

# The Sato–Tate Distribution and the Values of Fourier Coefficients of Modular Newforms

Josep González and Jorge Jiménez-Urroz

## CONTENTS

1. Introduction
2. Arithmetic Distribution
3. Applications
4. Arithmetic Independence
5. The Values of Coefficients of Modular Newforms

Acknowledgments

References

---

The Sato–Tate conjecture has been recently settled in great generality. One natural question now concerns the rate of convergence of the distribution of the Fourier coefficients of modular newforms to the Sato–Tate distribution. In this paper, we address this issue, imposing congruence conditions on the primes and on the Fourier coefficients as well. Assuming a proper error term in the convergence to a conjectural limiting distribution, supported by experimental data, we prove the Lang–Trotter conjecture, and in the direction of Lehmer’s conjecture, we prove that  $\tau(p) = 0$  has at most finitely many solutions. In fact, we propose a conjecture, much more general than Lehmer’s, about the vanishing of Fourier coefficients of any modular newform.

---

## 1. INTRODUCTION

Let  $E/\mathbb{Q}$  be an elliptic curve of conductor  $N$ , and for any given prime  $p \nmid N$ , let  $a_p$  be the trace of the Frobenius endomorphism acting on the Tate module of its reduction modulo  $p$ . It is well known that

$$\frac{|a_p|}{2\sqrt{p}} < 1.$$

Independently around 1960, Sato and Tate conjectured that for elliptic curves without complex multiplication (CM), these values are equidistributed by the semicircle distribution function given by

$$G(x) = \int_{-1}^x g(u) du \quad \text{for } x \in [-1, 1],$$

where  $g(u) = 2\sqrt{1-u^2}/\pi$ . This probability is called the Sato–Tate measure.

We have known since the Shimura–Taniyama–Weil conjecture was proved that there exist a normalized newform  $f = \sum_{n>0} b_n q^n \in S_2(\Gamma_1(N))$  with trivial nebentypus and a nonconstant morphism  $\pi : X_1(N) \rightarrow E$  defined over  $\mathbb{Q}$  such that  $\pi^*(\Omega_{E/\mathbb{Q}}^1) = f(q) dq/q \mathbb{Q}$ , and moreover,  $a_p = b_p$  for all  $p \nmid N$ . In fact, it was also expected that the Sato–Tate measure would govern similarly the distribution of the Fourier coefficients of other, more general, normalized modular newforms, i.e., newforms

2000 AMS Subject Classification: 11F30

Keywords: Sato–Tate distribution, Lang–Trotter conjecture, Lehmer’s conjecture

whose Fourier expansions  $f = \sum_{n>0} b_n q^n \in S_2(\Gamma_1(N))$  satisfy  $b_1 = 1$ . Recently, the following result was proved [Barnet-Lamb et al. 11, Theorem B].

**Theorem 1.1. (Barnet-Lamb, Geraghty, Harris, and Taylor.)** *Let  $k$  and  $N$  be integers such that  $k \geq 2$  and  $N \geq 1$ . Let  $f = \sum_{n>0} a_n q^n$  be a normalized newform of level  $N$  and weight  $k$  with nebentypus  $\varepsilon$  and without CM. Let  $\zeta$  be a root of unity such that  $\zeta^2 \in \text{Im}(\varepsilon)$ . Then for all  $a \in [-1, 1]$  we have*

$$\begin{aligned} \lim_{x \rightarrow +\infty} \frac{\#\left\{p \in \mathcal{P}(x) : \varepsilon(p) = \zeta^2, \frac{a_p}{2\zeta p^{(k-1)/2}} \leq a\right\}}{\#\{p \in \mathcal{P}(x) : \varepsilon(p) = \zeta^2\}} \\ = \frac{2}{\pi} \int_{-1}^a \sqrt{1-x^2} \, dx, \end{aligned}$$

where  $\mathcal{P}(x)$  denotes the set of primes  $p \nmid N$  up to  $x$ .

Based on computational evidence, we present two conjectures generalizing the previous result. The first of them, Conjecture 2.2, basically claims that the Sato–Tate distribution holds when we restrict to primes whose traces of Frobenius lie in an arithmetic progression containing infinitely many such traces. The second, Conjecture 4.3, states the stochastic independence of Sato–Tate distributions of several normalized newforms without CM when they are pairwise algebraically independent (for this notion see Definition 4.1). Although Conjecture 4.3 generalizes Conjecture 2.2, in order to get a better understanding of the arguments involved in the exposition, we have chosen to present them separately in Sections 2 and 4.

Another problem of great interest in this context is the study of the values that can be taken by the Fourier coefficients of modular newforms. This problem appeared from two different directions, first, from the study of the nonvanishing of the Fourier coefficients, beginning with Lehmer’s famous conjecture on the Ramanujan tau function, and then continuing in a wide variety of articles, initiated by Serre in his well-known article [Serre 81] (see also [Balog and Ono 01]); and second, with the intensively studied memoir [Lang and Trotter 76] about the values of the traces of Frobenius elements of elliptic curves defined over  $\mathbb{Q}$ .

In this article we also present a conjecture that relates both topics, the distribution and the particular values of the Fourier coefficients of modular newforms. More precisely, in Section 3, we show that a rate of convergence for Conjecture 2.2 as stated in Conjecture 3.2 would allow us to prove the Lang–Trotter conjecture for elliptic curves over  $\mathbb{Q}$  and to obtain the finiteness of the set of

vanishing Fourier coefficients of any modular newform of weight at least four with rational coefficients, and hence give a proper wide generalization of Lehmer’s conjecture. Finally, in Section 5, we extend this last result to newforms whose Fourier coefficients are in any number field.

Even though the results presented are conditional, the authors believe that the approach introduced in this paper could provide a new way to attack the problem of determining the vanishing of Fourier coefficients of modular newforms without CM.

## 2. ARITHMETIC DISTRIBUTION

Using results of [Barnet-Lamb et al. 11], Theorem 1.1 was extended in [González et al. 10] by restricting primes to certain classes of congruences. (In fact, in [González et al. 10], only the case  $k = 2$  was proved, but the general case  $k \geq 2$  follows by similar reasoning.)

**Theorem 2.1.** *Keep the assumptions as in Theorem 1.1. For any multiple  $M$  of the conductor of  $\varepsilon$  and for a root of unity  $\zeta$  such that  $\zeta^2 = \varepsilon(m)$  for some integer  $m$ , one has*

$$\begin{aligned} \lim_{x \rightarrow +\infty} \frac{\#\left\{p \in \mathcal{P}(x) : p \equiv m \pmod{M}, \frac{a_p}{2\zeta p^{(k-1)/2}} \leq a\right\}}{\#\{p \in \mathcal{P}(x) : p \equiv m \pmod{M}\}} \\ = \frac{2}{\pi} \int_{-1}^a \sqrt{1-x^2} \, dx, \end{aligned}$$

for all  $a \in [-1, 1]$ .

It is well known that for a normalized newform  $f = \sum_{n>0} a_n q^n \in S_k(\Gamma_1(N))^{\text{new}}$ , the field  $K = \mathbb{Q}(\{a_n\})$  is a number field, and the Fourier coefficients  $a_n$  are in  $\mathcal{O}_K$ , where  $\mathcal{O}_K$  denotes the ring of integers of  $K$ . Also, for every prime  $\lambda$  in  $K$  over a rational prime  $\ell$ , there is a continuous  $\lambda$ -adic representation

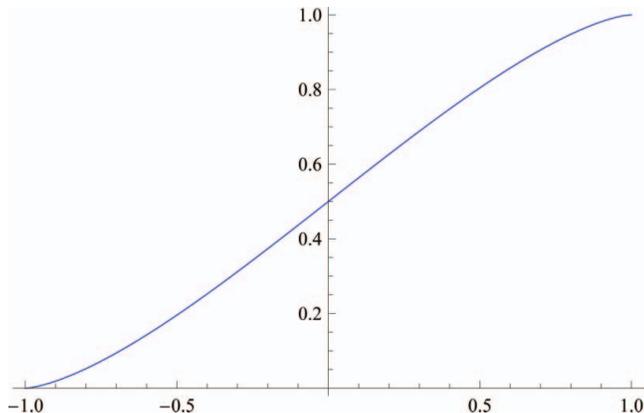
$$\rho_\lambda : G_{\mathbb{Q}} := \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}(2, \mathcal{O}_\lambda),$$

where  $\mathcal{O}_\lambda$  denotes the completion of  $\mathcal{O}_K$  by  $\lambda$ , unramified at every  $p \nmid N\ell$ , and such that  $\text{tr}(\rho_\lambda(\text{Frob}_p)) = a_p$  and  $\det(\rho_\lambda(\text{Frob}_p)) = \varepsilon(p)p^{k-1}$ . For any integer  $i \geq 1$ , we denote by  $r_{\lambda^i}$  the representation obtained by reducing modulo  $\lambda^i$ , i.e.,

$$r_{\lambda^i} : G_{\mathbb{Q}} \longrightarrow \text{GL}(2, \mathcal{O}_K/\lambda^i).$$

Let  $\mathfrak{m}$  be an ideal of  $\mathcal{O}_K$  and  $t \in \mathcal{O}_K$ . As a consequence of the existence of  $r_{\lambda^i}$ , there exists a representation

$$r_{\mathfrak{m}} : G_{\mathbb{Q}} \longrightarrow \text{GL}(2, \mathcal{O}_K/\mathfrak{m})$$



**FIGURE 1.** The graph of the Sato–Tate distribution function (color figure available online).

unramified at every prime  $p \nmid N \text{Norm}(\mathfrak{m})$  such that  $\text{tr}(r_{\mathfrak{m}}(\text{Frob}_p)) \equiv a_p \pmod{\mathfrak{m}}$ . By the Čebotarev density theorem, we know that the following limit exists:

$$f_{\mathfrak{m}}(t) := \lim_{x \rightarrow +\infty} \frac{\#\{p \in \mathcal{P}(x) : a_p \equiv t \pmod{\mathfrak{m}}\}}{\#\mathcal{P}(x)}.$$

After several computations, the authors think that the following conjecture is true.

**Conjecture 2.2.** *Keep the assumptions as in Theorem 1.1 and suppose  $f_{\mathfrak{m}}(t) \neq 0$ . For any multiple  $M$  of the conductor of  $\varepsilon$  and for a root of unity  $\zeta$  such that  $\zeta^2 = \varepsilon(m)$  for some integer  $m$ , one has*

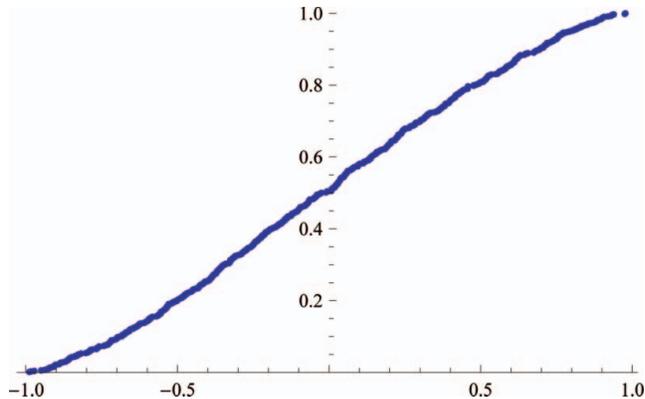
$$\begin{aligned} &\lim_{x \rightarrow +\infty} \#\left\{p \in \mathcal{P}(x) : p \equiv m \pmod{M}, a_p \equiv t \pmod{\mathfrak{m}}, \right. \\ &\quad \left. \frac{a_p}{2\zeta p^{(k-1)/2}} \leq a \right\} / \\ &\quad \#\{p \in \mathcal{P}(x) : p \equiv m \pmod{M}, a_p \equiv t \pmod{\mathfrak{m}}\} \\ &= \frac{2}{\pi} \int_{-1}^a \sqrt{1-x^2} dx \end{aligned}$$

for all  $a \in [-1, 1]$ .

The above conjecture states that the Sato–Tate distribution respects the arithmetic of  $\mathbb{Z}$  and  $\mathcal{O}_K$  if possible, i.e., when  $M$  is a multiple of the conductor of  $\varepsilon$  and  $f_{\mathfrak{m}}(t) \neq 0$ . Note that for  $\mathfrak{m} = \mathcal{O}_K$ , the above conjecture is Theorem 2.2. We present a few examples with trivial nebentypus and  $M = 1$  for this conjecture. The graph of the Sato–Tate distribution function

$$G(x) = \frac{1}{2} + \left( x\sqrt{1-x^2} + \frac{1}{\pi} \arcsin(x) \right)$$

is shown in Figure 1.



**FIGURE 2.** Graph of  $G(a, t, \mathfrak{m}; 30000)$  for  $f$  in Example 2.3 when  $(t, \mathfrak{m}) = (2, 3\mathbb{Z})$  (color figure available online).

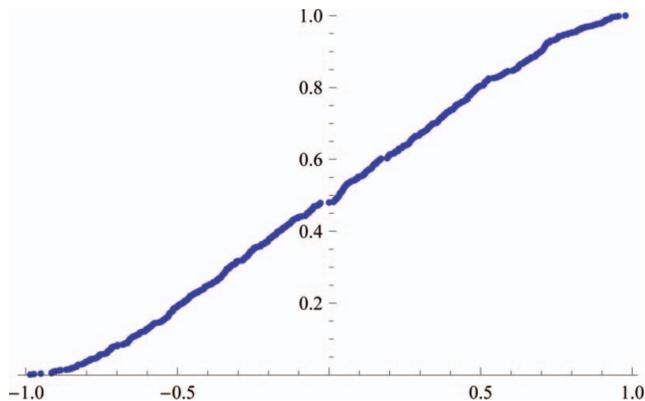
For a fixed newform  $f$  with real coefficients, set

$$G(a, t, \mathfrak{m}; x) := \frac{\#\left\{p \in \mathcal{P}(x) : a_p \equiv t \pmod{\mathfrak{m}}, \frac{a_p}{2p^{(k-1)/2}} \leq a \right\}}{\#\{p \in \mathcal{P}(x) : a_p \equiv t \pmod{\mathfrak{m}}\}}.$$

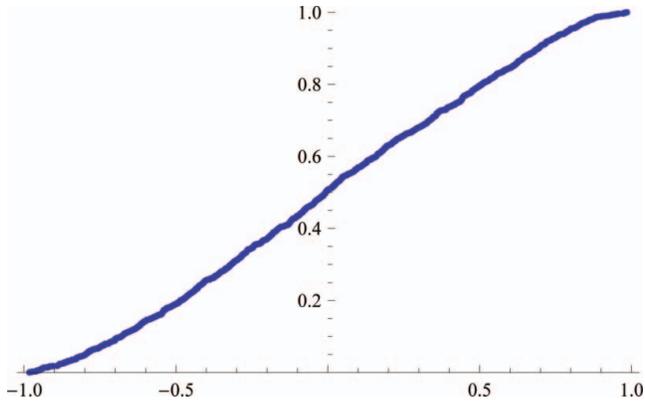
**Example 2.3. (Weight  $k = 2$ .)** Let  $f$  be the unique normalized newform in  $S_2(\Gamma_0(11))$ . We obtain the graphs shown in Figures 2 and 3 for  $G(a, t, \mathfrak{m}; 30000)$  when  $(t, \mathfrak{m}) = (2, 3\mathbb{Z})$  and  $(t, \mathfrak{m}) = (0, 4\mathbb{Z})$  respectively.

**Example 2.4. (Weight  $k > 2$ .)** Let  $f$  be the discriminant modular form

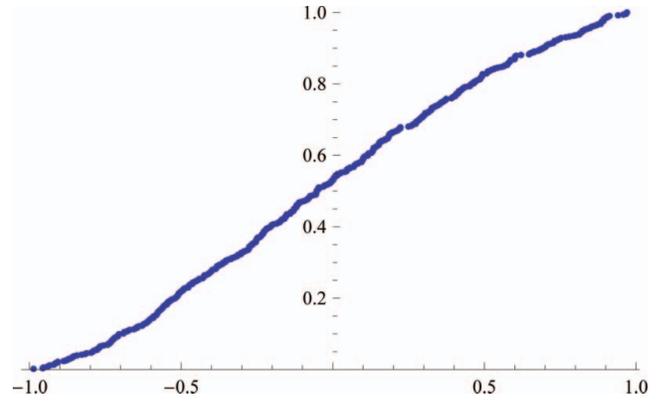
$$\Delta = q \prod_{n>0} (1 - q^n)^{24} \in S_{12}(\Gamma(1)),$$



**FIGURE 3.** Graph of  $G(a, t, \mathfrak{m}; 30000)$  for  $f$  in Example 2.3 when  $(t, \mathfrak{m}) = (0, 4\mathbb{Z})$  (color figure available online).



**FIGURE 4.** Graph of  $G(a, t, \mathfrak{m}; 30000)$  for  $f = \Delta$  when  $(t, \mathfrak{m}) = (2, 3\mathbb{Z})$  (color figure available online).



**FIGURE 6.** Graph of  $G(a, t, \mathfrak{m}; 55000)$  for  $f$  in Example 2.5 when  $(t, \mathfrak{m}) = (0, (4 + \sqrt{5})\mathcal{O}_K)$  (color figure available online).

$x = 30\,000$ , and  $(t, \mathfrak{m}) = (2, 3\mathbb{Z})$  respectively  $(t, \mathfrak{M}) = (0, 4\mathbb{Z})$  we obtain the graphs of Figures 4 and 5.

**Example 2.5. (Nonrational coefficients.)** Let  $f \in S_2(\Gamma_0(23))^{\text{new}}$  be the newform

$$f = q + \frac{-1 + \sqrt{5}}{2}q^2 + \dots$$

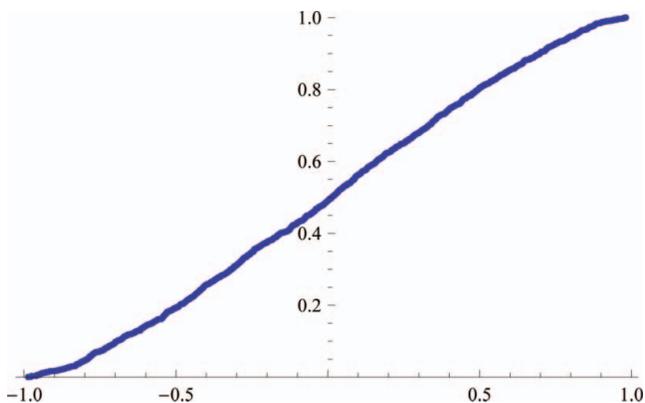
and  $x = 55000$ . For  $\mathfrak{m} = (4 + \sqrt{5})\mathcal{O}_K$  and  $t = 0, 2$  we obtain the graphs shown in Figures 6 and 7, and for  $\mathfrak{m} = 3, \mathcal{O}_K, t = 0, (-1 + \sqrt{5})/2$  we get the graphs of Figures 8 and 9.

The computations of Fourier coefficients were performed with MAGMA v2.15-13 using a personal computer with an Intel Core Duo processor running at 2.67 GHz with 4 GB of memory. The difficulty in obtaining a large number of Fourier coefficients of a normalized newform

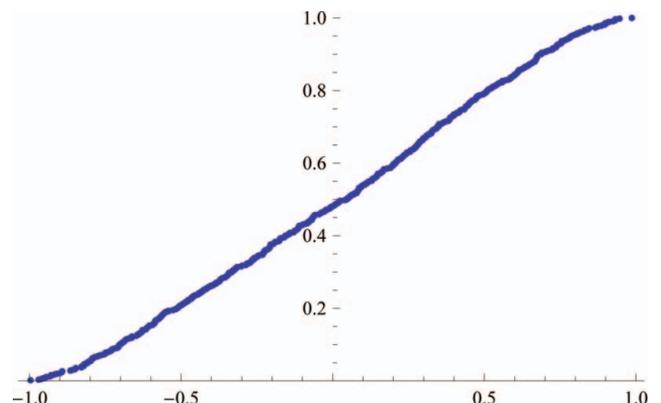
$f$  of level  $N$  and weight  $k$  is the limitation of the memory. The necessary memory depends on the modular symbol chosen by the MAGMA program to identify the newform  $f$  and the weight  $k$ , the degree of the number field  $K = \mathbb{Q}(\{a_n\})$ , and the genus of the modular curve, which tends to infinity as the level  $N$  approaches  $+\infty$ . For the lowest level  $N = 11$ , the lowest weight  $k = 2$ , and the lowest number field  $K = \mathbb{Q}$ , we were able to compute the first 300 000 Fourier coefficients in 16.6 hours, but we could not compute the first 400 000.

For a fixed newform  $f$  and  $x, m, M, t$ , and  $\mathfrak{m}$  as in Conjecture 2.2, let us denote by  $n$  the cardinality of the set

$$\mathcal{V} := \{p \in \mathcal{P}(x) : p \equiv m \pmod{M}, a_p \equiv t \pmod{\mathfrak{m}}\}.$$



**FIGURE 5.** Graph of  $G(a, t, \mathfrak{m}; 30000)$  for  $f = \Delta$  when  $(t, \mathfrak{m}) = (0, 4\mathbb{Z})$  (color figure available online).



**FIGURE 7.** Graph of  $G(a, t, \mathfrak{m}; 55000)$  for  $f$  in Example 2.5 when  $(t, \mathfrak{m}) = (2, (4 + \sqrt{5})\mathcal{O}_K)$  (color figure available online).

$t$	$\mathfrak{m}$	$m$	$M$	$n$	$D$	$t$	$\mathfrak{m}$	$m$	$M$	$n$	$D$
1	$\mathbb{Z}$	1	1	9591	0.005	0	$3\mathbb{Z}$	1	3	3229	0.014
1	$\mathbb{Z}$	1	1	25996	0.005	1	$3\mathbb{Z}$	1	3	4883	0.011
0	$2\mathbb{Z}$	1	3	8652	0.006	2	$3\mathbb{Z}$	1	3	4858	0.009
0	$2\mathbb{Z}$	2	3	8691	0.006	0	$3\mathbb{Z}$	2	3	6652	0.008
0	$2\mathbb{Z}$	1	4	8651	0.007	1	$3\mathbb{Z}$	2	3	3196	0.016
0	$2\mathbb{Z}$	3	4	8691	0.008	2	$3\mathbb{Z}$	2	3	3277	0.009
0	$2\mathbb{Z}$	1	5	4316	0.010	0	$5\mathbb{Z}$	1	3	3227	0.013
0	$2\mathbb{Z}$	2	5	4371	0.007	2	$5\mathbb{Z}$	1	3	2224	0.011
0	$2\mathbb{Z}$	3	5	4331	0.011	3	$5\mathbb{Z}$	1	3	3252	0.011
0	$2\mathbb{Z}$	4	5	4325	0.009	4	$5\mathbb{Z}$	1	3	3261	0.009
1	$2\mathbb{Z}$	1	3	4317	0.011	0	$5\mathbb{Z}$	2	3	3260	0.019
1	$2\mathbb{Z}$	2	3	4334	0.010	2	$5\mathbb{Z}$	2	3	3247	0.012
1	$2\mathbb{Z}$	1	4	4328	0.011	3	$5\mathbb{Z}$	2	3	3268	0.006
1	$2\mathbb{Z}$	3	4	4324	0.009	4	$5\mathbb{Z}$	2	3	3249	0.009
1	$2\mathbb{Z}$	1	5	2161	0.013	0	$7\mathbb{Z}$	1	3	1880	0.023
1	$2\mathbb{Z}$	2	5	2149	0.017	0	$7\mathbb{Z}$	1	4	1875	0.015
1	$2\mathbb{Z}$	3	5	2179	0.018	0	$7\mathbb{Z}$	1	5	883	0.018
1	$2\mathbb{Z}$	4	5	2161	0.014	0	$7\mathbb{Z}$	1	7	551	0.021

TABLE 1. Statistic  $D$  for  $f$  in Example 2.3.

In general,  $n$  is expected to be nearly

$$\frac{x}{\log x} \frac{1}{\text{Norm}(\mathfrak{m})\varphi(M)},$$

where  $\varphi$  denotes the Euler totient function. We point out that it is hard to test the conjecture for ideals  $\mathfrak{m}$  with large norm or for large values of  $M$ , even with a more powerful computer, since a large value of  $x$  is needed.

To measure the significance level of any sample of data to the Sato–Tate distribution, we shall use the

Kolmogorov–Smirnov statistic  $D$ , which measures the largest vertical difference between the empirical distribution function and the theoretical distribution. Set

$$D = \max \left\{ \left| \frac{1}{n} \# \left\{ p \in \mathcal{V} : \frac{a_p}{2\zeta p^{(k-1)/2}} \leq a \right\} - \frac{2}{\pi} \int_{-1}^a \sqrt{1-x^2} dx \right| \right\},$$

$t$	$\mathfrak{m}$	$m$	$M$	$n$	$D$	$t$	$\mathfrak{m}$	$m$	$M$	$n$	$D$
1	$\mathcal{O}$	1	1	9591	0.005	$t_0$	$3\mathcal{O}$	1	3	1277	0.012
1	$\mathcal{O}$	1	1	17983	0.004	$t_0$	$3\mathcal{O}$	2	3	1291	0.021
0	$2\mathcal{O}$	1	3	8648	0.006	$1+t_0$	$3\mathcal{O}$	1	3	1316	0.033
0	$2\mathcal{O}$	2	3	8679	0.008	$1+t_0$	$3\mathcal{O}$	2	3	1305	0.046
1	$2\mathcal{O}$	1	3	4322	0.011	$2+t_0$	$3\mathcal{O}$	2	3	2297	0.018
1	$2\mathcal{O}$	2	3	4345	0.006	$2t_0$	$3\mathcal{O}$	1	3	1295	0.018
0	$3\mathcal{O}$	1	3	3254	0.010	0	$(5+2t_0)\mathcal{O}$	1	1	2594	0.017
0	$3\mathcal{O}$	2	3	3243	0.012	0	$(5+2t_0)\mathcal{O}$	1	3	1294	0.024
1	$3\mathcal{O}$	1	3	2280	0.020	0	$(5+2t_0)\mathcal{O}$	1	5	636	0.023
2	$3\mathcal{O}$	1	3	2260	0.015	0	$(5+2t_0)\mathcal{O}$	1	7	433	0.054

TABLE 2. Statistic  $D$  for  $f$  in Example 2.5.

$t$	$\mathfrak{m}$	$m$	$M$	$n$	$D$	$t$	$\mathfrak{m}$	$m$	$M$	$n$	$D$
1	$\mathcal{O}$	1	8	6457	0.007	3	$(2+i)\mathcal{O}$	3	8	1626	0.017
1	$\mathcal{O}$	3	8	6493	0.008	4	$(2+i)\mathcal{O}$	3	8	1620	0.016
1	$\mathcal{O}$	5	8	6523	0.006	0	$3\mathcal{O}$	5	8	2421	0.016
1	$\mathcal{O}$	7	8	6522	0.006	$i$	$3\mathcal{O}$	5	8	2040	0.018
0	$(2+i)\mathcal{O}$	1	8	1598	0.017	$2i$	$3\mathcal{O}$	5	8	2062	0.010
2	$(2+i)\mathcal{O}$	1	8	1614	0.018	0	$3\mathcal{O}$	7	8	2466	0.024
3	$(2+i)\mathcal{O}$	1	8	1623	0.022	1	$3\mathcal{O}$	7	8	2074	0.020
4	$(2+i)\mathcal{O}$	1	8	1622	0.017	2	$3\mathcal{O}$	7	8	1982	0.018
0	$(2+i)\mathcal{O}$	3	8	1612	0.028	0	$(3+2i)\mathcal{O}$	1	8	516	0.054
2	$(2+i)\mathcal{O}$	3	8	1635	0.016	12	$(3+2i)\mathcal{O}$	1	8	475	0.035

TABLE 3. Statistic  $D$  for the newform  $f=q - (1+i)q^2 + \dots \in S_2(\Gamma_1(24))$ .

where  $a$  runs over the set

$$\left\{ \frac{a_p}{2\zeta p^{(k-1)/2}} : p \in \mathcal{V} \right\}.$$

Since the Sato–Tate distribution is free-parameter-dependent, it is possible to evaluate the  $p$ -value associated with a specific value of  $D$  calculated from a sample of size  $n$ . A large  $p$ -value implies that we should not reject the null hypothesis that the sample comes from the Sato–Tate distribution.

In Tables 1–3, we present more examples for three different normalized newforms, with the values  $n$  and  $D$  for  $x = 3 \cdot 10^5$  and different congruence classes. In order to have an idea about the expected size of  $D$ , we see that for the normalized newform as in Example 2.3, we obtain  $D = 0.005$  for  $x = 10^5$ , and this value does not change when we consider  $x = 3 \cdot 10^5$ . These are the first two entries in Table 1, which correspond to cases proved in Theorem 1.1.

Table 1 gives values of  $D$  for  $x = 3 \cdot 10^5$  with different choices of  $t, m, \mathfrak{m}$ , and  $M$ , except the initial data, which are for  $x = 10^5$ , as already mentioned.

For the normalized newform of level 23 as in Example 2.5, we obtain  $D = 0.005$  with  $x = 10^5$ . Then if we choose  $x = 3 \cdot 10^5$ ,  $D$  goes down to  $D = 0.004$ . These are again the first two entries of Table 2, which correspond to the cases proved in Theorem 1.1. The rest of the table collects values of  $D$  again for different choices of  $t, m, \mathfrak{m}$ , and  $M$  and always with  $x = 3 \cdot 10^5$ . For convenience of notation we fix  $t_0 = (-1 + \sqrt{5})/2$  and put  $\mathcal{O} := \mathbb{Z}[t_0]$ .

Finally, we present in Table 3 values for the modular form  $f$  of weight 2 and level 24 with quadratic nebentypus  $\varepsilon$  of conductor 8 and  $q$ -expansion

$$f = q - (i + 1)q^2 + \dots$$

Now  $\mathcal{O}$  denotes  $\mathbb{Z}[i]$ . We recall that  $M$  must be a multiple of 8, and for primes  $p$  in congruence classes  $m \pmod{M}$

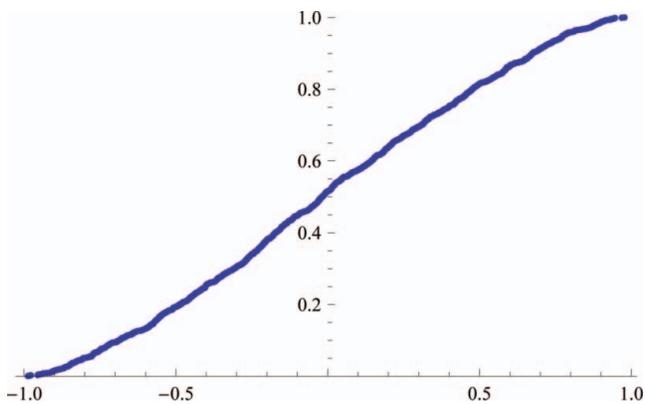


FIGURE 8. Graph of  $G(a, t, \mathfrak{m}; 55000)$  for  $f$  in Example 2.5 when  $(t, \mathfrak{m}) = (0, 3\mathcal{O}_K)$  (color figure available online).

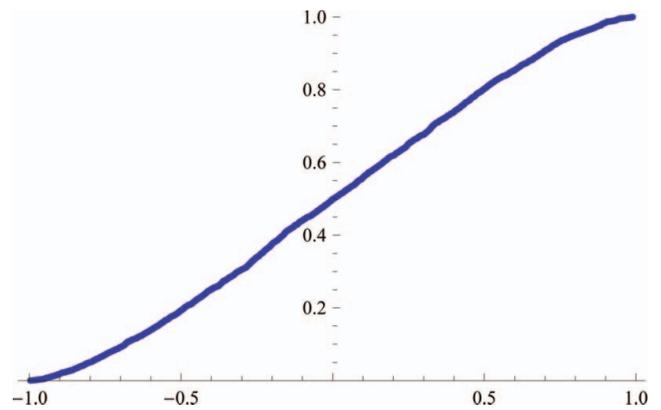


FIGURE 9. Graph of  $G(a, t, \mathfrak{m}; 55000)$  for  $f$  in Example 2.5 when  $(t, \mathfrak{m}) = ((-1 + \sqrt{5})/2, 3\mathcal{O}_K)$  (color figure available online).

such that  $\varepsilon(m) = -1$ , i.e.,  $m \equiv \pm 3 \pmod{8}$ , we are taking the sequence  $a_p / (2i\sqrt{p})$ , and  $x = 3 \cdot 10^5$  in all cases. Observe that the first four data in Table 3 correspond to cases proved in Theorem 2.1.

We used [D’Agostino and Stephens 86, Table 4.2] to obtain an approximation of the significance level of the statistic  $D$  for each of the 76 samples of Tables 1–3. All of these levels of significance are greater than 0.05 except the case  $(n, D) = (1305, 0.046)$  in Table 2. Therefore, the hypothesis that these samples come from the Sato–Tate distribution will not be rejected from a statistical point of view.

### 3. APPLICATIONS

In this section we focus our attention on the case  $\mathbb{Q}(\{a_n\}) = \mathbb{Q}$ . In this case, the weight  $k$  of the newform  $f$  must be even, and when  $M = 1$ , Conjecture 2.2 can be rewritten

$$\lim_{x \rightarrow +\infty} \frac{\#\left\{p \in \mathcal{P}(x) : a_p \equiv t \pmod{m}, \frac{a_p}{2p^{(k-1)/2}} \leq a\right\}}{\#\mathcal{P}(x)} = f_m(t) \int_{-1}^a g(u) du, \tag{3-1}$$

for all  $t \in \mathbb{Z}$ ,  $m \in \mathbb{Z}_{>0}$ , and  $a \in [-1, 1]$ . Here  $f_m$  denotes  $f_{\mathfrak{m}}$  for the ideal  $\mathfrak{m} = m\mathbb{Z}$ .

With the same notation as in the previous section, it is proved in [Ribet 85, Theorem 3.1] that

$$\rho_\ell(G_{\mathbb{Q}}) = \left\{ \sigma \in \text{GL}(2, \mathbb{Z}_\ell) : \det(\sigma) \in \mathbb{Z}_\ell^{*(k-1)} \right\}$$

for almost all primes  $\ell$ . In particular,  $\text{SL}(2, \mathbb{Z}_\ell) \subset \rho_\ell(G_{\mathbb{Q}})$  for almost all primes  $\ell$ . By the main lemma in [Serre 89, Chapter 4], the group  $(\prod_\ell \rho_\ell)(G_{\mathbb{Q}})$  is open in  $\prod_\ell \rho_\ell(G_{\mathbb{Q}})$ .

Now consider the set of positive integers ordered by the relation  $m \preceq m'$  if  $m \mid m'$ . Since  $(\prod_\ell \rho_\ell)(G_{\mathbb{Q}})$  is open in  $\prod_\ell \rho_\ell(G_{\mathbb{Q}})$  and  $r_\ell(G_{\mathbb{Q}}) = \text{GL}(2, \mathbb{Z}/\ell\mathbb{Z})$  for almost all primes  $\ell$ , with arguments used in [Lang and Trotter 76], we can see that the function  $F : \mathbb{Z}_{>0} \rightarrow \mathbb{R}$  with  $F(t) = \lim_{m \rightarrow +\infty} m f_m(t)$  is well defined, and moreover, there exists an integer  $m_0 > 0$  such that

$$F(t) = m_0 f_{m_0}(t) \prod_{\ell \nmid m_0} \ell f_\ell(t), \tag{3-2}$$

where for a prime  $\ell \nmid m_0$  we have

$$\ell f_\ell(t) = \begin{cases} \frac{\ell^2}{\ell^2 - 1} & \text{if } t \equiv 0 \pmod{\ell}, \\ \frac{\ell(\ell^2 - \ell - 1)}{(\ell - 1)(\ell^2 - 1)} & \text{otherwise.} \end{cases} \tag{3-3}$$

A natural question to ask is about the rate of convergence in (3–1). Concretely, we would like to have a bound for the error function

$$E(\Pi(x), t, m; I) = \frac{\#\{p \in \Pi(x) : a_p \equiv t \pmod{m}, \frac{a_p}{2p^{(k-1)/2}} \in I\}}{\#\Pi(x)} - f_m(t) \int_I g(u) du, \tag{3-4}$$

for a suitable set of primes  $\Pi(x)$  inside a suitably large interval, a fixed  $t$ , and where  $I$  is a subinterval of  $[-1, 1]$  containing 0.

For  $\Pi(x) = \mathcal{P}(x)$ , note that if  $p$  is a prime such that  $a_p \equiv t \pmod{m}$  and

$$\frac{a_p}{2p^{(k-1)/2}} \in I,$$

then for any  $x < p$  we have

$$E(\mathcal{P}(p), t, m; I) - E(\mathcal{P}(x), t, m; I) \gg \frac{1}{\#\mathcal{P}(x)}, \tag{3-5}$$

a natural lower bound for  $E(\mathcal{P}(x), t, m; I)$  that cannot be sharpened. In this case, and for  $m = 1$  and  $k = 2$ , Akiyama and Tanigawa, based on some computational data, made the following conjecture.

**Conjecture 3.1.** [Akiyama and Tanigawa 99] *For all subintervals  $I$  of  $[-1, 1]$ , one has*

$$E(\mathcal{P}(x), t, 1; I) = o\left(\frac{1}{x^{1/2-\varepsilon}}\right) \text{ as } x \rightarrow \infty.$$

For further information, see also [Mazur 08] and [Stein 07].

It appears natural to claim that the previous conjecture remains true for any fixed  $m > 1$  and  $k \geq 2$ . However, it would be unrealistic to expect it to be uniform either in  $m$  or in the diameter  $\delta(I)$  of  $I$ . Here, with applications in mind, we pursue the idea of making a sharper error term by simply abandoning uniformity in those parameters. In certain situations we need to deal with primes of the same order of magnitude, and hence we will also be considering the following sets of primes. We will define

$$\mathcal{P}_\nu(x) := \mathcal{P}((1 + \nu)x) \setminus \mathcal{P}(x) = \{x < p \leq (1 + \nu)x\}, \tag{3-6}$$

for any positive number  $\nu$ . In some cases,  $\nu$  will tend to 0 with  $x$  very slowly. Note that if, on the other hand,  $\nu$  is large enough, then  $\#\mathcal{P}_\nu(x) / \#\mathcal{P}(x) \sim \nu$  as  $x \rightarrow +\infty$ .

With this purpose in mind, we simply note that the main term in

$$\frac{\#\left\{p \in \Pi(x) : a_p \equiv t \pmod{m}, \frac{a_p}{2p^{(k-1)/2}} \in I\right\}}{\#\Pi(x)}$$

should match the main term in

$$f_m(t) \int_I g(u) du$$

as  $m \rightarrow \infty$  or  $\delta(I) \rightarrow 0$ .

Firstly, let us consider  $F_m(t) = mf_m(t)$ . Then by (3–2) and (3–3), we see that for  $m$  sufficiently large,  $F_m(t) > F(t)$  for  $t \neq 0$  and  $F_m(0) < F(0)$ . On the other hand, we take, without loss of generality,

$$m = m_0 \prod_{\substack{\ell \nmid m_0 \\ \ell < L}} \ell.$$

Then for  $L$  big enough,

$$F(t) - F_m(t) = F_m(t) \left( \prod_{\ell > L} F_\ell(t) - 1 \right).$$

Now since  $\log(1-x) = O(x)$  as  $x \rightarrow 0$ , taking logarithms, we see again from the definitions (3–2) and (3–3) that

$$\sum_{\ell > L} |\log F_\ell(t)| \ll \sum_{\ell > L} \frac{1}{\ell^2} = O\left(\frac{1}{L}\right),$$

and hence noting that  $|F_m(t)|$  is bounded, we get

$$f_m(t) = \frac{F(t)}{m} + O\left(\frac{1}{mL}\right).$$

Observe that for  $t \neq 0$ , one could replace  $1/L$  by  $1/L^2$ .

Secondly,  $g$  is a differentiable function, so there exist  $\xi, \hat{\xi} \in I$  such that

$$\begin{aligned} \int_I g(u) du &= \delta(I)g(\xi) = \delta(I)(g(0) + g'(\hat{\xi})\xi) \\ &= \delta(I)g(0) + O(\delta(I)^3), \end{aligned}$$

by the mean value theorem, as well as the bound  $g'(x) = O(x)$  as  $x \rightarrow 0$ . Combining both estimates, we get

$$\begin{aligned} f_m(t) \int_I g(u) du & \quad (3-7) \\ &= F(t)g(0)\frac{\delta(I)}{m} + O\left(\frac{\delta(I)}{mL}\right) + O\left(\frac{\delta(I)^3}{m}\right). \end{aligned}$$

Finally,

$$\begin{aligned} &\#\left\{p \in \Pi(x) : a_p \equiv t \pmod{m}, \frac{a_p}{2p^{(k-1)/2}} \in I\right\} \\ &= \#\left\{p \in \Pi(x) : \left(\frac{t}{2\delta(I)}\right)^{2/(k-1)} < p, \right. \\ &\quad \left. a_p \equiv t \pmod{m}, \frac{a_p}{2p^{(k-1)/2}} \in I\right\} \quad (3-8) \\ &+ O\left(\left(\frac{t}{2\delta(I)}\right)^{2/(k-1)}\right). \end{aligned}$$

Based on the previous analysis, the prime number theorem, Conjecture 2.2, and maintaining the square-root restriction of Conjecture 3.1, we make the following conjecture.

**Conjecture 3.2.** *Let  $x \geq 2$ . With notation as above, there exist constants  $C_1$  and  $C_2$  depending on  $t$  and the newform  $f$  such that as  $I$  runs through subintervals of  $[-1, 1]$  containing 0, we have*

$$E(\Pi(x), t, m; I) = O\left(\frac{\delta(I)}{m \log m}\right),$$

uniformly in the region given by  $\delta(I) < 1/\sqrt{\log m}$ , such that  $C_1(\log x)^2 < m \leq C_2\delta(I)x^{(k-1)/2}$ , where

$$\Pi(x) = \begin{cases} \mathcal{P}(x) & \text{for } k = 2, \\ \mathcal{P}_\nu(x) & \text{for } k > 2, \end{cases}$$

for any  $\nu$  decreasing as  $1/(\log x)^A$  for some  $A > 0$ .

**Remark 3.3.** Firstly, we should mention that the selection of two different sets of primes depending on  $k$  relies on the natural bound (3–5), which is never attained for  $k > 2$  and  $\Pi(x) = \mathcal{P}(x)$ . Now the conditions on  $m$  and the length of the interval are obtained by taking care of the error term in (3–8) and the last error term in (3–7). It is worth noting that in the case  $k = 2$ , the error term in Conjecture 3.2 when  $m = \delta(I)x^{1/2}$  is chosen is better than that in Conjecture 3.1. We cannot expect such an error term to be uniform in  $m$ . Indeed, as  $m \rightarrow \infty$ , the right-hand side of (3–4) tends to 0, while on the left-hand side, it remains

$$\frac{\#\{p \in \Pi(x) : a_p = t\}}{\#\Pi(x)}.$$

### 3.1. The Lang–Trotter Conjecture

We now consider  $k = 2$ , and thus there exists an elliptic curve  $E/\mathbb{Q}$  isogenous over  $\mathbb{Q}$  to the abelian variety attached to  $f$  by Shimura. Remark 3.3 leads us to the following question: what about the particular values that  $a_p$  attains as  $p$  varies? In this sense we are interested in

the function

$$D_t(x) = \#\{p \in \mathcal{P}(x) : a_p = t\}.$$

In principle, one should not expect to derive any property of  $D_t(x)$  from the Sato–Tate distribution. In general, obtaining information about a function knowing only its average is impossible, unless we know something else. In the beautiful and frequently cited probabilistic study [Lang and Trotter 76], the authors made use of extra arithmetic information about the traces of Frobenius elements at  $p$ , via the Čebotarev density theorem, and made the following conjecture.

**Conjecture 3.4. (Lang–Trotter conjecture.)** *For any given integer  $t$  we have*

$$D_t(x) = C_E(t) \frac{\sqrt{x}}{\log x} (1 + o(1)),$$

where  $C_E(t) = g(0)F(t) = \frac{2}{\pi}F(t)$ .

In order to make this conjecture, the authors used the representations  $\rho_\ell$  and  $r_M$  of the Galois group of  $\overline{\mathbb{Q}}/\mathbb{Q}$  and defined a probabilistic model for the asymptotic behavior of traces of Frobenius. It is, however, interesting that the authors did not seem to have checked the independence of the Sato–Tate distribution and the congruence condition for the traces, even though they use it. Here, using Conjecture 3.2, we provide a direct proof of the Lang–Trotter conjecture.

**Theorem 3.5.** *Let  $t \in \mathbb{Z}$  and suppose that Conjecture 3.2 is true for the normalized newform of weight two attached to an elliptic curve  $E/\mathbb{Q}$  without CM. Then*

$$\frac{\#\{p \in \mathcal{P}(x) : a_p = t\}}{\#\mathcal{P}(x)} = \frac{2}{\pi}F(t) \frac{\sqrt{x}}{\log x} (1 + o(1)).$$

*Proof.* For each real  $x \geq 2$ , let us take

$$Cx^{1/4} < m < \frac{x^{1/2}}{\log x},$$

where  $C = \max\{1, |t|\}$ , let  $I$  be an interval of length  $\delta(I) = (m - |t|)/x^{1/2}$  centered at the origin, and consider the set

$$\widehat{\mathcal{P}}(x) = \left\{ p \in \mathcal{P}(x) : p > \frac{x|t|^2}{(m - |t|)^2} \right\}.$$

Then clearly, we have

$$\begin{aligned} & \left\{ p \in \mathcal{P}(x) : \left| \frac{a_p}{2\sqrt{p}} \right| < \frac{m - |t|}{2\sqrt{x}}, a_p \equiv t \pmod{m} \right\} \\ &= \left\{ p \in \widehat{\mathcal{P}}(x) : \left| \frac{a_p}{2\sqrt{p}} \right| < \frac{m - |t|}{2\sqrt{x}}, a_p \equiv t \pmod{m} \right\} \\ & \quad + O\left(\frac{x^{1/2}}{(\log x)^2}\right) \\ &= \{p \in \mathcal{P}(x) : a_p = t\} + O\left(\frac{x^{1/2}}{(\log x)^2}\right). \end{aligned}$$

Now assume Conjecture 3.2. By multiplying the error  $E(\mathcal{P}(x), t, m; I)$  by  $\sqrt{x}$  and using (3–7), we obtain

$$\begin{aligned} & \frac{\sqrt{x}\#\{p \in \mathcal{P}(x) : a_p = t\}}{\#\mathcal{P}(x)} \\ &= mf_m(t) \frac{\int_{-\frac{m-|t|}{2\sqrt{x}}}^{\frac{m-|t|}{2\sqrt{x}}} g(u)du}{(m - |t|)/\sqrt{x}} \cdot \frac{m - |t|}{m} + O\left(\frac{1}{\log m}\right) \\ &= F(t)g(0) + O\left(\frac{1}{\log m}\right). \end{aligned}$$

Now taking  $x \rightarrow +\infty$  and then  $m \rightarrow +\infty$  gives

$$\lim_{x \rightarrow +\infty} \frac{\sqrt{x}\#\{p \in \mathcal{P}(x) : a_p = t\}}{\#\mathcal{P}(x)} = F(t)g(0) = \frac{2}{\pi}F(t),$$

which completes the proof. □

### 3.2. The Values of Fourier Coefficients of Modular Newforms of Weight at Least 4

For the Fourier coefficients of the discriminant modular form  $\Delta = q \prod_{n \geq 1} (1 - q^n)^{24}$ , i.e., for the values of the Ramanujan tau function, Lehmer conjectured that  $\tau(n) \neq 0$  for all  $n$  and proved that it is enough to verify it for prime frequencies (cf. [Lehmer 47]).

**Conjecture 3.6. (Lehmer’s conjecture.)** *One has  $\tau(p) \neq 0$  for all primes  $p$ .*

In the direction of the previous conjecture, and assuming Conjecture 3.2, we can prove a general result valid for any newform  $f = \sum_{n \geq 1} a_n q^n$  without CM of weight  $k \geq 4$ , level  $N$ , and such that  $\mathbb{Q}(\{a_n\}) = \mathbb{Q}$ , establishing the finiteness of the set of Fourier coefficients with prime frequency and fixed value.

**Theorem 3.7.** *Let  $t$  be a fixed integer and suppose that Conjecture 3.2 is true for a newform  $f = \sum_{n \geq 1} a_n q^n$  without CM of weight  $k \geq 4$ , level  $N$ , and such that  $\mathbb{Q}(\{a_n\}) = \mathbb{Q}$ . Then the set of primes  $p$  such that  $a_p = t$  is finite.*

*Proof.* It suffices to prove that the set  $\{p \in \mathcal{P}(x) : a_p = t\}$  is bounded, independently of  $x$ . For each real  $x \geq 2$ , we will split the set  $\mathcal{P}(x)$  into dyadic intervals. For each interval  $((1 + \nu)^l, (1 + \nu)^{l+1}]$ , we choose an integer  $m_l$  such that

$$(1 + \nu)^{l/4} < m_l < \frac{1}{l}(1 + \nu)^{(l+1)/2}$$

(when there is no such integer, we choose  $m_l = 1$ ) and an interval  $I_l$  centered at the origin of length

$$\delta(I_l) = \frac{m_l - |t|}{(1 + \nu)^{(l+1)(k-1)/2}}.$$

Let  $L = \log x / \log(1 + \nu)$ . Then

$$\begin{aligned} & \#\{p \in \mathcal{P}(x) : a_p = t\} \\ &= \sum_{l \leq L} \#\left\{p \in \mathcal{P}_\nu((1 + \nu)^l) : \frac{|a_p|}{2p^{\frac{k-1}{2}}} \in I_l, \right. \\ & \quad \left. a_p \equiv t \pmod{m_l}\right\} \\ &= \sum_{l \leq L} \#\mathcal{P}_\nu((1 + \nu)^l) f_{m_l}(t) \int_{-\frac{\delta(I_l)}{2}}^{\frac{\delta(I_l)}{2}} g(u) du \\ & \quad + O\left(\sum_{l \leq L} \frac{\nu \#\mathcal{P}_\nu((1 + \nu)^l)}{(1 + \nu)^{\frac{(l+1)(k-1)}{2}} l}\right) \\ &= F(t)g(0) \left(\sum_{l \leq L} \frac{\#\mathcal{P}_\nu((1 + \nu)^l)}{(1 + \nu)^{\frac{(l+1)(k-1)}{2}}}\right) \\ & \quad + O\left(\sum_{l \leq L} \frac{\nu \#\mathcal{P}_\nu((1 + \nu)^l)}{(1 + \nu)^{\frac{(l+1)(k-1)}{2}} l}\right). \end{aligned}$$

The statement of the theorem follows by letting  $x \rightarrow \infty$ , since the right-hand side defines a convergent series.  $\square$

In the case of vanishing Fourier coefficients for the case  $k > 2$ , a similar argument to that used in the proof of Theorem 3.5, based on the bound of the error term  $E(\mathcal{P}(x), 0, m; I)$  in Conjecture 3.2, would lead us to a vast generalization of Lehmer’s conjecture by proving

$$\lim_{x \rightarrow +\infty} \#\{p \in \mathcal{P}(x) : a_p = 0\} = 0.$$

Even though it is unlikely that this bound for the error term is true when the whole of  $\mathcal{P}(x)$  is used, we still believe that the following conjecture is true. Observe that for  $\varepsilon = 1$ , if  $p \mid N$ , then  $a_p = 0$  if and only if  $p^2 \mid N$ ; otherwise,  $a_p = \pm p^{k/2-1}$ .

**Conjecture 3.8.** *Let  $f = \sum_{n \geq 1} a_n q^n$  be a newform without CM of weight  $k \geq 4$ , level  $N$ , and such that  $\mathbb{Q}(\{a_n\}) = \mathbb{Q}$ . Then for a prime  $p$  we have that  $a_p = 0$  if and only if  $p^2 \mid N$ .*

This conjecture has been tested for the 49 normalized newforms without CM, with rational Fourier coefficients of level  $N \leq 10$ , weight  $4 \leq k \leq 12$ , and for all primes  $p < 30\,000$ .

In order to study the vanishing of the Fourier coefficients in general, i.e., not only for prime frequencies, we need the following result.

**Lemma 3.9.** *Let  $f = \sum_{n > 0} a_n q^n \in S_k(\Gamma_1(N))^{\text{new}}$  be a normalized modular newform (with or without CM) with nebentypus  $\varepsilon$  and let  $p$  be a prime not dividing  $N$ . Let  $\zeta$  be a root of unity such that  $\zeta^2 = \varepsilon(p)$ . For every integer  $m \geq 0$  there exists a monic polynomial  $P_m(x) \in \mathbb{Z}[\zeta^2][x]$  of degree  $m$  such that  $a_{p^m} = P_m(a_p)$  and satisfying*

$$\begin{aligned} & P_m \left( p^{(k-1)/2} \zeta \left( x + \frac{1}{x} \right) \right) x^m p^{-(k-1)m/2} \\ &= \zeta^m \frac{x^{2(m+1)} - 1}{x^2 - 1}. \end{aligned} \tag{3-9}$$

*Proof.* We know that for all integers  $m \geq 1$ , one has

$$a_{p^{m+1}} = a_p a_{p^m} - \varepsilon(p) p^{k-1} a_{p^{m-1}}. \tag{3-10}$$

Set  $P_0(x) = 1$  and  $P_1(x) = x$ . For every integer  $m > 1$ , let us denote by  $P_m(x) \in \mathbb{Z}[\zeta^2][x]$  the monic polynomial of degree  $m$  obtained through the recurrent relationship

$$P_{m+1}(x) = x P_m(x) - \zeta^2 p^{k-1} P_{m-1}(x).$$

By (3-10), it is clear that  $P_m(a_p) = a_{p^m}$ . Now the statement can be easily proved by induction.  $\square$

Next, we present the following generalization of [Lehmer 47, Theorem 2].

**Theorem 3.10.** *Let  $f = \sum_{n > 0} a_n q^n \in S_k(\Gamma_0(N))^{\text{new}}$  be a normalized modular newform (with or without CM) such that  $\mathbb{Q}(\{a_n\}) = \mathbb{Q}$ . If  $p$  is a prime such that  $a_{p^m} = 0$ , then one of the following four conditions is satisfied:*

- (i)  $a_p = 0$  and  $p^2 \mid N$ ; in this case,  $a_{p^n} = 0$  for all  $n \geq 1$ .
- (ii)  $a_p = 0$  and  $p \nmid N$ ; in this case,  $a_{p^n} = 0$  if and only if  $n$  is odd.
- (iii)  $p = 2$  and  $a_2 = \pm 2^{k/2}$ ; in this case,  $a_{2^n} = 0$  if and only if  $n \equiv -1 \pmod{4}$ .
- (iv)  $p = 3$  and  $a_3 = \pm 3^{k/2}$ ; in this case,  $a_{3^n} = 0$  if and only if  $n \equiv -1 \pmod{6}$ .

*Proof.* We can assume  $p \nmid N$ , since otherwise,  $a_{p^m} = a_p^m$ , and part (i) is obvious. Let  $\alpha \in \overline{\mathbb{Q}}$  be such that  $a_p = p^{(k-1)/2}(\alpha + 1/\alpha)$ . If  $a_{p^m} = 0$ , then  $\alpha\{2(m+1)-1$

by Lemma 3.9. Since  $a_p = p\{(k-1)/2\}(\alpha+1/\alpha) \in \mathbb{Z}$  and  $k$  is even, either the order  $s$  of  $\alpha$  is 4 or the pair  $(s, p)$  must be  $(8, 2)$  or  $(12, 3)$ . Now using (3–9), the statement follows.  $\square$

Note that condition (iii), respectively (iv), as in the above proposition does not occur when  $2 \mid N$ , respectively  $3 \mid N$ .

**Remark 3.11.** The above theorem can be adapted to a newform  $f \in S_k(\Gamma_1(N))^{\text{new}}$  with even weight and such that the number field  $K$  is  $\mathbb{Q}(\{a_n\}) \neq \mathbb{Q}$ . By Lemma 3.9, the condition  $a_p = 0$  implies that either  $a_p = 0$  or there exists a  $2(m+1)$ th root of unity  $\alpha$  such that  $\sqrt{p}\zeta(\alpha+1/\alpha) \in K \setminus \{0\}$ . In this last case,  $\mathbb{Q}(\sqrt{p}) \subseteq K(\zeta, \alpha+1/\alpha)$  and  $\varphi(2(m+1)) \mid 8[K:\mathbb{Q}]$ , where  $\varphi(\cdot)$  denotes as usual the Euler totient function. In particular,  $a_p = 0$  implies  $a_p = 0$  for almost all primes  $p$ .

The previous theorem, together with Conjecture 3.8, allows us to characterize completely the set of vanishing Fourier coefficients of a general newform.

**Theorem 3.12.** *Assume Conjecture 3.8. Let  $f$  be a newform  $\sum_{n>0} a_n q^n \in S_k(\Gamma_0(N))^{\text{new}}$  without CM, of weight  $k \geq 4$ , and such that  $\mathbb{Q}(\{a_n\}) = \mathbb{Q}$ . Then  $a_n = 0$  if and only if there exists a prime  $p \mid n$  satisfying one of the following three conditions (where  $v_p(n)$  denotes the  $p$ -adic valuation of  $n$ ):*

- (i)  $p^2 \mid N$ .
- (ii)  $p = 2$ ,  $a_2 = \pm 2^{k/2}$ , and  $v_2(n) \equiv -1 \pmod{4}$ .
- (iii)  $p = 3$ ,  $a_3 = \pm 3^{k/2}$ , and  $v_3(n) \equiv -1 \pmod{6}$ .

**Remark 3.13.** Observe that the above theorem states, for example, that the existence of zero Fourier coefficients depends only on  $N$ ,  $a_2$ , and  $a_3$ . For instance, if  $6 \mid N$  and  $N$  is square-free, then  $a_n \neq 0$  for all  $n$ .

#### 4. ARITHMETIC INDEPENDENCE

We begin this section by introducing the following definition.

**Definition 4.1.** Given two normalized newforms  $f \in S_k(\Gamma_1(N))^{\text{new}}$  and  $g \in S_{k'}(\Gamma_1(N'))^{\text{new}}$  without CM, we say that  $f$  and  $g$  are *algebraically independent* if there is no Dirichlet character  $\chi$  such that  $f = g \otimes \chi$ . Otherwise,  $f$  and  $g$  are said to be algebraically dependent.

Of course, if  $f$  and  $g$  are algebraically dependent, then both must have the same weight. We note that for  $k = 2$ , we have the following characterization.

**Proposition 4.2.** *Let  $f$  and  $g$  be normalized newforms of weight two without CM and let us denote by  $A_f$  and  $A_g$  the abelian varieties defined over  $\mathbb{Q}$  attached by Shimura to  $f$  and  $g$ . Then  $f$  and  $g$  are algebraically dependent if and only if there is a morphism  $\pi$  from  $A_f$  to  $A_g$  such that  $\langle \pi^*(g) \rangle = \langle f \rangle$ .*

*Proof.* If  $g = f \otimes \chi$  for some Dirichlet character, the assertion follows from [Shimura 73, Proposition 7]. Assume that there is a nonconstant morphism  $\pi : A_f \rightarrow A_g$ . By [González-Jiménez and Guitart 10, Proposition 1],  $A_g$  is isogenous over  $\mathbb{Q}$  to  $A_f \otimes \chi$  for some Dirichlet character  $\chi$ , and thus there is a  $\sigma \in G_{\mathbb{Q}}$  such that  $f \otimes \chi = g^\sigma$ . Since there is a nonconstant morphism  $\nu : A_f \rightarrow A_g$  such that  $\langle \nu^*(f \otimes \chi) \rangle = \langle f \rangle$ , if  $\langle \pi^*(g) \rangle = \langle f \rangle$ , then there exists  $\phi \in \text{End}(A_g)$  such that  $\langle \phi^*(g^\sigma) \rangle = \langle g \rangle$ . This fact occurs if  $\sigma$  provides an inner twist for  $g$ , i.e., if there exists a Dirichlet character  $\chi_\sigma$  such that  $g^\sigma = g \otimes \chi_\sigma$  (see [González and Lario 01, Lemma 2.1]). Therefore, we obtain that  $f = g \otimes (\chi_\sigma \cdot \chi^{-1})$ .  $\square$

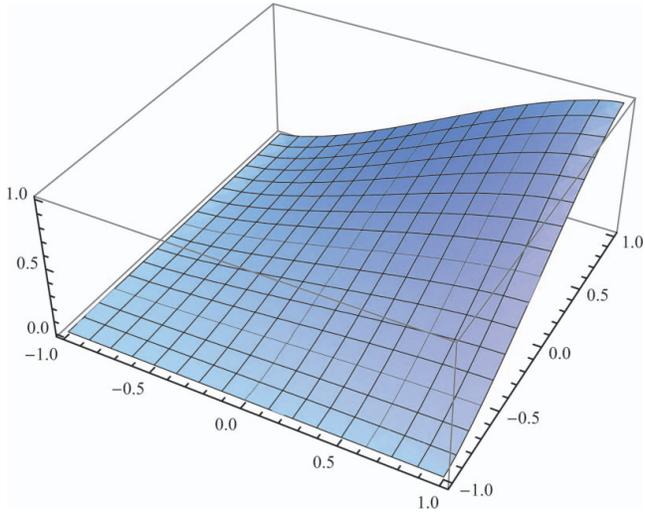
Supported by some computations, we present the following conjecture.

**Conjecture 4.3.** *For every  $1 \leq i \leq d$ , let*

$$f_i = \sum_{n>0} a_n^{(i)} q^n \in S_{k_i}(\Gamma_1(N_i))^{\text{new}}$$

*be a normalized newform without CM and with nebentypus  $\varepsilon_i$ . Let  $K_i = \mathbb{Q}(\{a_n^{(i)}\})$  and denote by  $\mathcal{O}_i$  its ring of integers. Let  $\mathfrak{m}_i$  be an ideal of  $\mathcal{O}_i$  and  $t_i \in \mathcal{O}_i$ . Let  $M$  be any multiple of the conductors of every  $\varepsilon_i$  and let  $\zeta_i$  be a root of unity such that  $\zeta_i^M = \varepsilon_i(M)$  for some integer  $m$  coprime to  $N = \prod_{i=1}^d N_i$ . Assume the following:*

- (i) *For every  $1 \leq i \leq d$ ,  $f_{\mathfrak{m}_i}(t_i) \neq 0$ .*
- (ii) *If there is a  $\sigma \in G_{\mathbb{Q}}$  such that  $f_i^\sigma = f_j$ , then the congruences  $x \equiv t_i^\sigma \pmod{\mathfrak{m}_i^\sigma}$  and  $x \equiv t_j \pmod{\mathfrak{m}_j}$  have a solution in  $\mathcal{O}_j$ .*
- (iii) *The newforms  $f_1, \dots, f_d$  are pairwise algebraically independent.*



**FIGURE 10.** Graph of the two-dimensional distribution function  $G_2(x, y) = G(x)G(y)$  (color figure available online).

Then one has

$$\begin{aligned} & \lim_{x \rightarrow +\infty} \# \left\{ p \in \mathcal{P}(x) : p \equiv m \pmod{M}, a_p^{(i)} \equiv t_i \pmod{m_i}, \right. \\ & \quad \left. \frac{a_p^{(i)}}{2\zeta_i p^{(k_i-1)/2}} \leq a_i, 1 \leq i \leq d \right\} / \\ & \quad \# \{ p \in \mathcal{P}(x) : p \equiv m \pmod{M}, \\ & \quad \quad a_p^{(i)} \equiv t_i \pmod{m_i}, 1 \leq i \leq d \} \\ & = \left( \frac{2}{\pi} \right)^d \int_{-1}^{a_1} \cdots \int_{-1}^{a_d} \sqrt{1-x_1^2} \cdots \sqrt{1-x_d^2} dx_1 \cdots dx_d, \end{aligned}$$

for all  $a_i \in [-1, 1]$ ,  $1 \leq i \leq d$ , where  $\mathcal{P}(x)$  denotes the set of primes up to  $x$  not dividing  $N$ .

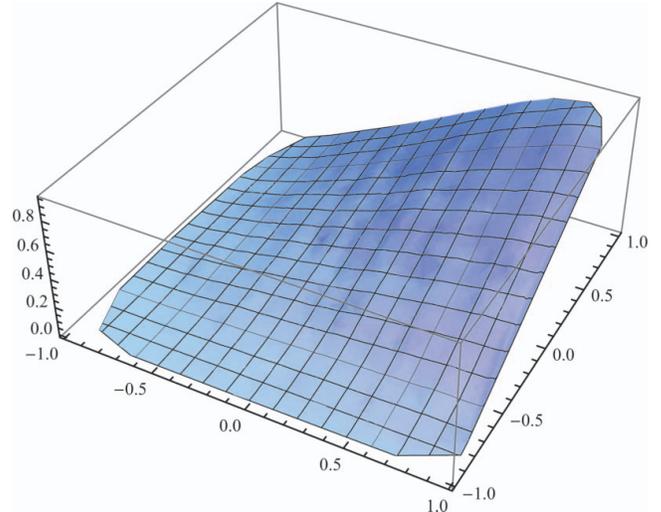
Observe that parts (i) and (ii) are compatibility conditions to avoid finiteness of the set

$$\left\{ p \in \mathcal{P}(x) : a_p^{(i)} \equiv t_i \pmod{m_i}, \leq a_i, 1 \leq i \leq d \right\}.$$

We present some examples with  $m_i = \mathcal{O}_i$ , trivial nebentypus,  $M = 1$ , and  $d = 2$  to support this conjecture. Let  $G(x)$  be the Sato–Tate distribution function (see Section 2). The graph of the two-dimensional distribution function  $G_2(x, y) = G(x)G(y)$  is displayed in Figure 10.

For two normalized newforms  $f_i = \sum_{n>0} a_n^{(i)} q^n \in S_{k_i}(\Gamma_0(N_i))^{\text{new}}$ , set

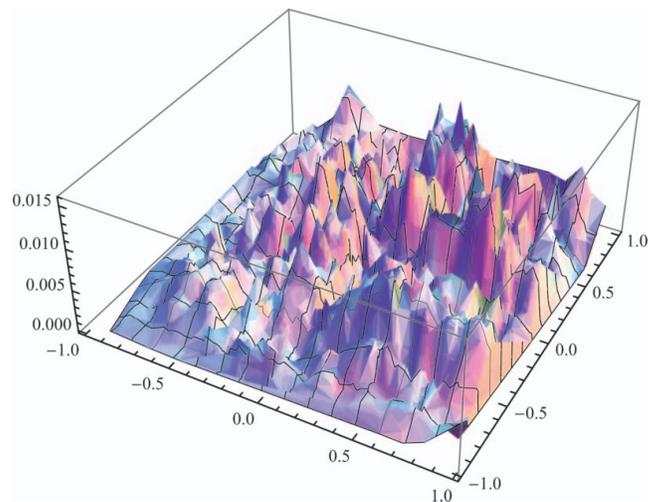
$$\begin{aligned} G_2(a_1, a_2; x) & := \frac{\# \left\{ p \in \mathcal{P}(x) : \frac{a_p^{(i)}}{2p^{(k_i-1)/2}} \leq a_i, 1 \leq i \leq 2 \right\}}{\#\mathcal{P}(x)}, \\ E(a_1, a_2; x) & := |G_2(a_1, a_2; x) - G_2(a_1, a_2)|. \end{aligned}$$



**FIGURE 11.** Graph of  $G_2(a_1, a_2, 30000)$  for  $f_1$  and  $f_2$  as in Example 4.4 (color figure available online).

**Example 4.4. (Distinct levels.)** Let  $f_1 \in S_2(\Gamma_0(11))$  be the normalized newform  $f$  as in Example 2.3 and let  $f_2 \in S_2(\Gamma_0(51))$  be the unique modular newform with rational coefficients. The graphs of  $G_2(a_1, a_2; 30\,000)$  and  $E(a_1, a_2; 30\,000)$  are shown in Figures 11 and 12.

**Example 4.5. (Distinct weights.)** Let  $f_1 \in S_2(\Gamma_0(11))$  be as in Example 4.4 and  $f_2 = \Delta \in S_{12}(\Gamma_0(1))$ . The graphs of  $G_2(a_1, a_2; 30\,000)$  and  $E(a_1, a_2; 30\,000)$  are shown in Figures 13 and 14.



**FIGURE 12.** Graph of  $E(a_1, a_2, 30000)$  for  $f_1$  and  $f_2$  as in Example 4.4 (color figure available online).

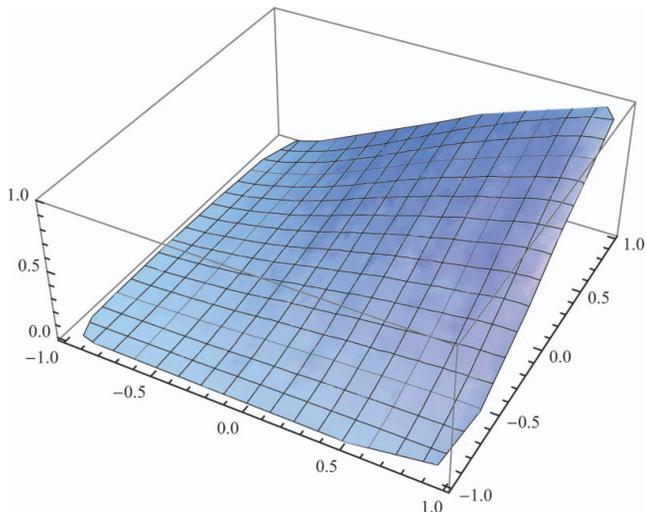


FIGURE 13. Graph of  $G_2(a_1, a_2, 30000)$  for  $f_1$  and  $f_2$  as in Example 4.5 (color figure available online).

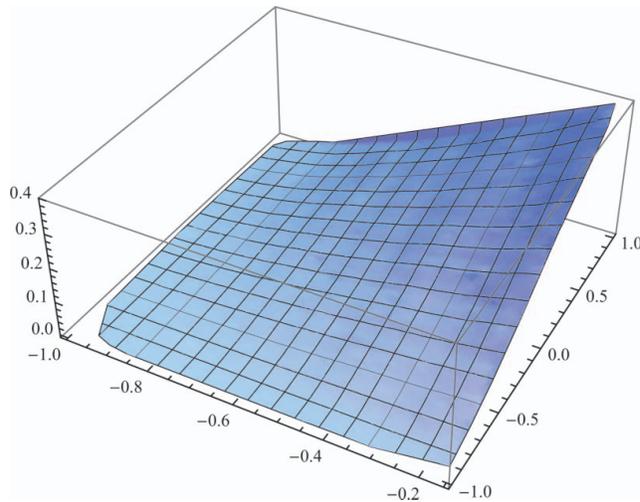


FIGURE 15. Graph of  $G_2(a_1, a_2, 55000)$  for  $f_1$  and  $f_2$  as in Example 4.6 (color figure available online).

**Example 4.6. (Galois conjugates.)** Let  $f_1 \in S_2(\Gamma_0(23))^{\text{new}}$  be as in Example 2.5 and let  $f_2$  be its Galois conjugate. The graphs of  $G_2(a_1, a_2; 55\,000)$  and  $E(a_1, a_2; 55\,000)$  are displayed in Figures 15 and 16.

For fixed newforms  $f_i = \sum_{n>0} a_n^{(i)} q^n$  and  $x, m, M, t_i$ , and  $m_i, 1 \leq i \leq d$ , as in Conjecture 4.3, let us denote by  $n$  the cardinality of the set

$$\mathcal{V} := \{p \in \mathcal{P}(x) : p \equiv m \pmod{M}, a_p^{(i)} \equiv t_i \pmod{m_i} \text{ for } i \leq d\}.$$

Now in general,  $n$  is expected to be nearly

$$\frac{x}{\log x} \frac{1}{\prod_{i=1}^d \text{Norm}(\mathfrak{m}_i) \varphi(M)}.$$

Set

$$D = \max \left\{ \left| \frac{1}{n} \# \left\{ p \in \mathcal{V} : \frac{a_p^{(i)}}{2\zeta_i p^{(k_i-1)/2}} \leq a_i \text{ for } i \leq d \right\} - \left( \frac{2}{\pi} \right)^d \prod_{i=1}^d \int_{-1}^{a_i} \sqrt{1-x^2} dx \right| \right\},$$

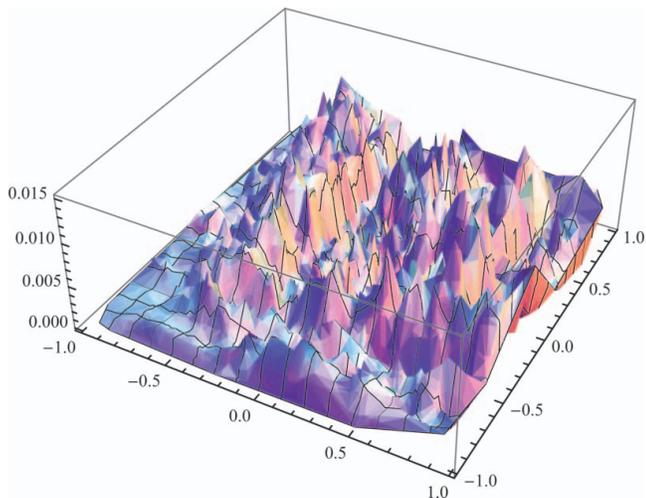


FIGURE 14. Graph of  $E(a_1, a_2, 30000)$  for  $f_1$  and  $f_2$  as in Example 4.5 (color figure available online).

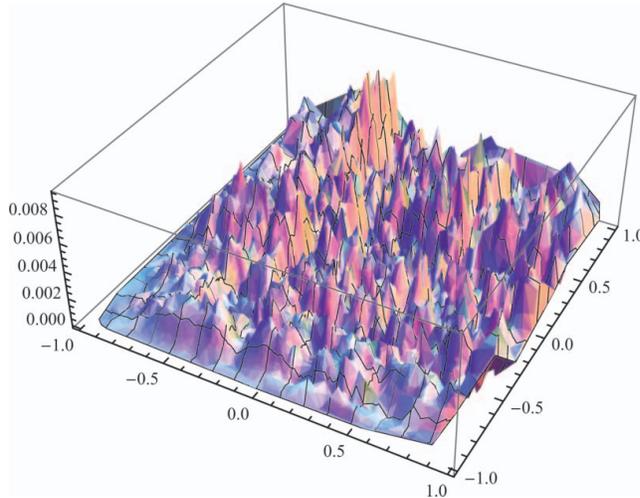


FIGURE 16. Graph of  $E(a_1, a_2, 55000)$  for  $f_1$  and  $f_2$  as in Example 4.6 (color figure available online).

$t_1$	$\mathfrak{m}_1$	$t_3$	$\mathfrak{m}_3$	$m$	$M$	$n$	$D$
1	$\mathcal{O}_1$	1	$\mathbb{Z}$	1	1	25995	0.007
1	$\mathcal{O}_1$	1	$\mathbb{Z}$	1	3	12970	0.008
1	$\mathcal{O}_1$	1	$\mathbb{Z}$	2	3	13024	0.010
0	$2\mathcal{O}_1$	1	$\mathbb{Z}$	1	3	8648	0.011
1	$2\mathcal{O}_1$	1	$\mathbb{Z}$	1	3	4322	0.014
0	$2\mathcal{O}_1$	1	$\mathbb{Z}$	2	3	8679	0.010
1	$2\mathcal{O}_1$	1	$\mathbb{Z}$	2	3	4346	0.017
0	$2\mathcal{O}_1$	1	$3\mathbb{Z}$	2	3	2138	0.020
1	$2\mathcal{O}_1$	0	$3\mathbb{Z}$	1	3	1100	0.039
1	$2\mathcal{O}_1$	1	$3\mathbb{Z}$	1	5	629	0.040
0	$2\mathcal{O}_1$	2	$3\mathbb{Z}$	1	7	929	0.027

**TABLE 4.** Statistic  $D$  for the three newforms  $f_1$  in Table 2,  $f_2$  the Galois conjugate of  $f_1$  and  $f_3$  in Table 1.

as  $(a_1, \dots, a_d)$  runs over the set

$$\left\{ \left( \frac{a_p^{(1)}}{2\zeta_1 p^{(k_1-1)/2}}, \dots, \frac{a_p^{(d)}}{2\zeta_d p^{(k_d-1)/2}} \right) : p \in \mathcal{V} \right\}.$$

Next, we present two tables for  $d = 3$  with the values of  $n$  and  $D$  for  $x = 3 \cdot 10^5$  and different congruence classes. Observe that the independence of such a multivariate measure implies the independence of the three possible bivariate measures. Let  $f_1 \in S_2(\Gamma_0(23))$  be as in Table 2, let  $f_2$  be the Galois conjugate of  $f_1$ , let  $f_3 \in S_2(\Gamma_0(11))$  be as in Table 1, and let  $f_4 \in S_2(\Gamma_1(24))^{\text{new}}$  be as in Table 3. Set  $\mathcal{O}_1 := \mathbb{Z}[\frac{-1+\sqrt{5}}{2}]$  and  $\mathcal{O}_2 := \mathbb{Z}[i]$ .

By part (ii) of Conjecture 4.3, for the newforms  $f_1, f_2, f_3$  we can take  $t_2 = t_1^\sigma$  and  $\mathfrak{m}_2 = \mathfrak{m}_1^\sigma$  without loss of generality, where  $\sigma$  is the nontrivial Galois conjugation on  $\mathbb{Q}(\sqrt{5})$ . We obtain the data displayed in Table 4.

For the newforms  $f_1, f_3, f_4$  we get the results shown in Table 5.

As a consequence of Conjecture 4.3, we present the following result.

**Proposition 4.7.** *Assume that Conjecture 4.3 is true. Let  $A/\mathbb{Q}$  be a modular abelian surface of conductor  $N$  such that  $\text{End}_{\overline{\mathbb{Q}}}(A) \otimes \mathbb{Q}$  is either a real quadratic field or  $\mathbb{Q} \times \mathbb{Q}$ . For a prime  $p \nmid N\ell$ , set  $b_p = \text{Tr}(\rho_\ell(\text{Frob}_p))$ . Then*

$$\lim_{x \rightarrow +\infty} \frac{\#\left\{p \in \mathcal{P}(x) : \frac{b_p}{4\sqrt{p}} \leq a\right\}}{\#\mathcal{P}(x)} = \int_{-1}^a h(u) du,$$

$t_1$	$\mathfrak{m}_1$	$t_3$	$\mathfrak{m}_3$	$t_4$	$\mathfrak{m}_4$	$m$	$M$	$n$	$D$
1	$\mathcal{O}_1$	1	$\mathbb{Z}$	1	$\mathcal{O}_2$	1	8	6457	0.014
1	$\mathcal{O}_1$	1	$\mathbb{Z}$	1	$\mathcal{O}_2$	3	8	6492	0.011
1	$\mathcal{O}_1$	1	$\mathbb{Z}$	1	$\mathcal{O}_2$	5	8	6523	0.013
1	$\mathcal{O}_1$	1	$\mathbb{Z}$	1	$\mathcal{O}_2$	7	8	6521	0.011
1	$\mathcal{O}_1$	1	$\mathbb{Z}$	0	$(2+i)\mathcal{O}_2$	1	8	1598	0.018
1	$\mathcal{O}_1$	1	$2\mathbb{Z}$	1	$\mathcal{O}_2$	3	8	2145	0.023
1	$2\mathcal{O}_1$	0	$2\mathbb{Z}$	1	$\mathcal{O}_2$	7	8	1434	0.037
1	$2\mathcal{O}_1$	2	$3\mathbb{Z}$	1	$\mathcal{O}_2$	5	8	690	0.034

**TABLE 5.** Statistic  $D$  for the three newforms  $f_1$  in Table 2,  $f_3$  in Table 1 and  $f_4$  in Table 3.

where

$$h(u) = \left| \frac{32}{3\pi^2} u(1+u^2) \text{E} \left( 1 - \frac{1}{u^2} \right) - 2\text{K} \left( 1 - \frac{1}{u^2} \right) \right|,$$

and  $\text{E}, \text{K}$  are the elliptic integrals

$$\begin{aligned} \text{E}(u) &= \int_0^1 (1-t^2)^{-1/2} (1-ut^2)^{-1/2} dt, \\ \text{K}(u) &= \int_0^1 (1-t^2)^{-1/2} (1-ut^2)^{1/2} dt. \end{aligned}$$

The even moments are given by

$$\int_{-1}^1 x^{2n} h(x) dx = \frac{c_n c_{n+1}}{16^n},$$

where  $c_n = \frac{1}{n+1} \binom{2n}{n}$  is the  $n$ th Catalan number.

*Proof.* There exist two normalized newforms

$$f_i = \sum_{n>0} a_n^{(i)} q^n \in S_{k_i}(\Gamma_0(N_i))^{\text{new}}, \quad 1 \leq i \leq 2,$$

without CM,  $N_i \mid N$ , and algebraically independent such that  $b_p = a_p^{(1)} + a_p^{(2)}$  for all  $p \nmid N$ . Since the sum of two independent continuous random variables with density functions  $g_1$  and  $g_2$  has as density function the convolution product  $g_1 * g_2$ , we have that

$$h(u) = 2(g * g)(2u) = 2 \int_{-2}^2 g(t)g(2u-t) dt.$$

Since

$$(g * g)(z) = \begin{cases} 0 & \text{if } z \notin [-2, 2], \\ \frac{4}{\pi^2} \int_{-1}^{1+z} \sqrt{1-t^2} \sqrt{1-(z-t)^2} dt & \text{if } z \in [-2, 0], \\ \frac{4}{\pi^2} \int_{-1+z}^1 \sqrt{1-t^2} \sqrt{1-(z-t)^2} dt & \text{if } z \in [0, 2], \end{cases}$$

we obtain that  $(g * g)(-z) = (g * g)(z)$  for all  $z \in [-2, 2]$  and

$$(g * g)(z) = \begin{cases} -2z \left( (4+z^2)E \left[ 1 - \frac{4}{z^2} \right] - 8K \left[ 1 - \frac{4}{z^2} \right] \right) / (3\pi^2) & \text{if } z \in [-2, 0), \\ \frac{16}{3\pi^2} & \text{if } z = 0. \end{cases}$$

Now,

$$\begin{aligned} I_{2n} &= \int_{-1}^1 x^{2n} h(x) dx = 2 \int_{-1}^1 x^{2n} \int_{-2}^2 g(t)g(2x-t) dt dx \\ &= \frac{4}{\pi} \int_{-1}^1 x^{2n} \int_{-1}^1 \sqrt{1-t^2} g(2x-t) dt dx \\ &= \frac{8}{\pi^2} \int_{-1}^1 \sqrt{1-t^2} \int_{(t-1)/2}^{(t+1)/2} x^{2n} \sqrt{1-(2x-t)^2} dx dt \\ &= \frac{1}{2^{2n-2}\pi^2} \int_{-1}^1 \sqrt{1-t^2} \int_{-1}^1 (t+v)^{2n} \sqrt{1-v^2} dv dt \\ &= \frac{1}{2^{2n-2}\pi^2} \sum_{j=0}^{2n} \binom{2n}{j} \int_{-1}^1 t^j \sqrt{1-t^2} dt \\ &\quad \times \int_{-1}^1 v^{2n-j} \sqrt{1-v^2} dv. \end{aligned}$$

An easy computation gives us

$$\int_{-1}^1 t^j \sqrt{1-t^2} dt = \begin{cases} 0 & \text{if } j = 2k + 1, \\ \frac{\pi}{2^{2k+1}} c_k & \text{if } j = 2k, \end{cases}$$

and plugging this back into the previous formula, we get

$$I_{2n} = \frac{1}{2^{4n}} \sum_{j=0}^{2n} \binom{2n}{2j} c_j c_{n-j}.$$

The result is proved modulo the following lemma. □

**Lemma 4.8.** *Let  $c_n$  be the  $n$ th Catalan number. Then*

$$\sum_{j=0}^n \binom{2n}{2j} c_j c_{n-j} = c_n c_{n+1}.$$

*Proof.* Noting that  $c_n = \frac{(2n)!}{n!(n+1)!}$ , we obtain

$$\begin{aligned} &\sum_{j=0}^n \binom{2n}{2j} c_j c_{n-j} \\ &= (2n)! \sum_{j=0}^n \frac{1}{j!(j+1)!(n-j)!(n-j+1)!}, \end{aligned}$$

and multiplying and dividing by  $n!(n+1)!$ , we conclude that

$$\sum_{j=0}^n \binom{2n}{2j} c_j c_{n-j} = \frac{c_n}{16^n} \sum_{j=0}^n \frac{1}{(n-j+1)} \binom{n}{j} \binom{n+1}{n-j}.$$

We now consider the Chu–Vandermonde identity (see, e.g., [Askey 75]) given by

$$\sum_{j=0}^n \binom{x}{j} \binom{y}{n-j} = \binom{x+y}{n}. \tag{4-1}$$

Then

$$\begin{aligned} \binom{2n+1}{n} &= \sum_{j=0}^n \binom{n}{j} \binom{n+1}{n-j} \\ &= \sum_{j=0}^n \frac{n-j+1}{n-j+1} \binom{n}{j} \binom{n+1}{n-j} \\ &= (n+1) \sum_{j=0}^n \frac{1}{n-j+1} \binom{n}{j} \binom{n+1}{n-j} \\ &\quad - \sum_{j=1}^n \frac{j}{n-j+1} \binom{n}{j} \binom{n+1}{n-j} \\ &= (n+1) \sum_{j=0}^n \frac{1}{n-j+1} \binom{n}{j} \binom{n+1}{n-j} - \binom{2n+1}{n-1}, \end{aligned}$$

where we have used again the identity in (4-1) after some rearrangement of the variables in the last sum. The previous identity is the same as

$$\begin{aligned} &\sum_{j=0}^n \frac{1}{n-j+1} \binom{n}{j} \binom{n+1}{n-j} \\ &= \frac{1}{n+1} \left( \binom{2n+1}{n} + \binom{2n+1}{n-1} \right) = c_{n+1}, \end{aligned}$$

which ends the proof of the lemma. □

**Remark 4.9.** The result of the above proposition agrees with that obtained in [Fité et al. 11]. However, when  $\text{End}_{\mathbb{Q}}(A) = \text{End}_{\overline{\mathbb{Q}}}(A)$  is a real quadratic field, the authors of [Fité et al. 11] indeed deduce the same distribution for  $b_p/\sqrt{p}$ , but from an assumption different from ours.

## 5. THE VALUES OF COEFFICIENTS OF MODULAR NEWFORMS

In this section we want to generalize the results obtained in Section 3.1 for newforms of weight at least four with rational Fourier coefficients to normalized newforms with Fourier coefficients lying in any number field. While the source of inspiration for Section 2 is the probabilistic model presented in [Lang and Trotter 76], this section is based on the generalization of this probabilistic model to modular abelian varieties made in [Bayer and González 97].

Let  $f = \sum_{n>0} a_n q^n \in S_k(\Gamma_1(N))$  be a normalized newform without CM and with nebentypus  $\varepsilon$ . Set

$$K := \mathbb{Q}(\{a_n\}), \quad F := \mathbb{Q}(\{a_p^2/\varepsilon(p) : p \nmid N\}), \\ d := [F : \mathbb{Q}].$$

The field  $F$ , with ring of integers  $\mathcal{O}_F$ , is a totally real subfield of  $K$ . We recall that a Dirichlet character  $\chi$  is called an inner twist of  $f$  if there is a  $\sigma \in G_{\mathbb{Q}}$  satisfying  $\sigma a_p = \chi(p)a_p$  for all primes  $p \nmid N$ . If for an embedding  $\sigma : K \hookrightarrow \overline{\mathbb{Q}}$  there is an inner twist, it is unique and is denoted by  $\chi_\sigma$ . The extension  $K/F$  is Galois, and moreover,  $\sigma \in G_{\mathbb{Q}}$  provides an inner twist if and only if  $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/F)$ . In particular, if  $\{\sigma_1, \dots, \sigma_d\}$  is a set of embeddings of  $F$  into  $\overline{\mathbb{Q}}$ , then the newforms  $f^{\sigma_1}, \dots, f^{\sigma_d}$  are pairwise algebraically independent.

Let  $L = \overline{\mathbb{Q}}^{\cap_{\sigma} \ker \chi_\sigma}$ , where  $\sigma$  runs over the set of  $F$ -embeddings of  $K$  into  $\overline{\mathbb{Q}}$ . The extension  $L/\mathbb{Q}$  is the compositum of the cyclic extension  $\overline{\mathbb{Q}}^{\ker \varepsilon}$  and a polyquadratic extension of  $\mathbb{Q}$ . Notice that  $L$  is contained in the  $N$ th cyclotomic field.

Set  $G_L := \text{Gal}(\overline{\mathbb{Q}}/L)$ . Let  $\kappa$  be the residue degree of a prime  $p \nmid N\ell$  in  $L$ . With the same arguments used in [Bayer and González 97, Lemma 6.1], we obtain that the trace and determinant of  $\rho_\ell(\text{Frob}_p^\kappa)$  are in  $\mathcal{O}_F \otimes \mathbb{Z}_\ell$ . So  $\rho_\ell$  can be taken such that  $\rho_\ell(G_L) \subseteq \text{GL}(2, \mathcal{O}_F \otimes \mathbb{Z}_\ell)$ . Let  $\Sigma$  be the set of primes of  $L$  not dividing  $N$ . As in [Bayer and González 97, Section 7], for a prime  $\mathfrak{p} \in \Sigma$  such that  $\ell \nmid N_{L/\mathbb{Q}}(\mathfrak{p})$ , we write

$$a(\mathfrak{p}) := \text{Tr}(\rho_{\ell|G_L}(\text{Frob}_{\mathfrak{p}})).$$

Replacing  $\rho_\ell$  with  $\rho_{\ell|G_L}$ , we redefine  $f_{\mathfrak{m}}(t)$  as follows. For an ideal  $\mathfrak{m}$  of  $\mathcal{O}_F$  and  $t \in \mathcal{O}_F$ , we now define

$$f_{\mathfrak{m}}(t) := \lim_{x \rightarrow +\infty} \frac{\#\{\mathfrak{p} \in \Sigma : N_{L/\mathbb{Q}}(\mathfrak{p}) \leq x, a(\mathfrak{p}) \equiv t \pmod{\mathfrak{m}}\}}{\#\{\mathfrak{p} \in \Sigma : N_{L/\mathbb{Q}}(\mathfrak{p}) \leq x\}}.$$

Since

$$\lim_{x \rightarrow +\infty} \frac{\#\{\mathfrak{p} \in \Sigma : N_{L/\mathbb{Q}}(\mathfrak{p}) = p \leq x\}}{\#\{p \in \Sigma : N_{L/\mathbb{Q}}(\mathfrak{p}) \leq x\}} = 1,$$

we have

$$f_{\mathfrak{m}}(t) = \lim_{x \rightarrow +\infty} \frac{\#\{p \in \mathcal{P}_L(x) : a_p \equiv t \pmod{\mathfrak{m}}\}}{\#\mathcal{P}_L(x)},$$

where  $\mathcal{P}_L(x)$  denotes the set of rational primes up to  $x$  not dividing  $N$  that split completely in  $L$ .

In this case, Conjecture 4.3 allows us to write, for  $t \in \mathcal{O}_F$  and an ideal  $\mathfrak{m}$  of  $\mathcal{O}_F$ ,

$$\lim_{x \rightarrow +\infty} \#\left\{p \in \mathcal{P}_L(x) : a_p \equiv t \pmod{\mathfrak{m}}, \frac{a_p^{\sigma_i}}{2p^{(k-1)/2}} \leq a_i, \right. \\ \left. 1 \leq i \leq d\right\} / \#\mathcal{P}_L(x) \\ = f_{\mathfrak{m}}(t) \left(\frac{2}{\pi}\right)^d \int_{-1}^{a_1} \cdots \int_{-1}^{a_d} \sqrt{1-x_1^2} \cdots \\ \times \sqrt{1-x_d^2} dx_1 \cdots dx_d,$$

for all  $a_i \in [-1, 1]$ .

Again by [Ribet 85, Theorem 3.1],

$$\rho_\ell(G_L) = \left\{ \sigma \in \text{GL}(2, \mathcal{O}_F \otimes \mathbb{Z}_\ell) : \det(\sigma) \in \mathbb{Z}_\ell^{*(k-1)} \right\}$$

for almost all primes  $\ell$ . In particular,  $\text{SL}(2, \mathcal{O}_F \otimes \mathbb{Z}_\ell) \subset \rho_\ell(G_L)$  for almost all primes  $\ell$ . By [Bayer and González 97, Lemma 7.1], the group  $(\prod_\ell \rho_\ell)(G_{\mathbb{Q}})$  is open in  $\prod_\ell \rho_\ell(G_{\mathbb{Q}})$ .

Now we consider the sequence  $N_{F/\mathbb{Q}}(\mathfrak{m})f_{\mathfrak{m}}(t)$ , where the indices  $\mathfrak{m}$  run through the filter of all nonzero ideals of the ring  $\mathcal{O}_F$ . Since  $(\prod_\ell \rho_\ell)(G_{\mathbb{Q}})$  is open in  $\prod_\ell \rho_\ell(G_{\mathbb{Q}})$  and  $r_\lambda(G_{\mathbb{Q}}) = \text{GL}(2, \mathcal{O}_F/\lambda)$  for almost all primes  $\lambda$  of  $F$ , by [Bayer and González 97, Lemma 7.4 and Theorem 7.5], there exists a bounded function  $F : \mathcal{O} \rightarrow \mathbb{R}$  with  $F(t) = \lim_{\mathfrak{m}} N_{L/\mathbb{Q}}(\mathfrak{m})f_{\mathfrak{m}}(t)$ , and moreover, there exists an ideal  $\mathfrak{m}_0$  such that

$$F(t) = N_{F/\mathbb{Q}}(\mathfrak{m}_0)f_{\mathfrak{m}_0}(t) \prod_{\lambda \nmid \mathfrak{m}_0} N_{F/\mathbb{Q}}(\lambda)f_\lambda(t),$$

where for the prime ideal  $\lambda \nmid \mathfrak{m}_0$  of  $F$  whose norm is  $\ell^\nu$ , we have

$$N_{F/\mathbb{Q}}(\lambda)f_\lambda(t) = \begin{cases} \frac{\ell^{2\nu}}{\ell^{2\nu}-1} & \text{if } t \equiv 0 \pmod{\lambda}, \\ \frac{\ell^\nu(\ell^{2\nu}-\ell^\nu-1)}{(\ell^\nu-1)(\ell^{2\nu}-1)} & \text{otherwise.} \end{cases}$$

In order to simplify the notation, for a prime  $p$  we write

$$\vec{A}_p = \left( \frac{a_p^{\sigma_1}}{p^{(k-1)/2}}, \dots, \frac{a_p^{\sigma_d}}{p^{(k-1)/2}} \right),$$

and  $\mu_d$  denotes the  $d$ -dimensional measure with density function  $\prod_{i=1}^d g(x_i)$ , where we recall that  $g(x)$  is the density of the Sato–Tate distribution. As in Section 3, we want to have a bound for the error function

$$E(\Pi(x), t, \mathbf{m}; I) = \frac{\#\{p \in \Pi(x) : a_p \equiv t \pmod{\mathbf{m}}, \vec{A}_p \in I^d\}}{\#\Pi(x)} - f_{\mathbf{m}}(t) \int_{I^d} d\mu_d$$

for a fixed  $t \in \mathcal{O}_F$ , where  $I$  is a subinterval of  $[-1, 1]$  containing 0. A completely analogous argument as in Section 3 leads us to

$$f_{\mathbf{m}}(t) \int_I d\mu_d = F(t) \left(\frac{2}{\pi}\right)^d \frac{\delta(I)^d}{N_{F/\mathbb{Q}}(\mathbf{m})} + O\left(\frac{\delta(I)^d}{N_{F/\mathbb{Q}}(\mathbf{m}) \log(N_{F/\mathbb{Q}}(\mathbf{m}))}\right) + O\left(\frac{\delta(I)^{d+2}}{N_{F/\mathbb{Q}}(\mathbf{m})}\right). \tag{5-1}$$

Hence, again by the previous identity, the Čebotarev density theorem, equation (3–8), Conjecture 4.3, and the square-root restriction, we end up with the following conjecture. We will use the set

$$\mathcal{P}_{L,\nu}(x) := \{p \in \mathcal{P}_L(x) : x < p \leq (1 + \nu)x\}.$$

**Conjecture 5.1.** *Let  $x \geq 2$ . With the notation as above, there exist constants  $C_1$  and  $C_2$  depending on  $t$  and the newform  $f$  such that as  $I$  runs through subintervals of  $[-1, 1]$  containing 0, we have*

$$E(\Pi(x), t, \mathbf{m}; I) = O\left(\frac{\delta(I)^d}{N_{F/\mathbb{Q}}(\mathbf{m}) \log(N_{F/\mathbb{Q}}(\mathbf{m}))}\right),$$

uniformly in the region

$$\delta(I) < \frac{1}{\sqrt{\log N_{F/\mathbb{Q}}(\mathbf{m})}},$$

$$C_1(\log x)^2 < N_{F/\mathbb{Q}}(\mathbf{m}) \leq C_2 \left(\delta(I)x^{(k-1)/2}\right)^d,$$

where

$$\Pi(x) = \begin{cases} \mathcal{P}_L(x) & \text{for } (k-1)d = 1, \\ \mathcal{P}_{L,\nu}(x) & \text{for } (k-1)d \geq 2, \end{cases}$$

and  $\nu$  is any positive number  $\nu > 1/\log x$ .

**Theorem 5.2.** *Keep the notation as above. Assume that Conjecture 5.1 is true. Let  $f = \sum_{n>0} a_n q^n \in S_k(\Gamma_1(N))^{\text{new}}$  be a normalized newform without CM and*

$k \geq 2$ . Then

$$\#\{p \in \mathcal{P}_L(x) : a_p = t\} = \begin{cases} \frac{2}{\pi^{[L:\mathbb{Q}]}} F(t) \frac{\sqrt{x}}{\log x} (1 + o(1)) & \text{if } (k-1)d = 1, \\ \frac{1}{[L:\mathbb{Q}]} F(t) \left(\frac{2}{\pi}\right)^d \log(\log x) \times (1 + o(1)) & \text{if } (k-1)d = 2, \\ O(1) & \text{if } (k-1)d > 2. \end{cases}$$

*Proof.* The cases  $(k-1)d = 1$  and  $(k-1)d \geq 3$  are completely analogous to Theorems 3.5 and 3.7 by replacing  $m$  by  $N_{F/\mathbb{Q}}(\mathbf{m})$  and using intervals of the appropriate length

$$\delta(I) = \frac{|N_{F/\mathbb{Q}}(\mathbf{m})|^{1/d} - |N_{F/\mathbb{Q}}(t)|^{1/d}}{x^{(k-1)/2}}$$

in the first case, and in the second,

$$\delta(I_l) = \frac{|N_{F/\mathbb{Q}}(\mathbf{m}_l)|^{1/d} - |N_{F/\mathbb{Q}}(t)|^{1/d}}{2^{(l+1)(k-1)/2}}.$$

We then focus on the case  $(k-1)d = 2$ .

For each real  $x \geq 2$ , we will choose  $\nu > 1/\log x$  and split the set  $\mathcal{P}_L(x)$  into dyadic intervals of length  $(1 + \nu)$ . On each interval  $J_\nu(l) = [(1 + \nu)^l, (1 + \nu)^{l+1})$  we choose an integer  $\mathbf{m}_l$  such that

$$(1 + \nu)^{l/4} < \mathbf{m}_l < \frac{(1 + \nu)^{(l+1)/2}}{l}$$

(when there is no such integer, we choose  $m_l = 1$ ) and an interval  $I_l$  of length

$$\delta(I_l) = \frac{|N_{F/\mathbb{Q}}(\mathbf{m})|^{1/d} - |N_{F/\mathbb{Q}}(t)|^{1/d}}{x^{(k-1)/2}}$$

centered at the origin. Then

$$\begin{aligned} & \{p \in \mathcal{P}_L(x) : a_p = 0\} \\ &= \sum_{l \leq B} \left\{ p \in \mathcal{P}_{L,\nu}((1 + \nu)^l) : \vec{A}_p \in I_l, a_p \equiv 0 \pmod{\mathbf{m}_l} \right\} \\ &= \sum_{l \leq B} \#\mathcal{P}_{L,\nu}((1 + \nu)^l) f_{\mathbf{m}}(t) \int_{I^d} d\mu_d \\ &+ O\left(\sum_{l \leq B} \frac{\#\mathcal{P}_{L,\nu}((1 + \nu)^l)}{(1 + \nu)^{\frac{d(l+1)(k-1)}{2}l}}\right). \end{aligned} \tag{5-2}$$

We now use (5–1) to obtain

$$\begin{aligned} & \sum_{l \leq B} \#\mathcal{P}_{L,\nu}((1+\nu)^l) f_m(t) \int_{I^d} d\mu_d \\ &= F(t)(g(0))^d \left( \sum_{l \leq B} \frac{\#\mathcal{P}_{L,\nu}((1+\nu)^l)}{(1+\nu)^{\frac{d(l+1)(k-1)}{2}}} \right) \\ &= F(t)(g(0))^d \left( \sum_{l \leq B} \sum_{\substack{p \in J_\nu(l) \\ p \in \mathcal{P}_L(x)}} \frac{1}{p} \right) \\ & \quad + O\left( \sum_{l \leq B} \frac{\nu \#\mathcal{P}_{L,\nu}((1+\nu)^l)}{(1+\nu)^{\frac{d(l+1)(k-1)}{2}}} \right) \\ &= F(t)(g(0))^d \left( \sum_{\substack{p \leq x \\ p \in \mathcal{P}_L(x)}} \frac{1}{p} \right) \\ & \quad + O\left( \sum_{l \leq B} \frac{\nu \#\mathcal{P}_{L,\nu}((1+\nu)^l)}{(1+\nu)^{\frac{d(l+1)(k-1)}{2}}} \right). \end{aligned}$$

The result follows by plugging this back into (5–2) and using

$$\sum_{\substack{p \leq x \\ p \in \mathcal{P}_L(x)}} \frac{1}{p} = \frac{1}{[L : \mathbb{Q}]} \log \log x + O(1).$$

This completes the proof of the theorem. □

We also state the following generalization of Conjecture 3.8 and thus also of Lehmer’s conjecture.

**Conjecture 5.3.** *With the same notation as in Theorem 5.2, if  $(k-1)[F : \mathbb{Q}] > 2$  and  $a_p = 0$ , then  $p \mid N$  or  $p$  does not split completely in  $L$ . In particular, if  $f$  does not have any inner twist and  $(k-1)[K : \mathbb{Q}] > 2$ , then  $a_p = 0$  if and only if  $p^2 \mid N$ .*

**ACKNOWLEDGMENTS**

We would like to thank Carles Barcelo for his help in the statistical part of this article, and also the referee for the suggestions that made the paper more complete.

The first author is partially supported by DGICYT grant MTM2009-13060-C02-02, the second by DGICYT grant MTM2009-11068.

**REFERENCES**

[Akiyama and Tanigawa 99] S. Akiyama and Y. Tanigawa. “Calculation of Values of  $L$ -Functions Associated to Elliptic Curves.” *Math. Comp.* 68:227 (1999), 1201–1231.

[Askey 75] R. Askey. *Orthogonal Polynomials and Special Functions*. SIAM, 1975.

[Balog and Ono 01] A. Balog and K. Ono. “The Chebotarev Density Theorem in Short Intervals and Some Questions of Serre.” *J. Number Theory* 91:2 (2001), 356–371.

[Barnet-Lamb et al. 11] T. Barnet-Lamb, D. Geraghty, M. Harris, and R. Taylor. “A Family of Calabi–Yau Varieties and Potential Automorphy II.” *Publ. Res. Inst. Math. Sci.* 47:1 (2011), 29–98.

[Bayer and González 97] P. Bayer and J. González. “On the Hasse–Witt Invariants of Modular Curves.” *Experiment. Math.* 6:1 (1997), 57–76.

[D’Agostino and Stephens 86] Ralph B. D’Agostino and Michael A. Stephens, editors. *Goodness-of-Fit Techniques*, Statistics: Textbooks and Monographs 68. Marcel Dekker, 1986.

[Fité et al. 11] F. Fité, K. S. Kedlaya, A. V. Sutherland, and V. Rotger. “The Sato–Tate Conjecture and Galois Representations.” Preprint, 2011.

[González and Lario 01] J. González and J.-C. Lario. “ $\mathbb{Q}$ -Curves and Their Manin Ideals.” *Amer. J. Math.* 123:3 (2001), 475–503.

[González-Jiménez and Guitart 10] E. González-Jiménez and X. Guitart. “On the Modularity Level of Modular Abelian Varieties over Number Fields.” *J. Number Theory* 130:7 (2010), 1560–1570.

[González et al. 10] J. González, J. Jiménez-Urroz, and J.-C. Lario. “Cropping Euler Factors of Modular  $L$ -Functions.” To appear in *Forum Math.* (available at <http://arxiv.org/abs/0810.4224v2>), 2010.

[Lang and Trotter 76] S. Lang and H. Trotter. *Frobenius Distributions in  $GL_2$ -Extensions*, Lecture Notes in Mathematics 504. Springer, 1976.

[Lehmer 47] D. H. Lehmer. “The Vanishing of Ramanujan’s Function  $\tau(n)$ .” *Duke Math. J.* 14 (1947), 429–433.

[Mazur 08] B. Mazur. “Finding Meaning in Error Terms.” *Bull. Amer. Math. Soc. (N.S.)* 45:2 (2008), 185–228.

[Ribet 85] K. A. Ribet. “On  $l$ -adic Representations Attached to Modular Forms, II.” *Glasgow Math. J.* 27 (1985), 185–194.

[Serre 81] J.-P. Serre. “Quelques applications du théorème de densité de Chebotarev.” *Inst. Hautes Études Sci. Publ. Math.* 54 (1981), 323–401.

[Serre 89] J.-P. Serre. *Abelian  $l$ -adic Representations and Elliptic Curves*, second edition, Advanced Book Classics. Addison-Wesley, 1989.

[Shimura 73] G. Shimura. “On the Factors of the Jacobian Variety of a Modular Function Field.” *J. Math. Soc. Japan* 25 (1973), 523–544.

[Stein 07] W. Stein. “Elliptic Curves and Convergence: Sato–Tate, GRH, and BSD.” Available online (<http://modular.math.washington.edu/talks/>), 2007.

Josep González, Departament de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya (UPC),  
Av. Víctor Balaguer, s/n., E-08800 Vilanova i la Geltrú (josepg@ma4.upc.edu)

Jorge Jiménez-Urroz, Departament de Matemàtica Aplicada IV, Universitat Politècnica de Catalunya (UPC), Edifici  
C3-Campus Nord, Jordi Girona, 1-3, E-08034 Barcelona (jjimenez@ma4.upc.edu)

Received June 2, 2011; accepted August 3, 2011.