_i u)(1 - \bar{\gamma}_i u)$$
for M even, and
$$\mathcal{L}(u, \chi_{\mathrm{quad}}) = \prod_{i=1}^{(M-1)/2} (1 - \gamma_i u)(1 - \bar{\gamma}_i u)$$
for M odd.

Proof. These properties are essentially consequences of a theorem of Weil, the function field analog of the Riemann hypothesis. Property (a) is immediate from our definition of Dirichlet L-series given in (5). Note that, for a non-principal character χ, the Dirichlet L-series $L(s, \chi)$ can be modified to give the Artin L-function by introducing a local factor at the infinite prime, which is $(1 - q^{-s})^{-1}$

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

if χ is even, and one otherwise. This, together with Weil's theorem, proves (b) and (c) (see [Ros02, Proposition 14.10]). Lastly, property (d) is immediate from property (b), property (c), and the fact that the inverse zeros of $\mathcal{L}(u, \chi_{\text{quad}})$ are stable under complex conjugation. □

THEOREM 6.5. *Suppose that m is an arbitrary (not necessarily irreducible) element in $\mathbb{F}[T]$ of degree M. Assume that the set of all non-principal Dirichlet character modulo m satisfies the GSH. For a fixed r,*

$$\max_{a_1,\dots,a_r \in (\mathbb{F}[T]/m)^*} \left| \delta(P_{m;a_1,\dots,a_r}) - \frac{1}{r!} \right| \to 0$$

as $M \to \infty$.

We begin the proof of Theorem 6.5. The modulus m is now taken to be arbitrary of degree M, and $a_1, \dots, a_r$, with r fixed, are distinct elements in $(\mathbb{F}[T]/m)^*$. Recall that $\hat{\mu}$ is the Fourier transform of a measure whose existence is established in Theorem 3.4. Let $\tilde{\mu}_{m;a_1,\dots,a_r}$ be the measure on $\mathbb{R}^r$ whose Fourier transform is

$$\hat{\mu}\left(\sqrt{\frac{q-1}{q}} \frac{\xi}{\sqrt{\Phi(m)M}} \right).$$

Then, as in [RS94], it is sufficient to prove that $\tilde{\mu}_{m;a_1,\dots,a_r}$ converges in measure to the Gaussian

$$\frac{e^{-(x_1^2+\cdots+x_r^2)}}{(2\pi)^{r/2}}\, dx_1 \dots dx_r$$

as $M \to \infty$. Fix a large A. For $\xi \in \mathbb{R}^r$ with $|\xi| \leqslant A$, we obtain

$$\begin{aligned} \log \hat{\tilde{\mu}}_{m;a_1,\dots,a_r}(\xi) &= \log \mathcal{B}_{m;a_1,\dots,a_r}\left(\sqrt{\frac{q-1}{q}} \frac{\xi}{\sqrt{\Phi(m)M}} \right) \\ &\quad + \sum_{\chi \neq \chi_0} \sum_{\Im(\gamma_\chi)>0} \log J_0\left(\left| \frac{2\gamma_\chi}{\gamma_\chi - 1} \right| \sqrt{\frac{q-1}{q}} \frac{|\sum_{l=1}^r \chi(a_l)\xi_l|}{\sqrt{\Phi(m)M}} \right) \end{aligned} \tag{48}$$

from Theorem 3.4. The proof of Theorem 6.5 will be completed by showing that the expression in (48) is asymptotic to $-(1/2)\sum_{l=1}^r {\xi_l}^2$ as $M \to \infty$. Again, by Levy's theorem, this implies the necessary convergence of $\tilde{\mu}_{m;a_1,\dots,a_r}$. As before, the most significant term in (48) comes from the first nonconstant term in the expansion of log of the Bessel function, and is given by

$$S := -\frac{1}{4} \sum_{\chi \neq \chi_0} \sum_{\Im(\gamma_\chi)>0} \left| \frac{2\gamma_\chi}{\gamma_\chi - 1} \right|^2 \left(\frac{q-1}{q} \right) \frac{|\sum_{l=1}^r \chi(a_l)\xi_l|^2}{\Phi(m)M}. \tag{49}$$

Define, for any non-principal Dirichlet character χ,

$$I(\chi) := \frac{1}{2} \sum_{\gamma_\chi} \left| \frac{\gamma_\chi}{\gamma_\chi - 1} \right|^2.$$

Here, the summation is taken for all inverse zeros γ_χ of absolute values $\sqrt{q}$, not only those with $\Im(\gamma_\chi) > 0$. It is easily shown that

$$S = -\frac{q-1}{q} \frac{1}{\Phi(m)M} \sum_{\chi \neq \chi_0} I(\chi) \left| \sum_{l=1}^r \chi(a_l)\xi_l \right|^2. \tag{50}$$

Let χ^* be the primitive Dirichlet character which induces χ, and let $M(\chi^*)$ be the degree of its modulus. Then, clearly $I(\chi) = I(\chi^*)$. Also, the technique used to establish (44) applies to $I(\chi^*)$ to yield

$$I(\chi^*) = \frac{q}{q-1} \frac{M(\chi^*)}{2} + O(\log M(\chi^*)).$$

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press

Then, from (50),

$$S = -\frac{1}{2\Phi(m)M}\sum_{\chi\neq\chi_0} M(\chi^*)\left|\sum_{l=1}^{r}\chi(a_l)\xi_l\right|^2 + O\left(A^2\frac{\log M}{M}\right). \tag{51}$$

The above summation can be simplified by applying the argument of Rubinstein and Sarnak [RS94, p. 186] with very minimal change. Essentially, this argument proves that the asymptotic behavior of S remains unchanged if $M(\chi^*)$ is replaced by M and if all of the cross terms in $|\sum_{l=1}^{r}\chi(a_l)\xi_l|^2$ are dropped. We conclude

$$S \to -\frac{1}{2}\sum_{l=1}^{r}{\xi_l}^2, \tag{52}$$

as $M\to\infty$. It remains to estimate that all of the other terms in (48) than S.

First, we let $d(m) := \sum_{f|m} 1$ be the number of monic divisors of m. Then, as with its number field counterpart, it is easy to see that $c(m,a) < d(m)$ for any $a \in (\mathbb{F}[T]/m)^*$ and $d(m) = O_\epsilon((q^M)^\epsilon)$ for any $\epsilon > 0$. Using this, one proves that

$$\log \mathcal{B}_{m;a_1,\dots,a_r}\left(\sqrt{\frac{q-1}{q}}\frac{\xi}{\sqrt{\Phi(m)M}}\right) = O\left(\frac{d(m)A}{\sqrt{\Phi(m)M}}\right). \tag{53}$$

Also, the higher terms in $\log J_0$ than S is $O(A^4/(\Phi(m)^2M))$. Combining all of the results so far,

$$\hat{\tilde{\mu}}_{m;a_1,\dots,a_r}(\xi) \to \exp\left(-\frac{1}{2}\sum_{l=1}^{r}{\xi_l}^2\right).$$

The proof of Theorem 6.5 is now complete.

References

Apo76 T. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics (Springer, New York, 1976).

Bil86 P. Billingsley, *Probability and measure*, second edition, Wiley Series in Probability and Mathematical Statistics: Probability and Mathematical Statistics (John Wiley & Sons, New York, 1986).

Cal06 J. Calcut, *Rationality and the tangent function*, Preprint (2006), available at http://www.ma.utexas.edu/users/jack/papers.htm.

Che53 P. L. Chebyshev, *Lettre de m. le professor tchébychev à m. fuss sur un nouveaux théorème relatif aux nombres premiers contenus dans les formes* $4n+1$*ets* $4n+3$, Bull. Cl. Phys. Acad. Imp. Sci. St. Petersburg **11** (1853), 208.

GM06 A. Granville and G. Martin, *Prime number races*, Amer. Math. Monthly **113** (2006), 1–33.

Lit28 J. E. Littlewood, *On the Class Number of the Corpus* $P(\sqrt{-k})$, Proc. London Math. Soc. (2) **27** (1928), 358–372.

Ros02 M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210 (Springer, New York, 2002).

RS94 M. Rubinstein and P. Sarnak, *Chebyshev's bias*, Expo. Math. **3** (1994), 173–197.

Byungchul Cha cha@muhlenberg.edu
Department of Mathematics and Computer Science, Muhlenberg College, 2400 Chew Street, Allentown, PA 18104, USA

https://doi.org/10.1112/S0010437X08003631 Published online by Cambridge University Press