Canad. Math. Bull Vol. 62 (1), 2019 pp. 149–167
http://dx.doi.org/10.4153/CMB-2018-002-4

One Level Density for Cubic Galois Number Fields

Patrick Meisner

Abstract. Katz and Sarnak predicted that the one level density of the zeros of a family of L-functions would fall into one of five categories. In this paper, we show that the one level density for L-functions attached to cubic Galois number fields falls into the category associated with unitary matrices.

1 Introduction

Given an L-function, the one-level density is the function

$$\mathscr{D}(L,f) := \sum_{\gamma} f\Big(\frac{\gamma \log X}{2\pi}\Big),$$

where f is an even Schwartz test function and the sum runs over all non-trivial zeros of the L-function $\rho = 1/2 + i\gamma$. The Generalized Riemann Hypothesis tells us that γ will always be real. However, we do not suppose this.

Remark 1.1 The log factor in the definition of the one-level density is to ensure our zeros have mean spacing 1.

One can think of f as a smooth approximation to the indicator function of an interval centered at 0. Therefore the one-level density can be thought of as a measure of how many zeros are close to the real line, the so-called low-lying zeros.

For a suitably nice family $\mathcal{F}$ of L-functions and Schwartz function f, Katz and Sarnak [5] predicted that

$$\big\langle \mathscr{D}(L,f) \big\rangle_{\mathcal{F}} := \lim_{X\to\infty} \frac{1}{|\mathcal{F}(X)|} \sum_{L\in\mathcal{F}(X)} \mathscr{D}(L,f) = \int_{-\infty}^{\infty} f(t)W(G)(t)dt,$$

where the $\mathcal{F}(X)$ are finite increasing subsets of $\mathcal{F}$ and $W(G)(t)$ is the one-level density scaling of eigenvalues near 1 in a group of random matrices (indicated by G). This group, G, is called the *symmetry type* of the family $\mathcal{F}$.

Received by the editors October 31, 2017; revised January 10, 2018.
Published electronically June 7, 2018.
The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement no. 320755.
AMS subject classification: **11M06**, 11M26, 11M50.
Keywords: L-function, one level density.

Moreover, Katz and Sarnak predicted that $W(G)(t)$ would fall into one of these five categories

$$W(G)(t) = \begin{cases} 1, & G = U, \\ 1 - \frac{\sin(2\pi t)}{2\pi t}, & G = Sp, \\ 1 + \frac{1}{2}\delta_0(t), & G = O, \\ 1 + \frac{\sin(2\pi t)}{2\pi t}, & G = SO(\text{even}), \\ 1 + \delta_0(t) - \frac{\sin(2\pi t)}{2\pi t}, & G = SO(\text{odd}), \end{cases}$$

where δ_0 is the Dirac distribution and U, Sp, O, SO(even), and SO(odd) are the groups of unitary, symplectic, orthogonal, even orthogonal, and odd orthogonal matrices, respectively.

1.1 Number Fields

In this section, we will discuss some known results for L-functions attached to number fields.

For any number field, K, define $\zeta_K(s) = \sum_{\mathfrak{a}} N\mathfrak{a}^{-s}$. Denote $\zeta_{\mathbb{Q}}(s) := \zeta(s)$. Then the L-function associated with the field K would be

$$L_K(s) = \frac{\zeta_K(s)}{\zeta(s)}.$$

Further, if we denote the discriminant of K by D_K, then the one-level density will be

$$\mathscr{D}(K, f) = \sum_{\gamma} f\Big(\frac{\gamma \log D_K}{2\pi}\Big), \tag{1.1}$$

i.e., set $X = D_K$. Then Katz and Sarnak [4] proved the following.

Theorem 1.2 *Let $\mathcal{F}(X)$ be the family of number fields of the form $\mathbb{Q}(\sqrt{8d})$ with $X \le d \le 2X$ and d square-free. Assuming GRH, if* $\operatorname{supp}(\widehat{f}) \subset (-2, 2)$, *then*

$$\lim_{X\to\infty} \frac{1}{|\mathcal{F}(X)|} \sum_{K\in\mathcal{F}(X)} \mathscr{D}(K, f) = \int_{\infty}^{\infty} f(t) W(Sp)(t) dt.$$

Therefore, we see that the symmetry type for quadratic extensions is symplectic.

Further, in his thesis [11], Yang considered the family of cubic non-Galois number fields.

Theorem 1.3 *Let $N_3(X)$ denote the set of cubic fields of discriminant between X and $2X$ and whose Galois closure is S_3. If* $\operatorname{supp}(\widehat{f}) \subset (-1/50, 1/50)$, *then*

$$\lim_{X\to\infty} \frac{1}{|N_3(X)|} \sum_{K\in N_3(X)} \mathscr{D}(K, f) = \int_{\infty}^{\infty} f(t) W(Sp)(t) dt.$$

Therefore, the symmetry type of cubic S_3-fields is symplectic as well.

https://doi.org/10.4153/CMB-2018-002-4 Published online by Cambridge University Press

1.2 Function Fields

Every finite extension of $\mathbb{F}_q(t)$ corresponds to a smooth projective curve C. We define the zeta-function of the curve as

$$Z_C(u) = \exp\Big(\sum_{n=1}^{\infty} N_n(C)\frac{u^n}{n}\Big),$$

where $N_n(C)$ is the number of $\mathbb{F}_{q^n}$-rational points on C. Since the GRH is known for $Z_C(u)$ (proved by Weil in [9]), we have

$$Z_C(u) = \frac{L_C(u)}{(1-u)(1-qu)},$$

where $L_C(u)$ is a polynomial that satisfies the function equations

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

where g is the genus of the curve C and all its roots lie on the "half-line" $|u| = q^{-1/2}$. Hence, we can find a unitary symplectic $2g \times 2g$ matrix Θ_C, called the *Frobenius class* of C, such that

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

Then the zeros of $L_C(u)$ correspond to the eigenangles of Θ_C.

Since the eigenangles of Θ_C are 2π-periodic, we need to modify the one-level density definition a bit. So, for an even Schwartz test function f, define

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

so that F is 2π-periodic and centered on an interval of size roughly $1/N$. Then for any $N \times N$ unitary matrix U with eigenangles $\theta_1 \dots, \theta_N$, define

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

Finally, we then get that the one-level density for C will be

$$\mathscr{D}(L_C, f) = Z_f(\Theta_C).$$

The literature on the one-level density in the function field setting give slightly different predictions than in the number field setting. For a suitably nice family of curves $\mathcal{F}$ and even Schwartz function f, the literature predicts

$$\frac{1}{|\mathcal{F}(X)|}\sum_{C\in\mathcal{F}(X)} Z_f(\Theta_C) = \int_G Z_f(U)dU + o(1),$$

where G is the symmetry type and dU is the Haar measure.

Specifically, Rudnick [7] proved the following theorem.

Theorem 1.4 *Let q be odd and let $\mathcal{F}_{2g+1}$ be the set of hyperelliptic curves with affine model $C\colon Y^2 = f(X)$ with $\deg(f) = 2g+1$ (and thus the genus of C is g). Then if* $\operatorname{supp}(\widehat{f}) \subset (-2,2)$,

$$\frac{1}{|\mathcal{F}_{2g+1}|}\sum_{C\in\mathcal{F}_{2g+1}} Z_f(\Theta_C) = \int_{USp(2g)} Z_f(U)dU + O\Big(\frac{1}{g}\Big).$$

Hence, the symmetry type of hyperelliptic curves is $USp(2g)$. This is to be expected, as all these curves correspond to quadratic extensions, and Theorem 1.2 shows that quadratic extensions in the number field setting have symmetry type Sp.

Bucur, Costa, David, Guerreiro, and Lowry-Duda [1] proved the following theorem.

Theorem 1.5 *Let $E_3(g)$ be the family of cubic non-Galois extension of $\mathbb{F}_q(X)$ with discriminant of degree $2g+4$. Then there exists a $\beta > 0$ such that if* $\operatorname{supp}(\widehat{f}) \subset (-\beta,\beta)$, *then*

$$\frac{1}{|E_3(g)|}\sum_{C\in E_3(g)} Z_f(\Theta_C) = \int_{USp(2g)} Z_f(U)dU + O\Big(\frac{1}{g}\Big).$$

This again, matches with what is know from the number field case in Theorem 1.3 as a cubic non-Galois extension would have Galois closure S_3.

Finally, in the same paper Bucur, Costa, David, Guerreiro, and Lowry-Duda extend Rudnick's result.

Theorem 1.6 *Let ℓ be an odd prime, $q \equiv 1 \mod \ell$, and let $\mathcal{F}_{g,\ell}$ be the moduli space of curves of ℓ covers of genus g. Then if* $\operatorname{supp}(\widehat{f}) \subset (-\frac{1}{\ell-1}, \frac{1}{\ell-1})$, *then*

$$\frac{1}{|\mathcal{F}_{g,\ell}|}\sum_{C\in\mathcal{F}_{g,\ell}} Z_f(\Theta_C) = \int_{U(2g)} Z_f(U)dU + O\Big(\frac{1}{g}\Big).$$

Here, we see a new symmetry type, that of $U(2g)$.

1.3 Main Theorem

The aim of this paper is to calculate the one-level density over cubic Galois number fields. Noticing the parallels in the function field setting, and the number field setting we can use Theorem 1.6 to predict that the symmetry type we should expect is U. Indeed, that is what we find.

Theorem 1.7 *Let $\mathcal{F}_3(X)$ be the family of cubic, Galois number fields of discriminant between X and $2X$. Then if f is an even Schwartz test function with* $\operatorname{supp}(\widehat{f}) \subset (-1/14, 1/14)$, *we have*

$$\frac{1}{|\mathcal{F}_3(X)|}\sum_{K\in\mathcal{F}_3(X)} \mathscr{D}(K,f) = \int_{-\infty}^{\infty} f(t)W(U)(t)dt + O\Big(\frac{1}{\log X}\Big).$$

Moreover, if we assume GRH, then we can take f with $\operatorname{supp}(\widehat{f}) \subset (-1/2, 1/2)$.

https://doi.org/10.4153/CMB-2018-002-4 Published online by Cambridge University Press

Two of the key ingredients of Theorem 1.7 are (1): 3 is a prime and (2): $\mathbb{Z}[\zeta_3]$ is a PID. Therefore, the same arguments could be extended to the family of $\mathbb{Z}/p\mathbb{Z}$ Galois number fields where p is an odd prime such that $\mathbb{Z}[\zeta_p]$ is a PID. Unfortunately, these conditions are very limiting as this is only true for primes less than 20. However, with this and Theorem 1.6, it is reasonable to conjecture the following.

Conjecture 1.8 *Let p be an odd prime and let $\mathcal{F}_p(X)$ be the family of $\mathbb{Z}/p\mathbb{Z}$ Galois number fields of discriminant between X and $2X$. Then there exists a $\beta > 0$ (dependent only on p) such that for every even Schwartz test function f such that* $\operatorname{supp}(\widehat{f}) \subset (-\beta, \beta)$, *we have*

$$\lim_{X\to\infty} \frac{1}{|\mathcal{F}_p(X)|} \sum_{K\in\mathcal{F}_p(X)} \mathscr{D}(K, f) = \int_{\infty}^{\infty} f(t)W(U)(t)dt.$$

2 Classifying Cubic Galois Extensions

In this section we will give a construction for all cubic Galois extensions of $\mathbb{Q}$.

2.1 Class Field Theory

We will begin by stating some main results of class field theory. For general reference, we refer the reader to [2].

Let K be a global field. Denote by $\mathcal{D}(K)$ the group of divisors of K. For any effective divisor $\mathfrak{m} \in \mathcal{D}(K)$, define

$$\begin{aligned}
\mathcal{D}_{\mathfrak{m}}(K) &= \{D \in \mathcal{D}(K) : \operatorname{supp}(D) \cap \operatorname{supp}(\mathfrak{m}) = \varnothing\},\\
\mathcal{P}_{\mathfrak{m}}(K) &= \{(a) : a \in K^*, a \equiv 1 \mod \mathfrak{P}^{\operatorname{ord}_{\mathfrak{P}}(\mathfrak{m})} \text{ for all places } \mathfrak{P} \text{ of } K\},\\
\mathcal{C}\ell_{\mathfrak{m}}(K) &= \mathcal{D}_{\mathfrak{m}}(K)/\mathcal{P}_{\mathfrak{m}}(K).
\end{aligned}$$

For a divisor D, we use $\operatorname{supp}(D)$ to denote the support of D: the set of primes that appear in D with non-zero coefficient. This is not to be confused with the support of a function as used in Section 1. $\mathcal{P}_{\mathfrak{m}}(K)$ is the *ray* of K modulo $\mathfrak{m}$, and $\mathcal{C}\ell_{\mathfrak{m}}(K)$ is the *ray class group* of K modulo $\mathfrak{m}$.

Theorem 2.1 *There is a one-to-one correspondence between finite abelian Galois extensions L of K unramified outside of $\mathfrak{m}$ with Galois group G and subgroups H of $\mathcal{C}\ell_{\mathfrak{m}}(K)$ such that $G \cong \mathcal{C}\ell_{\mathfrak{m}}(K)/H$.*

If we set $K = \mathbb{Q}$, then $\mathcal{D}(\mathbb{Q}) \cong \mathbb{Q}_{\geq 0}$ and effective divisors correspond to positive integers. Hence, we will write an effective divisor of $\mathbb{Q}$ as m instead of $\mathfrak{m}$ to illustrate that it is an integer. Further, we will denote by $\operatorname{supp}(m)$ the set of primes dividing m. Therefore, from the definitions, we get that

$$\mathcal{C}\ell_m(\mathbb{Q}) = (\mathbb{Z}/m\mathbb{Z})^*.$$

Moreover, if we want to find subgroups of $\mathcal{C}\ell_m(\mathbb{Q})$ such that

$$\mathcal{C}\ell_m(\mathbb{Q})/H \cong \mathbb{Z}/3\mathbb{Z}$$

it suffices to look for subgroups of index 3 of the three torsion subgroup of the ray class group:

$$\mathcal{C}\ell_m(\mathbb{Q})[3] = (\mathbb{Z}/3\mathbb{Z})^{\delta_m} \times \prod_{\substack{p|m \\ p\equiv 1 \mod 3}} \mathbb{Z}/3\mathbb{Z},$$

where $\delta_m = 1$ if $9|m$ and 0 otherwise. Finally, since $\mathcal{C}\ell_m(\mathbb{Q})$ is a finite abelian group, subgroups of $\mathcal{C}\ell_m(\mathbb{Q})$ of index 3 are in one-to-one correspondence with subgroups isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

Before we state the next result, we need a definition.

Definition 2.2 Call an integer 3-*split* if all its prime divisors are congruent to 0 or 1 mod 3.

Lemma 2.3 *For any integer m, there is a two-to-one correspondence between cube-free* 3*-split integers, D, such that* $\operatorname{supp}(D) \subset \operatorname{supp}(m)$ *and cubic Galois extensions of* $\mathbb{Q}$ *unramified outside of the primes dividing m.*

Proof As was stated above, there is a one-to-one correspondence between $\mathbb{Z}/3\mathbb{Z}$ subgroups of $\mathcal{C}\ell_m(\mathbb{Q})[3]$ and cubic Galois extensions of $\mathbb{Q}$ unramified outside of the primes dividing m. There is a one-to-two correspondence between such subgroups and non-zero elements of

$$\mathcal{C}\ell_m(\mathbb{Q})[3] = (\mathbb{Z}/3\mathbb{Z})^{\delta_m} \times \prod_{\substack{p|m \\ p\equiv 1 \mod 3}} \mathbb{Z}/3\mathbb{Z}.$$

Let e_p be the coordinates of a element in $\mathcal{C}\ell_m(\mathbb{Q})[3]$. Now we construct the cube-free 3-split integer as

$$D := \prod_{\substack{p|m \\ p\equiv 0,1 \mod 3}} p^{e_p}.$$

This correspondence is one-to-two, since there are two generators for each subgroup. ■

Corollary 2.4 *Let D_1 and D_2 be two distinct cube-free* 3*-split integers. Then they correspond to the same cubic Galois extension of* $\mathbb{Q}$ *if and only if there exists a $D \in \mathbb{Q}$ such that $D_2 = D_1^2 D^3$.*

Proof Let

$$D_i = \prod p^{e_{p,i}}$$

be the prime factorization of D_i, $i = 1, 2$. Then by the proof of Lemma 2.3, we see that D_1 and D_2 correspond to the same cubic extension of $\mathbb{Q}$ if and only if the vectors $(e_{p,1})$ and $(e_{p,2})$ generate the same subgroup in $\mathcal{C}\ell_m(\mathbb{Q})[3]$ where m is any positive integer such that $\operatorname{supp}(D_1) \cup \operatorname{supp}(D_2) \subset \operatorname{supp}(m)$. Since $D_1 \neq D_2$, this is if and only if $e_{p,2} \equiv 2e_{p,1} \mod 3$ for all primes p. Setting

$$D = \prod p^{\frac{e_{p,2}-2e_{p,1}}{3}}$$

suffices. ■

2.2 Explicit Correspondence

In this section, we will construct an explicit correspondence between cube-free 3-split integers and cubic Galois extensions of $\mathbb{Q}$.

Let ζ_3 be a primitive cubic root of unity and denote $K = \mathbb{Q}(\zeta_3)$. The following are well-known facts about the cyclotomic field K.

Lemma 2.5 (i) *The only ramified prime in K is 3, and a prime p splits if $p \equiv 1 \mod 3$ and is inert if $p \equiv 2 \mod 3$.*
(ii) *$\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ is a PID.*
(iii) *$\mathcal{O}_K^* = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$*
(iv) *K/Q is Galois with $\mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$*

Denote the unique prime dividing 3 in $\mathcal{O}_K$ by $\mathfrak{P}_3$. Hence, $3\mathcal{O}_K = \mathfrak{P}_3^2$. Moreover, denote the unique generator of $\mathrm{Gal}(K/\mathbb{Q})$ by σ.

Lemma 2.6 *Let D be a 3-split integer. Then there exists $D_1, D_2 \in \mathcal{O}_K$ such that $D = \pm D_1 D_2$, $\sigma(D_1) = D_2$ and $\gcd(D_1, D_2) = \mathfrak{P}_3^{v_3(D)}$.*

Proof Since D is 3-split, we can write

$$D = 3^{e_3} \prod_{\substack{p|D \\ p\neq 3}} p^{e_p},$$

where all the primes appearing in the product have the property that $p \equiv 1 \mod 3$ and hence split in K. That is, we can write $p\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$, where $\mathfrak{P}_1^\sigma = \mathfrak{P}_2$.

Define

$$\mathcal{D}_i := \prod_{\substack{p|D \\ p\neq 3}} \mathfrak{P}_i^{e_p}.$$

Since $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$ is a PID, we can find D_i' such that $\mathcal{D}_i = (D_i')$. Moreover, since $\mathcal{D}_1^\sigma = \mathcal{D}_2$, we can assume $\sigma(D_1') = D_2'$. Now we notice that $3 = (1-\zeta_3)(1-\bar{\zeta}_3)$. Define

$$D_1 = (1-\zeta_3)^{e_3} D_1' \quad D_2 = (1-\bar{\zeta}_3)^{e_3} D_2'.$$

Then $\sigma(D_1) = D_2$ and $D\mathcal{O}_K = (D_1 D_2)$. Therefore, $D = uD_1D_2$ for some unit u of $\mathcal{O}_K$. However, since both D and D_1D_2 are fixed by σ, we see that u is also fixed by σ, so $u = \pm 1$.

Finally, we remark that $\gcd(D_1', D_2') = 1$ and $\mathfrak{P}_3 = (1-\zeta_3)\mathcal{O}_K = (1-\bar{\zeta}_3)\mathcal{O}_K$. ∎

Definition 2.7 For any 3-split integer, we will call the factorization $D = \pm D_1 D_2$ as in Lemma 2.6 its 3-*split factorization*.

Remark 2.8 The 3-split factorization of an integer is not unique. It depends on choices of primes $\mathfrak{P} \in \mathcal{O}_K$ dividing 3-split primes $p \in \mathbb{Z}$. As we will see, the classification depends on the choice of factorization of the 3-split primes in $\mathcal{O}_K$, and hence is not canonical. However, when we count such extensions this choice will not matter (as it shouldn't). Therefore, for every 3-split prime $p \neq 3$, we will fix a prime $\mathfrak{P} \in \mathcal{O}_K$ dividing it and thus fix its 3-split factorization $p = \pm p_1 p_2$ where $\mathfrak{P} = p_1\mathcal{O}_K$

and $\mathfrak{P}^\sigma = p_2\mathcal{O}_K$. Further, we fix a generator of $\mathfrak{P}_3$, the unique prime dividing 3, to be $1-\zeta_3$. Consequently, this fixes a 3-split factorization of all 3-split integers.

As a result of fixing these primes we see that if D and E are two 3-split integers with 3-split factorizations $D = \pm D_1D_2$ and $E = \pm E_1E_2$, then $\gcd(D_1, E_2) = \gcd(D_2, E_1) = \mathfrak{P}_3^e$ for some integer e. This is due to the fact that the primes dividing D_1 and E_1 are the $\mathfrak{P}$ corresponding to the primes p dividing D and E, respectively, whereas the primes dividing D_2 and E_2 are the $\mathfrak{P}^\sigma$.

Lemma 2.9 *For any 3-split integer D with 3-split factorization $D = \pm D_1D_2$, the extension $K'_D := \mathbb{Q}(\zeta_3, \sqrt[3]{D_1D_2^2})$ is a Galois extension of $\mathbb{Q}$ with Galois group $\mathbb{Z}/6\mathbb{Z}$.*

Proof By Kummer theory, we have that K'_D is a Galois extension of K with Galois group $\mathbb{Z}/3\mathbb{Z}$ (since $\mu_3 \subset K$). Let τ be a generator of $\mathrm{Gal}(K'_D/K)$ such that $\tau(\sqrt[3]{D_1D_2^2}) = \zeta_3\sqrt[3]{D_1D_2^2}$ and let σ be the generator of $\mathrm{Gal}(K/\mathbb{Q})$ as above.

We know that $\sigma(D_1D_2^2) = D_1^2D_2$, and so, up to a choice of cube root of $D_1^2D_2$, we get $\sigma(\sqrt[3]{D_1D_2^2}) = \sqrt[3]{D_1^2D_2}$. Therefore, K'_D is a Galois extension of $\mathbb{Q}$.

Thus, σ is an element of order 2 and τ is an element of order 3 in $\mathrm{Gal}(K'_D/\mathbb{Q})$. Hence, σ and τ generate $\mathrm{Gal}(K'_D/\mathbb{Q})$, since $[K'_D : \mathbb{Q}] = 6$. So it remains to show that σ and τ commute.

Clearly, $\sigma\tau(\zeta_3) = \tau\sigma(\zeta_3)$, since τ fixes K. Now,

$$\sigma\tau\big(\sqrt[3]{D_1D_2^2}\big) = \sigma\big(\zeta_3\sqrt[3]{D_1D_2^2}\big) = \bar{\zeta}_3\sqrt[3]{D_1^2D_2},$$

$$\tau\sigma\big(\sqrt[3]{D_1D_2^2}\big) = \tau\big(\sqrt[3]{D_1^2D_2}\big) = \tau\Big(\frac{\sqrt[3]{D_1D_2^2}^{\,2}}{D_2}\Big) = \frac{\zeta_3^2\sqrt[3]{D_1D_2^2}^{\,2}}{D_2} = \bar{\zeta}_3\sqrt[3]{D_1^2D_2}.$$

Therefore, σ and τ commute and $\mathrm{Gal}(K'_D/\mathbb{Q}) = \mathbb{Z}/6\mathbb{Z}$, as claimed. ∎

Let $H = \{1, \sigma\} \subset \mathrm{Gal}(K'_D/\mathbb{Q})$ and let $K_D = (K'_D)^H$ be the fixed field of H. Then

$$K_D = \mathbb{Q}\big(\sqrt[3]{D_1D_2^2} + \sqrt[3]{D_1^2D_2}\big)$$

is Galois with $\mathrm{Gal}(K_D/\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$.

Lemma 2.10 *Let D_1, D_2 be distinct 3-split integers. Then $K_{D_1} = K_{D_2}$ if and only if there exists a $D \in \mathbb{Q}$ such that $D_2 = D_1^2D^3$.*

Proof Since $K'_{D_i} = K_{D_i}(\zeta_3)$ and $K_{D_i} = (K'_{D_i})^H$, we have $K_{D_1} = K_{D_2}$ if and only if $K'_{D_1} = K'_{D_2}$.

Let $D_1 = \pm D_{1,1}D_{1,2}$, $D_2 = \pm D_{2,1}D_{2,2}$ be the 3-split factorization of D_1 and D_2. Then Kummer Theory applied to K tells us that $K'_{D_1} = K'_{D_2}$ if and only if there exists $E \in K^*$ such that

$$D_{2,1}D_{2,2}^2 = D_{1,2}D_{1,1}^2E^3. \tag{2.1}$$

Let $p \neq 3$ be a prime and let $\mathfrak{P}$ be the fixed prime lying above it in $\mathcal{O}_K$. Then by Remark 2.8, we have that $\mathfrak{P}$ does not divide $D_{1,2}$ nor $D_{2,2}$. Thus, $v_{\mathfrak{P}}(D_{1,1}) = v_p(D_1)$ and $v_{\mathfrak{P}}(D_{1,2}) = v_p(D_2)$.

https://doi.org/10.4153/CMB-2018-002-4 Published online by Cambridge University Press

Combining this with (2.1), we get

$$v_P(D_2) = v_{\mathfrak{P}}(D_{2,1}D_{2,2}^2) = v_{\mathfrak{P}}(D_{1,2}D_{1,1}^2E^3) = 2v_p(D_1) + 3v_{\mathfrak{P}}(E).$$

In particular, $v_p(D_2) \equiv 2v_p(D_1) \mod 3$.

Finally, if we let $\mathfrak{P}_3$ be the unique prime lying over 3 in K, and consider just the powers of $\mathfrak{P}_3$ appearing in (2.1), then by the construction of the 3-split factorization we get

$$3^{v_3(D_2)}(1-\zeta_3)^{v_3(D_2)} = 3^{v_3(D_1)}(1-\bar{\zeta}_3)^{v_3(D_1)}E_3^3,$$

where E_3 is the part of E divisible by $\mathfrak{P}_3$. Using the fact that $1-\zeta_3 = 3/(1-\bar{\zeta}_3)$ and rearranging, we get

$$3^{2v_3(D_2)-v_3(D_1)} = (1-\bar{\zeta}_3)^{v_3(D_1)+v_3(D_2)}E_3^3. \tag{2.2}$$

Now, $E_3 = u(1-\zeta_3)^n$ for some unit u and some integer n. Since all the units satisfy $u^3 = \pm 1$, we have $E_3^3 = \pm(1-\zeta_3)^{3n}$. Therefore, (2.2) implies that $v_3(D_1)+v_3(D_2) = 3n$. In particular, $v_3(D_1) \equiv 2v_3(D_2) \mod 3$, as required. ■

Proposition 2.11 *The two-to-one correspondence from cube-free* 3*-split integers D such that* $\operatorname{supp}(D) \subset \operatorname{supp}(m)$ *to cubic Galois extensions of* $\mathbb{Q}$ *unramified outside the primes dividing m, as in Lemma 2.3, can be explicitly given by*

$$D \longmapsto K_D = \mathbb{Q}\Big(\sqrt[3]{D_1D_2^2} + \sqrt[3]{D_1^2D_2}\Big).$$

Proof We must first show that this map is well defined. That is, that K_D is cubic, Galois, and unramified outside of the primes dividing m. We have already shown that K_D is in fact cubic and Galois. Since $[K:\mathbb{Q}] = 2$ is coprime to $3 = [K_D:\mathbb{Q}] = [K_D':K]$, we see that a prime ramifies in K_D if and only if a prime lying above it in $\mathcal{O}_K$ ramifies in K_D' if and only if $p|D$. Therefore, the map is well defined. Finally, Lemmas 2.3, 2.10, and Corollary 2.4 show that this map is two-to-one and surjective. ■

From now on, D will always denote a cube-free 3-split integer.

2.3 Discriminant

Denote Δ_D as the discriminant of K_D. If we let f_D be the conductor of K_D, then we have $\Delta_D = f_D^2$. Theorem 10 of [3] states that $v_p(f) = 1$ or 0 if $p \neq 3$, while $v_3(f) = 2$ or 0. Thus, we get that

$$\Delta_D = 3^{4\delta_D} \prod_{p \text{ ramified in } K_D} p^2, \tag{2.3}$$

where δ_D is 1 if 3 is ramified in K_D and 0 otherwise. Therefore, it remains to determine which primes ramify in K_D.

As was mentioned in the proof of Proposition 2.11, a prime p ramifies in K_D if and only if $p|D$. Since D is cube-free we can find d_1, d_2 square-free, coprime, and coprime to 3 such that $D = 3^{v_3(D)}d_1d_2^2$. Then we have

$$\Delta_D = (9^{\delta_D}d_1d_2)^2,$$

where δ_D is 1 if $3|D$ and 0 otherwise. (Note that this definition of δ_D agrees with the definition in (2.3) as 3 is ramified if and only if $3|D$.)

https://doi.org/10.4153/CMB-2018-002-4 Published online by Cambridge University Press

Finally, recall that $\mathcal{F}_3(X)$ is the set of cubic, Galois extensions of determinant between X and $2X$. Then [10, Theorem 1.2] states that there exists a constant c, such that

$$|\mathcal{F}_3(X)| \sim cX^{1/2}. \tag{2.4}$$

3 L-Functions and Explicit Formula

Before we begin, we will fix some notation. We will denote p as a prime in $\mathbb{Q}$, $\mathfrak{p}$ as a prime in K_D, and $\mathfrak{P}$ as a prime in $K = \mathbb{Q}(\zeta_3)$. Hence, when we write an infinite product over primes, the set of primes that we run over will be indicated by which of the above three symbols we use. Moreover, we will denote by $N\mathfrak{p}$ and $N\mathfrak{P}$ the norms of $\mathfrak{p}$ and $\mathfrak{P}$ over $\mathbb{Q}$. Later, in Section 4, we will also use ℓ to denote a prime in $\mathbb{Q}$ and $\mathfrak{l}$ a prime dividing it in K and $N\mathfrak{l}$ to denote the norm over $\mathbb{Q}$.

For any prime p denote by $e(p)$ and $f(p)$ the ramification index and inertial degree of p in K and by $e_D(p)$ and $f_D(p)$ the ramification index and inertial degree of p in K_D. Further, let $g(p)$ and $g_D(p)$ be the number or primes dividing p in K and K_D, respectively.

3.1 L-Functions

Let $\zeta(s)$, $\zeta_K(s)$ and $\zeta_D(s)$ be the ζ-functions of $\mathbb{Q}$, K and K_D, respectively. That is,

$$\zeta(s) = \prod_p \Big(1 - \frac{1}{p^s}\Big)^{-1}, \quad \zeta_K(s) = \prod_{\mathfrak{P}} \Big(1 - \frac{1}{N\mathfrak{P}^s}\Big)^{-1}, \quad \zeta_D(s) = \prod_{\mathfrak{p}} \Big(1 - \frac{1}{N\mathfrak{p}^s}\Big)^{-1},$$

which all converge for $\Re(s) > 1$.

Let

$$L_K(s) = \frac{\zeta_K(s)}{\zeta(s)} \quad \text{and} \quad L_D(s) = \frac{\zeta_D(s)}{\zeta(s)}$$

be the L-functions of K and K_D, respectively.

Since both K and K_D are Galois, we can rewrite ζ_K and ζ_D as

$$\zeta_K(s) = \prod_p \Big(1 - \frac{1}{p^{f(p)s}}\Big)^{-g(p)},$$
$$\zeta_D(s) = \prod_p \Big(1 - \frac{1}{p^{f_D(p)s}}\Big)^{-g_D(p)}.$$

From Lemma 2.5, we have that

$$(e(p), f(p), g(p)) = \begin{cases} (2,1,1) & p = 3, \\ (1,1,2) & p \equiv 1 \mod 3, \\ (1,2,1) & p \equiv 2 \mod 3. \end{cases}$$

Therefore, it remains to determine the possible values of $(e_D(p), f_D(p), g_D(p))$.

Since $[K:\mathbb{Q}] = 2$ is coprime to $[K_D:\mathbb{Q}] = 3$ and K'_D is the compositum of K and K_D, we get that if $\mathfrak{P}$ is the prime dividing p in K that was fixed in Remark 2.8, then

$$\big(e_D(p), f_D(p), g_D(p)\big) = \big(e_{K'_D/K}(\mathfrak{P}), f_{K'_D/K}(\mathfrak{P}), g_{K'_D/K}(\mathfrak{P})\big).$$

A prime $\mathfrak{P}$ in K ramifies in K'_D if $\mathfrak{P}|D_1D_2^2$, splits if $D_1D_2^2$ is a cube modulo $\mathfrak{P}$ and is inert otherwise. Therefore,

$$(e_D(p), f_D(p), g_D(p)) = \begin{cases} (3,1,1) & p|D, \\ (1,1,3) & \left(\frac{D_1D_2^2}{\mathfrak{P}}\right)_3 = 1, \\ (1,3,1) & \left(\frac{D_1D_2^2}{\mathfrak{P}}\right)_3 \neq 0,1, \end{cases} \tag{3.1}$$

where $\left(\frac{\cdot}{\cdot}\right)_3$ is the cubic residue symbol for K.

Since $D_2 = \sigma(D_1)$, where σ is the generator of $\mathrm{Gal}(K/\mathbb{Q})$, we get that

$$\left(\frac{D_2}{\mathfrak{P}}\right)_3 = \sigma\left(\frac{D_1}{\mathfrak{P}}\right)_3 = \left(\frac{D_1}{\mathfrak{P}}\right)_3^2.$$

Hence,

$$\left(\frac{D_1D_2^2}{\mathfrak{P}}\right)_3 = \left(\frac{D_1}{\mathfrak{P}}\right)_3^2.$$

Now, every integer can be written as DD' where D is 3-split and all of the primes dividing D' are $2 \mod 3$. Define a multiplicative character on the integers as

$$\chi_p(DD') = \left(\frac{D_1}{\mathfrak{P}}\right)_3. \tag{3.2}$$

Then we can rewrite (3.1) as

$$(e_D(p), f_D(p), g_D(p)) = \begin{cases} (3,1,1) & p|D, \\ (1,1,3) & \chi_p(D) = 1, \\ (1,3,1) & \chi_p(D) \neq 0,1. \end{cases}$$

Note that χ_p is not a Dirichlet character.

Remark 3.1 In the case of $p = 3$, everything will be a cube modulo $\mathfrak{P}_3$. Hence, we have $\chi_3(D) = 1$ unless $3|D$, and therefore

$$(e_D(3), f_D(3), g_D(3)) = \begin{cases} (3,1,1) & 3|D, \\ (1,1,3) & \text{otherwise.} \end{cases}$$

Further, if n is an integer such that all its prime factors are $2 \mod 3$, then $\chi_p(n) = 1$.

Putting everything together, we can write the L-functions of K and K_D as

$$\begin{aligned} L_K(s) &= \prod_{p\equiv 1 \mod 3}\left(1-\frac{1}{p^s}\right)^{-1}\prod_{p\equiv 2 \mod 3}\left(1+\frac{1}{p^s}\right)^{-1}, \\ L_D(s) &= \prod_{\substack{p \\ \chi_p(D)=1}}\left(1-\frac{1}{p^s}\right)^{-2}\prod_{\substack{p \\ \chi_p(D)\neq 0,1}}\left(1+\frac{1}{p^s}+\frac{1}{p^{2s}}\right)^{-1}. \end{aligned} \tag{3.3}$$

If χ is any character on K modulo $\mathfrak{f}$, we define the L-function associated with this character as

$$L_K(\chi, s) = \prod_{\mathfrak{P}}\left(1-\frac{\chi_p(\mathfrak{P})}{N\mathfrak{P}^s}\right)^{-1}.$$

Finally, we will need a zero density theorem. We use [6, Theorem 2.3].

Theorem 3.2 *For any* $1/2 \le \alpha \le 1$ *and* $T > 0$*, let* $N(\alpha, T, \chi)$ *be the number of zeros* $\rho = \beta + i\gamma$ *of* $L_K(\chi, s)$ *with* $\alpha \le \beta \le 1$ *and* $|\gamma| \le T$*. Then there exists an* $A > 0$ *such that*

$$\sum_{q \le Q} \sum_{\chi \bmod q}^{*} N(\alpha, T, \chi) \ll (Q^2 T)^{\frac{4(1-\alpha)}{3-2\alpha}} (\log QT)^A,$$

where $\sum^*$ *indicates that we sum over principal characters.*

3.2 Explicit Formula

Since K_D has one embedding into $\mathbb{R}$ and two embeddings into $\mathbb{C}$, the function

$$\Lambda_D(s) := |\Delta_D|^{s/2} \Gamma_{\mathbb{R}}(s) \Gamma_{\mathbb{C}}(s) \zeta_D(s)$$

satisfies the functional equation

$$\Lambda_D(s) = \Lambda_D(1-s),$$

where

$$\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2) \quad \Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s) = \Gamma_{\mathbb{R}}(s)\Gamma_{\mathbb{R}}(s+1)$$

and $\Gamma(s)$ is the usual Gamma function.

Let $\rho_{D,j} = 1/2 + i\gamma_{D,j}$ be the zeros of $L_D(s)$ and let f be an even Schwartz function. Proposition 2.1 of [8] gives the explicit formula

$$\sum f(\gamma_{D,j}) = \frac{1}{2\pi} \int_{-\infty}^{\infty} f(x) \log \Delta_D dx - \frac{2}{2\pi} \sum_{n=1}^{\infty} \frac{\Lambda(n)\lambda_D(n)}{\sqrt{n}} \widehat{f}\Big(\frac{\log n}{2\pi}\Big) + C_f,$$

where the sum runs over all zeros of $L_D(s)$, $\Lambda(n)$ is the von-Magoldt function, $\lambda_D(n)$ satisfies

$$\frac{L_D'(s)}{L_D(s)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)\lambda_D(n)}{n^s}$$

and

$$C_f = \frac{1}{2\pi} \int_{-\infty}^{\infty} f(x) \bigg(2\frac{\Gamma_{\mathbb{R}}'}{\Gamma_{\mathbb{R}}}\Big(\frac{1}{2} + ix\Big) + 2\frac{\Gamma_{\mathbb{R}}'}{\Gamma_{\mathbb{R}}}\Big(\frac{1}{2} - ix\Big) + \frac{\Gamma_{\mathbb{R}}'}{\Gamma_{\mathbb{R}}}\Big(\frac{3}{2} + ix\Big) + \frac{\Gamma_{\mathbb{R}}'}{\Gamma_{\mathbb{R}}}\Big(\frac{3}{2} - ix\Big) \bigg) dx$$

is independent of our choice of D.

Recalling that the definition of $\mathscr{D}(K, f)$ from (1.1) requires multiplying the zeros by a factor of $L := \frac{\log \Delta_D}{2\pi}$, we apply the explicit formula and the definition of $\Lambda(n)$ to get

$$\text{(3.4)} \quad \mathscr{D}(K_D, f) = \sum f(L\gamma_{D,j}) = \int_{-\infty}^{\infty} f(x) dx - \frac{2}{\log \Delta_D} \sum_{m=1}^{\infty} \sum_{p} \frac{\lambda_D(p^m) \log p}{\sqrt{p^m}} \widehat{f}\Big(\frac{\log p^m}{\log \Delta_D}\Big) + \widetilde{C_f}(D),$$

where we use the observation that $\widehat{f(Lx)} = 1/L \widehat{f}(x/L)$ and $\widetilde{C_f}(D)$ is the same as C_f with f replaced with $f(L\cdot)$.

3.3 Main Term

Applying the explicit formula (3.4), we get

$$\frac{1}{|\mathcal{F}_3(X)|}\sum_{K_D\in\mathcal{F}_3(X)}\mathscr{D}(K_D,f)=\int_{-\infty}^{\infty}f(t)W(U)(t)dt-ET,$$

where

$$ET=\frac{1}{|\mathcal{F}_3(X)|}\sum_{K_D\in\mathcal{F}_3(X)}\Big(\frac{2}{\log\Delta_D}\sum_{m=1}^{\infty}\sum_{p}\frac{\lambda_D(p^m)\log p}{\sqrt{p^m}}\widehat{f}\Big(\frac{\log p^m}{\log\Delta_D}\Big)+\widetilde{C_f}(D)\Big). \tag{3.5}$$

So it remains to show that $ET=O\big(\frac{1}{\log X}\big)$.

4 Error Term

First, we note that if $K_D\in\mathcal{F}_3(X)$, then $X\le\Delta_D\le 2X$, and so $\log\Delta_D\sim\log X$, and we can rewrite (3.5)

$$ET\sim\frac{1}{c\sqrt{X}}\sum_{K_D\in\mathcal{F}_3(X)}\frac{2}{\log X}\Big(\sum_{m=1}^{\infty}\sum_{p}\frac{\lambda_D(p^m)\log p}{\sqrt{p^m}}\widehat{f}\Big(\frac{\log p^m}{\log X}\Big)+\widetilde{C_f}(D)\Big),$$

where we also use (2.4) to write $|\mathcal{F}_3(X)|\sim c\sqrt{X}$.

4.1 Easy Error Terms

In this section, we show that most of terms of ET are trivially $O\big(\frac{1}{\log X}\big)$.

By a change of variable in the definition C_f, we see that $\widetilde{C_f}(D)=O\big(\frac{1}{\log\Delta_D}\big)$, and hence

$$\frac{1}{c\sqrt{X}}\sum_{K_D\in\mathcal{F}_3(X)}\widetilde{C_f}(D)=O\Big(\frac{1}{\sqrt{X}}\sum_{K_D\in\mathcal{F}_3(X)}\frac{1}{\log\Delta_D}\Big)=O\Big(\frac{1}{\log X}\Big).$$

Now, we use the known bound $\lambda_D(p^m)=O(m)$ and the trivial bound $\widehat{f}(x)=O(1)$ to get

$$\begin{aligned}\frac{1}{c\sqrt{X}}\sum_{K_D\in\mathcal{F}_3(X)}\frac{2}{\log X}\sum_{m=3}^{\infty}\sum_{p}\frac{\lambda_D(p^m)\log p}{\sqrt{p^m}}\widehat{f}\Big(\frac{\log p^m}{\log X}\Big)\\ \ll\frac{1}{\sqrt{X}\log X}\sum_{K_D\in\mathcal{F}_3(X)}\sum_{p}\sum_{m=3}^{\infty}\frac{m\log p}{\sqrt{p^m}}\\ \ll\frac{1}{\log X}\sum_{p}\frac{1}{p^{3/2-\epsilon}}=O\Big(\frac{1}{\log X}\Big).\end{aligned}$$

It remains to determine what happens to the sums when $m=1$ or 2.

https://doi.org/10.4153/CMB-2018-002-4 Published online by Cambridge University Press

4.2 Coefficients of $\frac{L_D'}{L_D}$

Direct computation from (3.3) shows

$$\lambda_D(p) = \lambda_D(p^2) = \begin{cases} 0 & \chi_p(D) = 0, \\ 2 & \chi_p(D) = 1, \\ -1 & \chi_p(D) \neq 0, 1. \end{cases}$$

Moreover, if χ_p is as in (3.2), it is easy to see that

$$\lambda_D(p) = \lambda_D(p^2) = \chi_p(D) + \chi_p^2(D),$$

since χ_p is a cubic character.

Therefore, we need to estimate

$$\frac{1}{\sqrt{X}\log X} \sum_{K_D \in \mathcal{F}_3(X)} \sum_p \frac{\log p(\chi_p(D) + \chi_p^2(D))}{\sqrt{p^m}} \widehat{f}\Big(\frac{\log p^m}{\log X}\Big)$$

for $m = 1, 2$.

Since χ_p is a cubic character, we have $\chi_p^2 = \overline{\chi_p}$. Hence, it will be enough to determine

$$\frac{1}{\sqrt{X}\log X} \sum_{K_D \in \mathcal{F}_3(X)} \sum_p \frac{\chi_p(D)\log p}{\sqrt{p^m}} \widehat{f}\Big(\frac{\log p^m}{\log X}\Big) \tag{4.1}$$

for $m = 1, 2$.

Applying Proposition 2.11, we can write (4.1) as

$$\frac{1}{\sqrt{X}\log X} \sideset{}{'}\sum_{\sqrt{X} \le d_1 d_2 \le \sqrt{2X}} \sum_p \frac{\chi_p(d_1 d_2^2)\log p}{\sqrt{p^m}} \widehat{f}\Big(\frac{\log p^m}{\log X}\Big)$$
$$+ \frac{1}{\sqrt{X}\log X} \sideset{}{'}\sum_{\sqrt{X/81} \le d_1 d_2 \le \sqrt{2X/81}} \sum_p \frac{\chi_p(3d_1 d_2^2)\log p}{\sqrt{p^m}} \widehat{f}\Big(\frac{\log p^m}{\log X}\Big)$$
$$+ \frac{1}{\sqrt{X}\log X} \sideset{}{'}\sum_{\sqrt{X/81} \le d_1 d_2 \le \sqrt{2X/81}} \sum_p \frac{\chi_p(9d_1 d_2^2)\log p}{\sqrt{p^m}} \widehat{f}\Big(\frac{\log p^m}{\log X}\Big),$$

where $\sum'$ means we are summing over all pairs d_1, d_2 that are square-free, 3-split, coprime and coprime to 3. We see then it will be sufficient to estimate

$$\frac{1}{\sqrt{X}\log X} \sum_p \frac{\log p}{\sqrt{p^m}} \widehat{f}\Big(\frac{\log p^m}{\log X}\Big) \sideset{}{'}\sum_{d_1 d_2 \le Y} \chi_p(d_1 d_2^2)$$

for $m = 1, 2$.

4.3 Generating Series

Fix a prime p and consider the generating series

$$\mathcal{G}_p(s) = \sideset{}{'}\sum_{d_1, d_2} \frac{\chi_p(d_1 d_2^2)}{(d_1 d_2)^s},$$

which converges for $\Re(s) > 1$.

https://doi.org/10.4153/CMB-2018-002-4 Published online by Cambridge University Press

It is tempting to treat $\mathcal{G}_p(s)$ as a multi-Dirichlet L-function. However, χ_p is not a Dirichlet character. It is, however, related to a cubic Dirichlet character on $K = \mathbb{Q}(\zeta_3)$ modulo $\mathfrak{P}$. The following proposition shows exactly how $\mathcal{G}_p(s)$ is related to L-functions over K.

Proposition 4.1 *Let $\mathfrak{P}$ be the prime in K dividing p fixed in Remark 2.8 and let $\chi_{\mathfrak{P}} = \left(\frac{\cdot}{\mathfrak{P}}\right)_3$ be the cubic residue symbol modulo $\mathfrak{P}$ on K. Then*

$$\mathcal{G}_p(s) = \sqrt{L_K(\chi_{\mathfrak{P}}, s) L_K(\chi_{\mathfrak{P}}^2, s) H_p(s)}, \tag{4.2}$$

where $H_p(s)$ is some function (defined in the proof) that absolutely converges for $\Re(s) > 1/2$.

Proof We can write an Euler product expansion for $\mathcal{G}_p(s)$ as follows:

$$\mathcal{G}_p(s) = \prod_{\ell \equiv 1 \mod 3} \left(1 + \frac{\chi_p(\ell) + \chi_p^2(\ell)}{\ell^s}\right).$$

If $\mathfrak{l}$ is the fixed prime dividing ℓ in K, then we get $\chi_p(\ell) = \chi_{\mathfrak{P}}(\mathfrak{l})$. Moreover, we see that

$$\chi_p(\ell) + \chi_p^2(\ell) = \chi_{\mathfrak{P}}(\mathfrak{l}) + \chi_{\mathfrak{P}}^2(\mathfrak{l}) = \chi_{\mathfrak{P}}^2(\mathfrak{l}^\sigma) + \chi_{\mathfrak{P}}(\mathfrak{l}^\sigma),$$

where σ is the generator of $\mathrm{Gal}(K/Q)$. That is, the argument in the Euler product is independent of the choice of prime dividing ℓ.

Further, if $\ell \equiv 1 \mod 3$, then there always exist two primes lying above it with $N\mathfrak{l} = \ell$. Thus,

$$\prod_{\ell \equiv 1 \mod 3} \left(1 + \frac{\chi_p(\ell) + \chi_p^2(\ell)}{\ell^s}\right) = \prod_{\substack{\mathfrak{l} \mid \ell \\ \ell \equiv 1 \mod 3}} \left(1 + \frac{\chi_{\mathfrak{P}}(\mathfrak{l}) + \chi_{\mathfrak{P}}^2(\mathfrak{l})}{N\mathfrak{l}^s}\right)^{1/2}.$$

Finally, if $\ell \equiv 2 \mod 3$, then there exists a unique $\mathfrak{l} | \ell$ and $N\mathfrak{l} = \ell^2$. Therefore,

$$\begin{aligned}
&\prod_{\substack{\mathfrak{l} \mid \ell \\ \ell \equiv 1 \mod 3}} \left(1 + \frac{\chi_{\mathfrak{P}}(\mathfrak{l}) + \chi_{\mathfrak{P}}^2(\mathfrak{l})}{N\mathfrak{l}^s}\right) \\
&\quad = \prod_{\mathfrak{l} \neq \mathfrak{P}_3} \left(1 + \frac{\chi_{\mathfrak{P}}(\mathfrak{l}) + \chi_{\mathfrak{P}}^2(\mathfrak{l})}{N\mathfrak{l}^s}\right) \prod_{\ell \equiv 2 \mod 3} \left(1 + \frac{\chi_{\mathfrak{P}}(\mathfrak{l}) + \chi_{\mathfrak{P}}^2(\mathfrak{l})}{\ell^{2s}}\right)^{-1} \\
&\quad = \prod_{\mathfrak{l}} \left(1 - \frac{\chi_{\mathfrak{P}}(\mathfrak{l})}{N\mathfrak{l}^s}\right)^{-1} \prod_{\mathfrak{l}} \left(1 - \frac{\chi_{\mathfrak{P}}^2(\mathfrak{l})}{N\mathfrak{l}^s}\right)^{-1} H_p(s) \\
&\quad = L_K(\chi_{\mathfrak{P}}, s) L_K(\chi_{\mathfrak{P}}^2, s) H_p(s),
\end{aligned}$$

where $H_p(s)$ is some Euler product that converges for $\Re(s) > 1/2$. ∎

Corollary 4.2

$$\sum_{d_1 d_2 \leq Y}{}' \chi_p(d_1 d_2^2) = \int_{1-i\infty}^{1+i\infty} \mathcal{G}_p(s) \frac{Y^s}{s} ds.$$

Proof We know that $L_K(\chi_{\mathfrak{P}}, s)$ and $L_K(\chi_{\mathfrak{P}}^2, s)$ are entire and zero free on $\Re(s) = 1$. And since $H_p(s)$ can be written as an Euler product that converges for $\Re(s) > 1/2$, it will also be analytic and zero free on $\Re(s) = 1$. Hence, $\mathcal{G}_p(s)$ will be analytic on $\Re(s) = 1$. The result then follows from Perron's formula. ∎

The goal now is to analytically continue $\mathcal{G}_p(s)$ to a region to the left of $\Re(s) = 1$ and move this contour integral as far as we can. Since we do not know anything about the convergence of $H_p(s)$ to the left of $\Re(s) = 1/2$, the furthest we can hope to move the contour is to the line $\Re(s) = 1/2 + \epsilon$. Moreover, if $L_K(\chi_{\mathfrak{P}}, s)$ has a zero, then the right-hand side of (4.2) fails to be analytic at this zero.

Our plan moving forward is to move the contour for as many primes as we can and use Theorem 3.2 to bound the number of bad primes for which we cannot move the contour. Of course GRH implies that we can move all the contours to the line $\Re(s) = 1/2 + \epsilon$, but we will refrain from using that for now.

4.4 Bounding the Error Term

Proposition 4.3 *Suppose* $\operatorname{supp}(\widehat{f}) \subset (-\beta, \beta)$. *Then for any* T *and* $13/14 < \alpha < 1$, *we have*

$$\frac{1}{\sqrt{X}\log X}\sum_p \frac{\log p}{\sqrt{p^m}}\widehat{f}\Big(\frac{\log p^m}{\log X}\Big)\sideset{}{'}\sum_{d_1 d_2 \le Y}\chi_p(d_1 d_2^2) \ll \frac{X^{(\beta-1)/2+\epsilon}}{\log X}\Big(\frac{Y}{T} + Y^{\alpha+\epsilon}\Big) + \frac{Y(X^{2\beta}T)^{\frac{4(1-\alpha)}{3-2\alpha}}(\log XT)^A}{X^{(\beta+1)/2}}.$$

Proof First of all, if $\operatorname{supp}(\widehat{f}) \subset (-\beta, \beta)$, then this will restrict the sum over the primes to the region $X^{\beta/m}$. Combining this with Corollary 4.2, we get

$$\frac{1}{\sqrt{X}\log X}\sum_p \frac{\log p}{\sqrt{p^m}}\widehat{f}\Big(\frac{\log p^m}{\log X}\Big)\sideset{}{'}\sum_{d_1 d_2 \le Y}\chi_p(d_1 d_2^2) = \frac{1}{\sqrt{X}\log X}\sum_{p\le X^{\beta/m}} \frac{\log p}{\sqrt{p^m}}\widehat{f}\Big(\frac{\log p^m}{\log X}\Big)\int_{1-i\infty}^{1+i\infty}\mathcal{G}_p(s)\frac{Y^s}{s}\,ds.$$

We can write

$$\int_{1-i\infty}^{1+i\infty}\mathcal{G}_p(s)\frac{Y^s}{s}\,ds = \int_{1-iT}^{1+iT}\mathcal{G}_p(s)\frac{Y^s}{s}\,ds + \int_{\substack{\Re(s)=1\\ |\Im(s)|>T}}\mathcal{G}_p(s)\frac{Y^s}{s}\,ds.$$

Let S_1 be the sum consisting of the former and S_2 the latter. Then

$$\begin{aligned} S_2 &= \frac{1}{\sqrt{X}\log X}\sum_{p\le X^{\beta/m}}\frac{\log p}{\sqrt{p^m}}\widehat{f}\Big(\frac{\log p^m}{\log X}\Big)\int_{\substack{\Re(s)=1\\ |\Im(s)|>T}}\mathcal{G}_p(s)\frac{Y^s}{s} \\ &\ll \frac{Y}{T\sqrt{X}\log X}\sum_{p\le X^{\beta/m}}\frac{\log p}{\sqrt{p^m}} \\ &\ll \frac{Y}{T\sqrt{X}\log X}\begin{cases} X^{\beta/2+\epsilon} & m=1,\\ \log X^{\beta/2} & m=2,\end{cases} \ll \frac{YX^{(\beta-1)/2+\epsilon}}{T\log X}. \end{aligned}$$

Define

$\mathcal{E}_\alpha(Q,T) = \left\{ p \le Q : L_K(\chi_{\mathfrak{P}}, s) \text{ has a zero in the region } \alpha < \Re(s) < 1, |\Im(s)| < T \right\}.$

Then we will write $S_1 = S_3 + S_4$, where S_3 consists of the sum of primes not in $\mathcal{E}_\alpha(Q,T)$ and S_4 consists of the sum of primes in $\mathcal{E}_\alpha(Q,T)$.

By definition, $\mathcal{G}_p(s)$ is analytic in the region $\alpha < \Re(s) < 1, |\Im(s)| < T$ for $p \notin \mathcal{E}_\alpha(X^\beta, T)$, so we can shift the contour for these primes. That is,

$$\begin{aligned}
S_3 &= \frac{1}{\sqrt{X}\log X} \sum_{\substack{p \le X^{\beta/m} \\ p \notin \mathcal{E}_\alpha(X^\beta, T)}} \frac{\log p}{\sqrt{p^m}} \widehat{f}\Big(\frac{\log p^m}{\log X}\Big) \int_{1-iT}^{1+iT} \mathcal{G}_p(s) \frac{Y^s}{s} ds \\
&= \frac{1}{\sqrt{X}\log X} \sum_{\substack{p \le X^{\beta/m} \\ p \notin \mathcal{E}_\alpha(X^\beta, T)}} \frac{\log p}{\sqrt{p^m}} \widehat{f}\Big(\frac{\log p^m}{\log X}\Big) \\
&\quad \times \Big(\int_{\alpha+\epsilon-iT}^{\alpha+\epsilon+iT} \mathcal{G}_p(s) \frac{Y^s}{s} ds + \int_{\substack{\alpha+\epsilon \le \Re(s) \le 1 \\ |\Im(s)| = T}} \mathcal{G}_p(s) \frac{Y^s}{s} ds \Big) \\
&\ll \frac{1}{\sqrt{X}\log X} \sum_{\substack{p \le X^{\beta/m} \\ p \notin \mathcal{E}_\alpha(X^\beta, T)}} \frac{\log p}{\sqrt{p^m}} \Big(Y^{\alpha+\epsilon} + \frac{Y}{T} \Big) \\
&\ll \frac{1}{\sqrt{X}\log X} \Big(Y^{\alpha+\epsilon} + \frac{Y}{T} \Big) \begin{cases} X^{\beta/2+\epsilon} & m = 1 \\ \log X^{\beta/2} & m = 2 \end{cases} \ll \frac{X^{(\beta-1)/2+\epsilon}}{\log X} \Big(Y^{\alpha+\epsilon} + \frac{Y}{T} \Big).
\end{aligned}$$

Finally, recall that $N(\alpha, T, \chi)$ is the number of zeros of $L_K(\chi, s)$ in the region $\alpha < \Re(s) < 1, |\Im(s)| < T$. Therefore, by Theorem 3.2, we get for some $A > 0$

$$|\mathcal{E}_\alpha(Q,T)| \le \sum_{q \le Q} \sum_{\chi \bmod q}^{*} N(\alpha, T, \chi) \ll (Q^2 T)^{\frac{4(1-\alpha)}{3-2\alpha}} (\log QT)^A.$$

Therefore,

$$\begin{aligned}
S_4 &= \frac{1}{\sqrt{X}\log X} \sum_{\substack{p \le X^{\beta/m} \\ p \in \mathcal{E}_\alpha(X^{\beta/m}, T)}} \frac{\log p}{\sqrt{p^m}} \widehat{f}\Big(\frac{\log p^m}{\log X}\Big) \int_{1-iT}^{1+iT} \mathcal{G}_p(s) \frac{Y^s}{s} ds \\
&\ll \frac{Y}{\sqrt{X}} \sum_{\substack{p \le X^{\beta/m} \\ p \in \mathcal{E}_\alpha(X^{\beta/m}, T)}} \frac{1}{\sqrt{p^m}}.
\end{aligned}$$

For $m = 2$, we can bound the remaining sum by $\log X$ and get that $S_4 \ll \frac{Y}{\sqrt{X}} \log X$ which suffices. In order to manage when $m = 1$, we will split it up into dyadic intervals. Therefore,

$$\begin{aligned}
\sum_{\substack{X^\beta/2^j < p \le X^\beta/2^{j-1} \\ p \in \mathcal{E}_\alpha(X^\beta, T)}} \frac{1}{\sqrt{p}} &= \sum_{\substack{X^\beta/2^j < p \le X^\beta/2^{j-1} \\ p \in \mathcal{E}_\alpha(X^\beta/2^{j-1}, T)}} \frac{1}{\sqrt{p}} \ll |\mathcal{E}_\alpha(X^\beta/2^{j-1}, T)| \frac{2^{j/2}}{X^{\beta/2}} \\
&\ll \frac{(X^{2\beta} T)^{\frac{4(1-\alpha)}{3-2\alpha}} (\log XT)^A}{X^{\beta/2}} 2^{j/2(1 - \frac{16(1-\alpha)}{3-2\alpha})}.
\end{aligned}$$

https://doi.org/10.4153/CMB-2018-002-4 Published online by Cambridge University Press

And so,

$$S_4 \ll \frac{Y(X^{2\beta}T)^{\frac{4(1-\alpha)}{3-2\alpha}}(\log XT)^A}{X^{(\beta+1)/2}} \sum_{j=1}^{\beta \log_2 X} 2^{j/2(1-\frac{16(1-\alpha)}{3-2\alpha})}$$

$$\ll \frac{Y(X^{2\beta}T)^{\frac{4(1-\alpha)}{3-2\alpha}}(\log XT)^A}{X^{(\beta+1)/2}}.$$

This last line is true because the sum converges, since $\alpha > 13/14$ (and hence the exponent appearing is negative). ■

Corollary 4.4 *Assuming GRH, we have*

$$\frac{1}{\sqrt{X}\log X}\sum_p \frac{\log p}{\sqrt{p^m}}\widehat{f}\Big(\frac{\log p^m}{\log X}\Big)\sum_{d_1 d_2 \le Y}{}' \chi_p(d_1 d_2^2) \ll \frac{Y^{1/2+\epsilon}X^{(\beta-1)/2+\epsilon}}{\log X}.$$

Proof In the notation of the proof of Proposition 4.3, GRH implies that $\mathscr{E}_{1/2}(Q,T) = \varnothing$ for all choices of Q and T. Therefore, $S_4 = 0$, and we can take $T \to \infty$ to get that $S_2 = 0$ and

$$S_3 \ll \frac{Y^{1/2+\epsilon}X^{(\beta-1)/2+\epsilon}}{\log X}.$$ ■

4.5 Proof of Theorem 1.7

Now, we can finally prove Theorem 1.7.

Proof of Theorem 1.7 By Propositions 4.3 and 3.3, we see that if $\operatorname{supp}(\widehat{f}) \subset (-\beta,\beta)$, then

$$\frac{1}{|\mathcal{F}_3(X)|}\sum_{K_D \in \mathcal{F}_3(X)} \mathscr{D}(K_D, f) = \int_{-\infty}^{\infty} f(t)W(U)(t)dt - ET,$$

where for any $T > 0$ and $13/14 < \alpha < 1$,

$$ET \ll \frac{X^{(\beta-1)/2+\epsilon}}{\log X}\Big(\frac{X^{1/2}}{T} + X^{\alpha/2+\epsilon}\Big) + \frac{X^{1/2}(X^{2\beta}T)^{\frac{4(1-\alpha)}{3-2\alpha}}(\log XT)^A}{X^{(\beta+1)/2}} + \frac{1}{\log X}.$$

Setting $T = X^\beta$, we get

$$ET \ll \frac{1}{X^{\beta/2-\epsilon}\log X} + \frac{X^{(\alpha+\beta-1)/2+\epsilon}}{\log X} + X^{\beta(\frac{12(1-\alpha)}{3-2\alpha}-\frac{1}{2})}(\log X)^A + \frac{1}{\log X}.$$

Since $\alpha > 13/14$, we get that $\frac{12(1-\alpha)}{3-2\alpha} - \frac{1}{2} < 0$, and so the only restriction on β comes from the second term. That is as long as $\beta < 1-\alpha < 1/14$ we have

$$ET \ll \frac{1}{\log X}.$$

If we assume GRH, then by Corollary 4.4 we get

$$ET \ll \frac{X^{(\beta-1/2)/2+\epsilon}}{\log X} + \frac{1}{\log X},$$

and as long as $\beta < 1/2$, we get $ET \ll \frac{1}{\log X}$. ■

https://doi.org/10.4153/CMB-2018-002-4 Published online by Cambridge University Press

Acknowledgments I would like to thank Zeév Rudnick for useful discussions.

References

[1] A. Bucur, E. Costa, C. David, J. Guerreiro, and D. Lowry-Duda, *Traces, high powers and one level density for families of curves over finite fields*. Math. Proc. Cambridge Philos. Soc. 2017. http://dx.doi.org/10.1017/S030500411700041X

[2] J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*. London Mathematical Society, London, 1967.

[3] L. Häberle, *On cubic Galois field extensions*. J. Number Theory **130**(2010), no. 2, 307–317. http://dx.doi.org/10.1016/j.jnt.2009.09.001

[4] N. Katz and P. Sarnak, *Zeroes of zeta functions and symmetry*. Bull. Amer. Math. Soc.**36**(1999), no. 1, 1–26. http://dx.doi.org/10.1090/S0273-0979-99-00766-1

[5] ———, *Random matrices, Frobenius eigenvalues, and monodromy*. American Mathematical Society Colloquium Plublications, 45, American Mathematical Society, Providence, RI, 1999.

[6] F. B. Koval'chik, *Density theorems for sectors and progressions*. Lithuanian Math. J. **15**(1975), no. 4, 618–631.

[7] Z. Rudnick, *Traces of high powers of the Frobenius class in the hyperelliptic ensemble*. Acta Arith. **143**(2010), no. 1, 81–99. http://dx.doi.org/10.4064/aa143-1-5

[8] Z. Rudnick and P. Sarnak, *Zeros of principal l-functions and random matrix theory*. Duke Math. J. **81**(1996), no. 2, 269–322. http://dx.doi.org/10.1215/S0012-7094-96-08115-6

[9] A. Weil, *Sur les courbes algébriques et les variétés qui s' en déduisent*. Actualités Sci. Ind., 1041, Hermann, Paris, 1948.

[10] D. J. Wright, *Distribution of discriminants of abelian extensions*. Proc. London Math. Soc. 3(1989), no. 1, 17–50. http://dx.doi.org/10.1112/plms/s3-58.1.17

[11] A. Yang, *Distribution problems associated to zeta functions and invariant theory*. Ph.D. Thesis, Princeton University, 2009.

Tel Aviv University, 6997801 Tel Aviv, Israel
e-mail: meisner@mail.tau.ac.il