Journal of Number Theory 129 (2009) 681–714

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Effective equidistribution of eigenvalues of Hecke operators

M. Ram Murty [a,*,1], Kaneenika Sinha [b]

[a] Department of Mathematics and Statistics, Queen's University, Jeffery Hall, 99 University Avenue, Kingston, Ontario, Canada K7L 3N6
[b] Department of Mathematical and Computational Sciences, University of Toronto at Mississauga, Mississauga, Ontario, Canada L5L 1C6

ARTICLE INFO

Article history:
Received 13 October 2007
Revised 9 May 2008
Available online 17 December 2008
Communicated by David Goss

ABSTRACT

In 1997, Serre proved an equidistribution theorem for eigenvalues of Hecke operators on the space $S(N,k)$ of cusp forms of weight k and level N. In this paper, we derive an effective version of Serre's theorem. As a consequence, we estimate, for a given d and prime p coprime to N, the number of eigenvalues of the pth Hecke operator T_p acting on $S(N,k)$ of degree less than or equal to d. This allows us to determine an effectively computable constant B_d such that if $J_0(N)$ is isogenous to a product of $\mathbb{Q}$-simple abelian varieties of dimensions less than or equal to d, then $N \leqslant B_d$. We also study the effective equidistribution of eigenvalues of Frobenius acting on a family of curves over a fixed finite field as well as the eigenvalue distribution of adjacency matrices of families of regular graphs. These results are derived from a general "all-purpose" equidistribution theorem.

1. Introduction

Let $S(N,k)$ be the space of cusp forms of weight k on $\Gamma_0(N)$ and for every positive integer n, let $T_n(N,k)$ be the nth Hecke operator acting on $S(N,k)$. Let $s(N,k)$ be the dimension of $S(N,k)$ and let $a_{p,i}$, $1 \leqslant i \leqslant s(N,k)$, denote the eigenvalues of T_p, counted with multiplicity. The asymptotic distribution of eigenvalues of the Hecke operator T_p on $S(N,k)$ for a prime p is an interesting and difficult problem. By a result of Deligne [7], we know that the eigenvalues of T_p lie in the interval

$$\left[-2p^{\frac{k-1}{2}}, 2p^{\frac{k-1}{2}}\right].$$

* Corresponding author.
E-mail addresses: murty@mast.queensu.ca (M.R. Murty), kansinha@math.ualberta.ca (K. Sinha).
1 Research partially supported by an NSERC grant.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2008.10.010

Thus, the eigenvalues of the normalized Hecke operator

$$T'_p = \frac{T_p}{p^{\frac{k-1}{2}}}$$

lie in the interval $[-2, 2]$. If we fix N and k and vary the prime p, the distribution of the eigenvalues is predicted by the Sato–Tate conjecture (see [27]). In the generic case, the eigenvalues of a fixed Hecke eigenform are expected to be equidistributed in $[-2, 2]$ with respect to the measure

$$\mu_\infty = \frac{1}{\pi}\sqrt{1 - \frac{x^2}{4}}\,dx.$$

Recently, Taylor [29] has announced that this conjecture is true in the case $k = 2$ and N is squarefree and the eigenform has rational integer coefficients. Such forms correspond to elliptic curves over $\mathbb{Q}$ by a celebrated theorem of Wiles [31].

In his 1997 paper [26], Serre considered a "vertical" Sato–Tate conjecture by fixing a prime p and varying N and k. He proved the following theorem:

Theorem 1. *Let N_λ, k_λ be positive integers such that k_λ is even, $N_\lambda + k_\lambda \to \infty$ and p is a prime not dividing N_λ for any λ. Then the family of eigenvalues of the normalized pth Hecke operator*

$$T'_p(N_\lambda, k_\lambda) = \frac{T_p(N_\lambda, k_\lambda)}{p^{(k_\lambda - 1)/2}}$$

is equidistributed in the interval $\Omega = [-2, 2]$ with respect to the measure

$$\mu_p := \frac{p+1}{\pi}\frac{(1 - x^2/4)^{1/2}}{(p^{1/2} + p^{-1/2})^2 - x^2}\,dx.$$

Serre's theorem has several applications, and some of the most interesting ones are as follows. For any positive integer d,

$$\#\bigl\{1 \leqslant i \leqslant s(N,k)\colon\ \bigl[\mathbb{Q}(a_{p,i}) : \mathbb{Q}\bigr] \leqslant d\bigr\} = \mathrm{o}\bigl(s(N,k)\bigr) \quad \text{as } N + k \to \infty.$$

In particular,

$$\#\bigl\{1 \leqslant i \leqslant s(N,k)\colon\ a_{p,i} \in \mathbb{Z}\bigr\} = \mathrm{o}\bigl(s(N,k)\bigr) \quad \text{as } N + k \to \infty.$$

Consequently, there are only finitely many values of N such that $J_0(N)$ is isogenous to a product of elliptic curves. More generally, there are only finitely many values of N such that $J_0(N)$ is isogenous to a product of $\mathbb{Q}$-simple abelian varieties A_f with dimensions less than or equal to d. The limitation of Serre's theorem and its proof is that it does not give us an effective bound for these values of N. In this paper, we obtain an effective version of Serre's theorem. We prove

Theorem 2. *Let N be a positive integer and p a prime number coprime to N. For an interval $[\alpha, \beta] \subset [-2, 2]$,*

$$\frac{1}{s(N,k)}\#\left\{1 \leqslant i \leqslant s(N,k)\colon\ \frac{a_{p,i}}{p^{\frac{k-1}{2}}} \in [\alpha, \beta]\right\} = \int_\alpha^\beta \mu_p + \mathrm{O}\left(\frac{\log p}{\log kN}\right),$$

where the implied constant is effectively computable.

Remark 3. In the special case $N = 1$ and $k \to \infty$, Serre's equidistribution theorem was also discovered by Conrey, Duke and Farmer [6]. A version of Serre's theorem with error term, in this special case, was obtained by E.P. Golubeva in [9], but this result is not effective. The error obtained there is

$$O_\epsilon\left(\frac{\log p}{(\log k)^{1-\epsilon}}\right)$$

for any $\epsilon > 0$. However, it seems that in the application of Vinogradov's trigonometric polynomial, only the cosine polynomial is treated and the sine polynomial is left untreated in [9]. Thus, the proof seems to be incomplete. In the context of Maass forms, Sarnak [24] obtained an analogous theorem in 1984.

If $\alpha = \beta$, then the integral in Theorem 2 is zero. Thus, for a fixed number α,

$$\#\left\{i\colon\ \frac{a_{p,i}}{p^{\frac{k-1}{2}}} = \alpha\right\} = O\left(\frac{s(N,k)\log p}{\log kN}\right). \tag{1}$$

By careful estimation, in the special case $\alpha = \beta$, we also get a sharper error term. Moreover, keeping future applications in mind, we determine an explicit constant in the error term. In fact, we have the following result:

Theorem 4. *Let N be a positive integer and p be a prime not dividing N. Then, for a fixed number α lying in $[-2, 2]$,*

$$\#\left\{i\colon\ \frac{a_{p,i}}{p^{\frac{k-1}{2}}} = \alpha\right\} \leqslant \frac{3s(N,k)\log p}{\log kN} + \frac{63kN\log p}{\log kN},$$

for $N \geqslant e^{1024}$.

As a consequence of Theorem 4, we deduce the following:

Theorem 5. *Let $r = s(N,k)$. Let d be a positive integer and $K_{p,i} = \mathbb{Q}(a_{p,i})$ for every $1 \leqslant i \leqslant r$. Then*

$$\#\left\{i\colon\ [K_{p,i} : \mathbb{Q}] = d\right\} \leqslant d\prod_{j=1}^{d}\left(2\binom{d}{j}\left(2p^{\frac{k-1}{2}}\right)^j + 1\right)\left(3s(N,k)\frac{\log p}{\log kN} + \frac{63kN}{\log kN}\right),$$

provided $N \geqslant e^{1024}$.

Theorems 4 and 5 will be proved in Sections 14 and 15. Theorem 5 gives us important arithmetic information about $J_0(N)$, the Jacobian of the modular curve $X_0(N)$. In Section 16, we prove the following theorem:

Theorem 6. *If $J_0(N)$ is isogenous to a product of $\mathbb{Q}$-simple abelian varieties of dimension less than or equal to d, then $N \leqslant C(d)$ for some effectively computable constant $C(d)$.*

As will be seen later, the effective nature of $C(d)$ allows us to deduce the following corollary, a result also obtained by Royer [23] using different methods.

Corollary 7. *$J_0(N)$ has a $\mathbb{Q}$-simple factor of dimension*

$$\gg \sqrt{\log\log N}.$$

The main ingredients in the proof of Theorem 2 are the Theorem 8 (stated below), the Eichler–Selberg trace formula and certain trigonometric polynomials, which give a good approximation for the characteristic function of an interval contained in [0, 1]. In the next eight sections, we will briefly state the information needed in order to prove Theorem 2.

As in [26], there are two other analogous contexts in which one can ask similar questions. The first is the case where we fix a finite field $\mathbb{F}_q$ and consider a family of curves C_r of genus g_r with g_r tending to infinity as $r \to \infty$. The Frobenius endomorphism acts on the curve over $\bar{\mathbb{F}}_q$ and one can study the equidistribution of the sets A_r of eigenvalues of this endomorphism acting on the curves C_r. The precise result can be found in Theorem 33. In a similar vein, let X_i be a family of k-regular graphs. In Theorem 34, we derive an equidistribution theorem concerning the eigenvalues of the adjacency matrices of the X_i's.

All of these results will be derived from an "all-purpose" equidistribution theorem (Theorem 8 below). We believe this theorem will have further applications and expect to pursue them in future research.

2. Uniform distribution of sequences

A sequence of real numbers $\{x_n\}$ is said to be *uniformly distributed* (or equivalently, *equidistributed*) mod 1 if for every interval $I \subset [0, 1]$, we have

$$\lim_{V\to\infty} \frac{\#\{n \leqslant V:\ x_n \bmod 1 \in I\}}{V} = \ell(I),$$

where $\ell(I)$ is the usual Lebesgue measure equal to the length of the interval I. The well-known criterion of Weyl [16] states that the sequence $\{x_n\}$ is uniformly distributed if and only if

$$\sum_{n\leqslant V} e(mx_n) = o(V), \quad e(t) = e^{2\pi i t},$$

as $V \to \infty$ for every integer $m \neq 0$. Since the trigonometric polynomials are dense in $C^1[0, 1]$, this criterion is equivalent to the assertion that

$$\lim_{V\to\infty} \frac{1}{V} \sum_{n\leqslant V} f(x_n) = \int_0^1 f(t)\,dt,$$

for every continuous function f. It is easy to see that Weyl's criterion is necessary. Indeed, if the limits

$$\lim_{V\to\infty} \frac{\#\{n \leqslant V:\ x_n \bmod 1 \in I\}}{V} = \ell(I)$$

hold for every interval I, then, by the usual argument of approximating continuous functions via step functions and using the theory of the Riemann integral, we deduce that for every piece-wise continuous function f (or more generally, for any Riemann integrable function f),

$$\lim_{V\to\infty} \frac{1}{V} \sum_{n\leqslant V} f(x_n) = \int_0^1 f(t)\,dt.$$

Putting $f(x) = e(mx)$, we deduce Weyl's criterion. For the sufficiency, one needs to approximate the characteristic function of an interval by trigonometric polynomials. This is usually done by invoking the Weierstrass approximation theorem. Though this is the most expedient route to prove sufficiency, its limitation is that we cannot write down error estimates.

In 1948, Erdös and Turán [8] proved an inequality which can be viewed as an effective version of Weyl's criterion in the sense that it allows us to deduce error estimates in terms of exponential sums. They proved that there exist constants c_1, c_2 such that

$$\left|\#\{n \leqslant V\colon\ x_n \bmod 1 \in I\} - V\ell(I)\right| \leqslant \frac{c_1 V}{M+1} + c_2 \sum_{m=1}^{M} \frac{1}{m}\left|\sum_{n \leqslant V} e(mx_n)\right|.$$

The pair of constants $c_1 = 1$, $c_2 = 3$ is given on p. 8 of Montgomery [16]. The pair $c_1 = c_2 = 1$ was recently derived in [15]. Before we proceed, we clarify our use of the term "effective." The Erdös–Turán inequality is effective in the sense that it allows us to determine the error term in the equidistribution theorem, provided we have estimates for the exponential sums that appear in the inequality. It is strong enough to establish Weyl's theorem on equidistribution. Indeed, if Weyl's criterion holds, then for any given M and $\epsilon_1 > 0$,

$$\left|\sum_{n \leqslant V} e(mx_n)\right| \ll \epsilon_1 V,$$

for $m \neq 0$ and $m \leqslant M$ and $V \geqslant c(M, \epsilon_1)$, a sufficiently large constant depending on M and ϵ_1. By the Erdös–Turán inequality, we have

$$\left|\frac{1}{V}\#\{n \leqslant V\colon\ x_n \bmod 1 \in I\} - \ell(I)\right| \leqslant \frac{1}{M+1} + 3\epsilon_1 \log M.$$

Choosing $M = [1/\epsilon_1]$ and observing that $x \log x \to 0$ as $x \to 0$, we deduce that the sequence is uniformly distributed.

In many applications of interest (like the context of the present paper), the sequence x_n may not be uniformly distributed with respect to the Lebesgue measure, but with respect to some other measure. Let μ be a measure on $[0, 1]$. We will say that the sequence $\{x_n\}$, with $0 \leqslant x_n \leqslant 1$, is μ-equidistributed in the following sense. For any piece-wise continuous function $f \in L^1[0, 1]$, we have

$$\lim_{V \to \infty} \frac{1}{V} \sum_{n \leqslant V} f(x_n) = \int_0^1 f(x)\, d\mu.$$

With this generalization in hand, it is useful to derive a variant of the Erdös–Turán inequality. To this end, suppose that the *Weyl limits*

$$c_m := \lim_{V \to \infty} \frac{1}{V} \sum_{n \leqslant V} e(mx_n),$$

exist for every integer m. A classical theorem of Schoenberg and Wiener (see [14]) states that the x_n's are equidistributed with respect to some positive continuous measure if and only all the Weyl limits exist and

$$\lim_{V \to \infty} \frac{1}{V} \sum_{|m| \leqslant V} |c_m|^2 = 0.$$

A simple application of the Cauchy–Schwarz inequality shows that this is equivalent to

$$\sum_{|m|\leqslant V} |c_m| = o(V).$$

In our context, we will suppose that

$$\sum_{m=-\infty}^{\infty} |c_m| < \infty.$$

Since the c_m's are bounded, this certainly implies the Wiener–Schoenberg condition. Our assumption allows us to write down an absolutely convergent Fourier series for the measure. Let

$$\mu = F(-x)\,dx,$$

where

$$F(x) = \sum_{m=-\infty}^{\infty} c_m e(mx).$$

We also define $\|\mu\|$ to be the supremum of $|F(x)|$ for $x \in [0,1]$.

We will prove this using the following variant of the Erdös–Turán inequality. Define

$$N_I(V) := \#\{n \leqslant V\colon\ x_n \in I\}.$$

Theorem 8. *With the c_m's defined as above, and $I = [a,b]$, set*

$$D_{I,V}(\mu) := \bigl|N_I(V) - V\mu(I)\bigr|.$$

Then,

$$D_{I,V}(\mu) \leqslant \frac{V\|\mu\|}{M+1} + \sum_{1\leqslant|m|\leqslant M}\left(\frac{1}{M+1} + \min\left(b-a,\, \frac{1}{\pi|m|}\right)\right)\left|\sum_{n=1}^{V} e(mx_n) - Vc_m\right|,$$

if V and M are natural numbers.

We will prove this theorem in Section 4. It follows the same line of proof as in [16] in the classical case and makes essential use of the Beurling–Selberg polynomials which we review in the next section. The reader may also consult [17].

3. The Beurling–Selberg polynomials

In this section, we will describe some tools provided by the theory of Fourier series and harmonic analysis, which will play an important role in proving Theorems 2 and 8. For convenience of the reader, we review the relevant facts about Fourier series that will be used later.

Let $f(x)$ be a function of a real variable that is bounded, measurable and periodic with period 1. For each $n \in \mathbb{Z}$, the nth Fourier coefficient of f is given by

$$\widehat{f}(n) = \int_0^1 f(x)e(-nx)\,dx, \quad \text{where } e(x) = e^{2\pi i x}.$$

When $f(x)$ is continuous and

$$\sum_{-\infty}^{\infty} \left|\widehat{f}(n)\right| < \infty,$$

then the function $f(x)$ is represented by the absolutely convergent Fourier series

$$f(x) = \sum_{n=-\infty}^{\infty} \widehat{f}(n)e(nx).$$

We now describe some trigonometric polynomials which give a good approximation for the characteristic function $\chi_I(x)$ of an interval $I = [a, b]$ contained in $[0, 1]$. For a positive integer M, we define $\Delta_M(x)$ to be Féjer's kernel, given as below:

$$\Delta_M(x) = \sum_{|n|<M} \left(1 - \frac{|n|}{M}\right)e(nx) = \frac{1}{M}\left(\frac{\sin \pi Mx}{\sin \pi x}\right)^2.$$

The *Mth order Beurling polynomial* is defined as follows:

$$B_M^*(x) = \frac{1}{M+1}\sum_{n=1}^{M}\left(\frac{n}{M+1} - \frac{1}{2}\right)\Delta_M\left(x - \frac{n}{M+1}\right) + \frac{1}{2\pi(M+1)}\sin\bigl(2\pi(M+1)x\bigr) - \frac{1}{2\pi}\Delta_{M+1}(x)\sin 2\pi x + \frac{1}{2(M+1)}\Delta_{M+1}(x).$$

For an interval $[a, b]$, we define the *Mth order Selberg polynomials* as:

$$S_M^+(x) = b - a + B_M^*(x - b) + B_M^*(a - x)$$

and

$$S_M^-(x) = b - a - B_M^*(b - x) - B_M^*(x - a).$$

Clearly, both the above polynomials are trigonometric polynomials of degree at most M. From the work of Vaaler [30], we also have the following facts:

(a) For a subinterval $I = [a, b]$ of $[0, 1]$,

$$S_M^-(x) \leqslant \chi_I(x) \leqslant S_M^+(x). \tag{2}$$

(b)

$$\int_0^1 S_M^+(x)\,dx = b - a + \frac{1}{M+1}$$

and

$$\int_0^1 S_M^-(x)\,dx = b - a - \frac{1}{M+1}.$$

(c)

$$\left\| S_M^+(x) - \chi_I(x) \right\|_{L^1} \leqslant \frac{1}{M+1}.$$

Thus, if $\widehat{S}_M^+(n)$ denotes the nth Fourier coefficient of $S_M^+(x)$, then

$$\left|\widehat{S}_M^+(n) - \widehat{\chi}_I(n)\right| \leqslant \left\| S_M^+(x) - \chi_I(x) \right\|_{L^1} \leqslant \frac{1}{M+1}.$$

The same property holds for Fourier coefficients of $S_M^-(x)$.

(d) For $n \neq 0$,

$$\widehat{\chi}_I(n) = \frac{e(na) - e(nb)}{2\pi i n}.$$

Thus, for non-zero n,

$$\left|\widehat{\chi}_I(n)\right| = \left|\frac{\sin \pi n(b-a)}{\pi n}\right| \leqslant \min\left(b-a, \frac{1}{\pi|n|}\right).$$

Combining this with the inequality in fact (c), we find that for $0 < |n| < M$,

$$\left|\widehat{S}_M^+(n)\right| \leqslant \frac{1}{M+1} + \min\left(b-a, \frac{1}{\pi|n|}\right).$$

Suppose now we have a sequence x_n of points lying in $[0,1]$. If

$$Z(r; a, b) = \#\{1 \leqslant n \leqslant r:\ x_n \in [a,b]\},$$

then clearly,

$$Z(r; a, b) = \sum_{n=1}^{r} \chi_I(x_n).$$

Thus, from the properties of Selberg polynomials described above, we see that

$$\sum_{n=1}^{r} S_M^-(x_n) \leqslant Z(r; a, b) \leqslant \sum_{n=1}^{r} S_M^+(x_n). \tag{3}$$

In what follows, we will denote

$$s_n = \widehat{S}_M^+(n) \quad \text{and} \quad t_n = \widehat{S}_M^-(n).$$

4. A variant of the Erdös–Turán inequality

We can now prove Theorem 8. Let χ_I be the characteristic function of the interval I. Then,

$$\sum_{n\leqslant V} S_M^-(x_n) \leqslant \sum_{n\leqslant V} \chi_I(x_n) \leqslant \sum_{n\leqslant V} S_M^+(x_n).$$

Now,

$$\sum_{n\leqslant V} S_M^{\pm}(x_n) = \sum_{|m|\leqslant M} \widehat{S}_M^{\pm}(m) \sum_{n\leqslant V} e(mx_n).$$

Subtracting the expected value of $c_m V$ from the inner exponential sum, we get

$$\sum_{n\leqslant V} S_M^{\pm}(x_n) - V \sum_{|m|\leqslant M} \widehat{S}_M^{\pm}(m)c_m = \sum_{|m|\leqslant M} \widehat{S}_M^{\pm}(m)\left(\sum_{n\leqslant V} e(mx_n) - Vc_m\right).$$

Noting that the inner sum on the right-hand side is zero for $m = 0$, we get upon putting absolute values,

$$\left|\sum_{n\leqslant V} S_M^{\pm}(x_n) - V \sum_{|m|\leqslant M} \widehat{S}_M^{\pm}(m)c_m\right| \leqslant \sum_{1\leqslant|m|\leqslant M} \left|\widehat{S}_M^{\pm}(m)\right|\left|\sum_{n\leqslant V} e(mx_n) - Vc_m\right|.$$

Let us consider the sum

$$\sum_{|m|\leqslant M} \widehat{S}_M^{\pm}(m)c_m.$$

Since $\widehat{S}_M^{\pm}(m) = 0$ for $|m| > M$, we extend the range of the sum to all $m \in \mathbb{Z}$. Then,

$$\sum_m \widehat{S}_M^{\pm}(m)c_m = \sum_m c_m \int_0^1 S_M^{\pm}(t)e(-mt)\,dt = \int_0^1 S_M^{\pm}(t)\,d\mu,$$

upon interchanging the sum and the integral. Since

$$\left|\int_0^1 \left(S_M^{\pm}(t) - \chi_I(t)\right) d\mu\right| \leqslant \frac{\|\mu\|}{M+1},$$

we obtain the desired result using the estimate for $\widehat{S}_M^{\pm}(m)$. This proves Theorem 8.

5. A generalized Koksma inequality

In this section, we give an interesting application of Theorem 8. When a sequence $x_1, x_2, \ldots$ is uniformly distributed mod 1, we have noted above that for any Riemann integrable function f,

$$\lim_{V\to\infty} \frac{1}{V} \sum_{n=1}^{V} f(x_n) = \int_0^1 f(t)\,dt.$$

It will be useful to have an effective version of this theorem. Indeed, such a theorem was derived by Koksma in 1950. He showed the following. Suppose that we are given a finite sequence of numbers $x_1, \ldots, x_V$ in $[0,1]$. Define the *discrepancy*

$$D_V = \sup_{I\subseteq[0,1]} \left| N_I(V) - \ell(I)V \right|,$$

where $\ell(I)$ denotes the length of I and the supremum is over all subintervals of $[0,1]$. Then, for any Riemann integrable function f of bounded variation $\delta(f)$, we have

$$\left| \sum_{n=1}^{V} f(x_n) - V \int_0^1 f(t)\,dt \right| \leqslant \delta(f) D_V.$$

The classical inequality of Erdös and Turán gives us an upper bound for the discrepancy. Consequently, one has the following effective result. For any function f of bounded variation $\delta(f)$, we have

$$\left| \sum_{n=1}^{V} f(x_n) - V \int_0^1 f(t)\,dt \right| \leqslant \delta(f) \left(\frac{V}{M+1} + \sum_{m=1}^{M} \frac{1}{m} \left| \sum_{n\leqslant V} e(mx_n) \right| \right),$$

invoking the improvement of [15].

One interesting consequence of Theorem 8 is its application to a generalized version of this classical result of Koksma. We have

Theorem 9. *Given a sequence of numbers $x_1, x_2, \ldots$ in $[0,1]$ which is μ-equidistributed, define the μ-discrepancy as*

$$D_V(\mu) = \sup_{I\subseteq[0,1]} \left| N_I(V) - \mu(I)V \right|.$$

Then, for any function f of bounded variation $\delta(f)$, we have

$$\left| \sum_{n=1}^{V} f(x_n) - V \int_0^1 f(t)\,d\mu \right| \leqslant \delta(f) D_V.$$

Consequently, this is bounded by

$$\leqslant \delta(f) \left(\frac{V\|\mu\|}{M+1} + \sum_{1\leqslant|m|\leqslant M} \left(\frac{1}{M+1} + \frac{1}{\pi m} \right) \left| \sum_{n=1}^{V} e(mx_n) - Vc_m \right| \right),$$

where the c_m's are the Weyl limits.

The proof of this follows the classical proof as given in [14]. Indeed, the relevant result on μ-discrepancy needed in the proof has been derived in Theorem 3.3 of [10] which states the following. Given any positive measure μ and a sequence of points $x_1, x_2, \dots, x_V$ in $[0,1]$, define $D_V(\mu)$ as above. Then, for any Riemann integrable function f of bounded variation $\delta(f)$ on $[0,1]$, we have

$$\left|\sum_{n=1}^{V} f(x_n) - V\int_0^1 f(t)\,d\mu\right| \leqslant \delta(f) D_V(\mu).$$

Theorem 9 follows immediately upon noting that $b-a \leqslant 1$ and injecting Theorem 8 to obtain a bound for $D_V(\mu)$.

6. Set equidistribution

It is convenient to have a mild variant of the notion of equidistribution of sequences. We will say that a sequence of finite multisets A_n with $\#A_n \to \infty$ is *set equidistributed* mod 1 with respect to a probability measure μ if for every continuous function f on $[0,1]$, we have

$$\lim_{n\to\infty} \frac{1}{\#A_n} \sum_{t\in A_n} f(t) = \int_0^1 f(x)\,d\mu.$$

If μ is the Lebesgue measure and $A_n = \{x_1, x_2, \dots, x_n\}$, this recovers the classical notion of uniform distribution mod 1. It is not difficult to show that the Wiener–Schoenberg theorem extends to this context. That is, the sequence $\{A_n\}$ is set equidistributed with respect to some positive continuous measure if and only if the Weyl limits

$$c_m := \lim_{n\to\infty} \frac{1}{\#A_n} \sum_{t\in A_n} e^{2\pi imt}$$

exist and

$$\sum_{m=1}^{N} |c_m|^2 = o(N).$$

Clearly, the discussion can be generalized to treat set equidistribution in an arbitrary interval. After suitable rescaling, the problem becomes equivalent to set equidistribution in $[0,1]$. In addition, the analogue of Theorem 8 translates without change, into the context of set-equidistribution.

In the setting discussed below, we will be considering the family of normalized eigenvalues of T_p acting on $S(N,k)$ and study their equidistribution. In later sections, we consider the eigenvalues of the Frobenius automorphism acting on a family of curves over a fixed finite field. Finally, we consider the eigenvalues of adjacency matrices of a sequence of regular graphs and study their equidistribution.

7. The Eichler–Selberg trace formula

To prove Theorem 2, a principal role is played by the Eichler–Selberg trace formula, which gives us a formula for the trace Tr of T_n acting on $S(N,k)$ in terms of class numbers of binary quadratic forms. In this section, we will follow the presentation of this formula in [25]. For a negative integer Δ congruent to 0 or 1 (mod 4), let $B(\Delta)$ be the set of all positive definite binary quadratic forms with discriminant Δ. That is,

$$B(\Delta) = \left\{ax^2 + bxy + cy^2\colon\ a,b,c \in \mathbb{Z},\ a > 0,\ b^2 - 4ac = \Delta\right\}.$$

By $b(\Delta)$, we denote the set of primitive forms

$$b(\Delta) = \{ f(x, y) \in B(\Delta) \colon \gcd(a, b, c) = 1 \}.$$

One can define a right action of the group $SL_2(\mathbb{Z})$ on $B(\Delta)$ as follows:

For $f(x, y) \in B(\Delta)$, let

$$f(x, y) \cdot \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} := f(\alpha x + \beta y, \gamma x + \delta y).$$

It is not difficult to show that this action respects the primitive forms. It is a well-known fact that this action has only finitely many orbits (See for example [1].) We define $h(\Delta)$ to be the number of orbits of $b(\Delta)$.

Let h_w be defined as follows:

$$h_w(-3) = 1/3,$$

$$h_w(-4) = 1/2,$$

$$h_w(\Delta) = h(\Delta) \quad \text{for } \Delta < -4.$$

Theorem 10 *(Eichler–Selberg Trace Formula). For every integer $n \geqslant 1$, the trace* Tr *of T_n acting on $S(N, k)$ is given by*

$$\operatorname{Tr} T_n = A_1(n) + A_2(n) + A_3(n) + A_4(n),$$

where $A_i(n)$'s are as follows:

$$A_1(n) = \begin{cases} n^{(k/2-1)} \cdot \frac{k-1}{12} \psi(N) & \text{if } n \text{ is a square}, \\ 0 & \text{otherwise}, \end{cases} \quad \text{where } \psi(N) = N \prod_{p|N} \left(1 + \frac{1}{p}\right); \tag{4}$$

$$A_2(n) = -\frac{1}{2} \sum_{t \in \mathbb{Z},\ t^2 < 4n} \frac{\varrho^{k-1} - \bar{\varrho}^{k-1}}{\varrho - \bar{\varrho}} \sum_f h_w\left(\frac{t^2 - 4n}{f^2}\right) \mu(t, f, n); \tag{5}$$

Here ϱ and $\bar{\varrho}$ are the zeroes of the polynomial $x^2 - tx + n$ and the inner sum runs over all positive divisors f of $t^2 - 4n$ such that $(t^2 - 4n)/f^2 \in \mathbb{Z}$ is congruent to 0 *or* 1 (mod 4)*. $\mu(t, f, n)$ is given by*

$$\mu(t, f, n) = \frac{\psi(N)}{\psi(\frac{N}{N_f})} M(t, n, NN_f),$$

where $N_f = \gcd(N, f)$ and $M(t, n, K)$ denotes the number of solutions of the congruence $x^2 - tx + n \equiv 0 \pmod{K}$;

$$A_3(n) = -\sum_{d|n, 0 < d \leqslant \sqrt{n}} d^{k-1} \sum_{c|N} \phi\left(\gcd\left(c, \frac{N}{c}\right)\right); \tag{6}$$

Here, ϕ denotes Euler's function and in the first summation, if there is a contribution from the term $d = \sqrt{n}$, it should be multiplied by $\frac{1}{2}$. In the inner sum, we also need the condition that $\gcd(c, N/c)$ *divides* $\gcd(N, n/d - d)$;

$$A_4(n) = \begin{cases} \sum_{t|n,\ t>0} t & \text{if } k = 2, \\ 0 & \text{otherwise}. \end{cases} \tag{7}$$

In his paper [26], Serre proves the following proposition:

Proposition 11. *If n is a square,*

$$\left| \operatorname{Tr} T_n - \frac{k-1}{12} n^{k/2-1} \psi(N) \right| \ll_n n^{k/2} N^{1/2} d(N),$$

where $d(N)$ is the number of positive divisors of N.

In order to refine Serre's equidistribution theorem, we would like to obtain precise estimates for the terms $A_i(n)$ in the Eichler–Selberg Trace Formula and make their dependence on n explicit.

To this end, we need the following lemma, due to Huxley [13].

Lemma 12. *Suppose a and b are integers such that $a^2 - 4b \neq 0$. Given K, let $M(a, b, K)$ be the number of solutions* mod K *of the congruence*

$$x^2 - ax + b \equiv 0 \bmod K.$$

Then,

$$M(a, b, K) \leqslant 2^{\nu(K)} \cdot \left|a^2 - 4b\right|^{\frac{1}{2}},$$

where $\nu(K)$ denotes the number of distinct prime divisors of K.

As in [25], specializing the Eichler–Selberg trace formula to the case $n = 1$ gives us a formula for the dimension of $S(N, k)$.

Theorem 13.

$$s(N,k) = \frac{k-1}{12}\psi(N) - \left(\frac{k-1}{3} - \left[\frac{k}{3}\right]\right)\delta_1(N) - \left(\frac{k-1}{4} - \left[\frac{k}{4}\right]\right)\delta_2(N) - \frac{1}{2}\sum_{c|N, c>0} \phi\big(\gcd(c, N/c)\big) + \delta_3(k),$$

where $\delta_1(N)$ and $\delta_2(N)$ are respectively the number of solutions of the congruences

$$x^2 + x + 1 \equiv 0 \ (\text{mod } N) \quad \text{and} \quad x^2 + 1 \equiv 0 \ (\text{mod } N),$$

$\delta_3(k) = 1$ if $k = 2$ and zero otherwise.

Observing that

$$\sum_{c|N} \phi\big(\gcd(c, N/c)\big) \geqslant 2^{\nu(N)},$$

and that

$$-\frac{1}{3} \leqslant \frac{k-1}{3} - \left[\frac{k}{3}\right] \leqslant \frac{2}{3}, \qquad -\frac{1}{4} \leqslant \frac{k-1}{4} - \left[\frac{k}{4}\right] \leqslant \frac{3}{4},$$

we easily deduce upon inserting Huxley's estimate into the case $n = 1$ of the above theorem, the following useful inequality.

Corollary 14.

$$s(N,k) \leqslant \frac{k-1}{12}\psi(N) + \left(\frac{2}{\sqrt{3}} + 1\right)2^{\nu(N)} + \delta_3(k).$$

For computational purposes, we will prove

Corollary 15. *For $N \geqslant 61$,*

$$\frac{3\psi(N)}{200} \leqslant s(N,2) \leqslant \frac{\psi(N)}{12} + 1.$$

Proof. In the case $k = 2$, it is easily seen that apart from the terms $\psi(N)/12$ and $\delta_3(2) = 1$, all of the other terms appearing in the formula for $s(N,2)$ are negative. Thus, the upper bound is clear. For the lower bound, we appeal to a result of Halberstadt and Kraus [11] where it is proved that the dimension $g_0^+(N)$, of the space of new forms of weight 2 and level N is at least $3\phi(N)/200$ for $N \geqslant 61$. Since

$$s(N,2) = \sum_{d|N} g_0^+(N/d)\sigma_0(d),$$

where $\sigma_0(n)$ is the number of divisors of n, we obtain

$$s(N,2) \geqslant \frac{3}{200}\sum_{d|N}\phi(N/d)\sigma_0(d).$$

As the sum on the right-hand side is multiplicative, we find that it is greater than $\psi(N)$ from which the stated result follows. □

8. Estimating the term A_2

We define the Hurwitz class number $H(n)$ as

$$H(n) = \sum_{f^2|n} h_w\big(-n/f^2\big).$$

We have the following classical result due to Hurwitz (see [4, p. 236]).

Lemma 16.

$$\sum_{t^2<4n} H\left(4n-t^2\right) = 2\sigma(n) - \lambda(n),$$

where

$$\lambda(n) = \sum_{d\mid n} \min(d, n/d),$$

and $\sigma(n)$ is the sum of the positive divisors of n.

Putting this estimate into the expression for A_2 and inserting Huxley's estimate for $\mu(t, f, n)$, we obtain as in [26],

$$|A_2| < 2\sigma(n)n^{(k-1)/2}2^{\nu(N)} \sup_{f^2<4n} \psi(f).$$

Now,

$$\psi(f) = f\prod_{p\mid f}\left(1+\frac{1}{p}\right).$$

There are various ways of estimating $\psi(f)$. The most trivial estimate is

$$\psi(f)/f \leqslant \exp\left(\sum_{p\leqslant\nu(f)}\frac{1}{p}\right) \leqslant \exp\left(\sum_{n\leqslant\nu(f)}\frac{1}{n}\right) \leqslant e\nu(f),$$

using the elementary inequality

$$\sum_{n\leqslant x}\frac{1}{n} \leqslant 1+\log x.$$

We also have the trivial bound $\nu(f) \leqslant \log f/\log 2$. This gives us a final estimate of

$$|A_2| \leqslant e2^{\nu(N)+2}n^{k/2}\sigma(n)\frac{\log 4n}{\log 2}. \tag{8}$$

For future refinements, we observe that several improvements can be made in this estimate. For instance, there is an effective constant B such that

$$\sum_{p\leqslant x}\frac{1}{p} < \log\log x + B,$$

so that this would give $e^B \log\nu(f)$ instead of $e\nu(f)$ in the above estimation. Furthermore, there is Ramanujan's bound

$$\nu(f) \leqslant \frac{C\log f}{\log\log f},$$

for some effectively computable C that can be utilized. This would give

$$|A_2| \ll 2^{\nu(N)}\sigma(n)n^{k/2}\log\log n,$$

where the implied constant is effectively computable.

We recall that T_n' is the normalized nth Hecke operator

$$T_n' = \frac{T_n}{n^{\frac{k-1}{2}}}.$$

Thus, for $m \geqslant 1$,

$$\operatorname{Tr} T'_{p^m} = B_1(m) + B_2(m) + B_3(m) + B_4(m),$$

where

$$B_i(m) = \frac{A_i(p^m)}{p^{m\frac{k-1}{2}}}, \quad 1 \leqslant i \leqslant 4.$$

Thus,

$$B_1(m) = \begin{cases} p^{\frac{-m}{2}} \cdot \frac{k-1}{12}\psi(N) & \text{if } m \text{ is even,} \\ 0 & \text{if } m \text{ is odd.} \end{cases} \tag{9}$$

Also, for every integer $m \geqslant 1$, we have

$$\sigma\left(p^m\right) = \frac{p^{m+1}-1}{p-1} \leqslant \frac{p^{m+1}}{p-1} \leqslant 2p^m,$$

so that

$$\left|B_2(m)\right| \leqslant \frac{8e}{\log 2} 2^{\nu(N)} p^{\frac{3m}{2}} \log 4p^m.$$

Let us also note for future reference

$$B_3(m) - B_3(m-2) \leqslant 2f(N),$$

where

$$f(N) = \sum_{c|N} \phi\left(\gcd(c, N/c)\right),$$

and $B_4(m) - B_4(m-2) = 0$ if $k \neq 2$ and $\leqslant 2p^{m/2}$ if $k = 2$. A crude estimate for $f(N)$ is $\sqrt{N}d(N)$ since

$$\gcd(c, N/c) \leqslant \sqrt{N},$$

for any $c|N$.

For $n \geqslant 0$, the nth Chebychev polynomial $X_n(x)$ is defined as follows:

$$X_n(x) = \frac{\sin(n+1)\theta}{\sin\theta}, \quad \text{where } x = 2\cos\theta.$$

The following lemma can be found in [26]:

Lemma 17. *Let p be a prime. Then, for $m \geqslant 0$,*

$$T'_{p^m} = X_m\bigl(T'_p\bigr).$$

Now, for $1 \leqslant i \leqslant r$, we write

$$\frac{a_{p,i}}{p^{\frac{k-1}{2}}} = 2\cos\theta_{p,i}$$

for the eigenvalues of T'_p. Thus, for $m = 1$,

$$\sum_{i=1}^{r} 2\cos\theta_{p,i} = \operatorname{Tr} T'_p.$$

Since

$$2\cos m\theta = X_m(2\cos\theta) - X_{m-2}(2\cos\theta), \quad m \geqslant 2,$$

we have for $m \geqslant 2$,

$$\sum_{i=1}^{r} 2\cos m\theta_i = \operatorname{Tr} T'_{p^m} - \operatorname{Tr} T'_{p^{m-2}}.$$

9. The measure μ_p

As before, we let $\theta_i \in [0, \pi]$ be such that

$$\cos\theta_i = \frac{a_{p,i}}{2p^{\frac{k-1}{2}}}.$$

We will consider the sequence $\pm\theta_i/2\pi$ $(1 \leqslant i \leqslant r)$ and study its equidistribution. Accordingly, let

$$c_m = \lim_{r\to\infty} \frac{1}{r} \sum_{i=1}^{r} 2\cos m\theta_i,$$

and define

$$\mu = F(-x)\,dx,$$

where

$$F(x) = \sum_{m=-\infty}^{\infty} c_m e(mx).$$

By our calculation in the previous section, we have $c_0 = 2$, $c_m = 0$ for m odd and for m even,

$$c_m = \frac{1}{p^{|m|/2}} - \frac{1}{p^{(|m|-2)/2}}.$$

Consequently, we need to determine

$$\sum_{m=-\infty}^{\infty} c_m e(mx).$$

We have

$$F(x) = 2 + 2\sum_{m=1}^{\infty} \left(\frac{1}{p^m} - \frac{1}{p^{m-1}}\right) \cos 4\pi mx.$$

This is easily summed as follows. For t, x real, with $|t| < 1$, we have

$$\sum_{m=0}^{\infty} t^m \cos mx = \operatorname{Re}\left(\sum_{m=0}^{\infty} t^m e(mx)\right) = \operatorname{Re}\left(\frac{1}{1-te(x)}\right) = \frac{1-t\cos x}{|1-te(x)|^2}.$$

Thus,

$$F(x) = 2(p+1)\frac{1-\cos 4\pi x}{p+1/p-2\cos 4\pi x} = 4(p+1)\frac{\sin^2 2\pi x}{(p^{1/2}+p^{-1/2})^2 - 4\cos^2 2\pi x}.$$

This determines a measure $F(x)\,dx$ on $[0,1]$ and is the distribution function for the numbers $x_i = \pm\theta_i/2\pi$. The measure giving the distribution of $\cos\theta_i$ is therefore

$$F\left(\frac{\cos^{-1} x}{2\pi}\right) d\left(\frac{\cos^{-1} x}{2\pi}\right) = \frac{2(p+1)}{\pi} \frac{\sqrt{1-x^2}}{(p^{1/2}+p^{-1/2})^2 - 4x^2}\,dx.$$

Thus, the distribution of the numbers $2\cos\theta_i$ is given by μ_p, after an easy change of variable.

From the discussion in the previous section, we now have

Theorem 18. *The Weyl limits c_m are given by $c_0 = 1$ and for $m \geqslant 1$,*

$$c_m = \begin{cases} p^{-m/2} - p^{-(m-2)/2} & \text{if } m \text{ is even}, \\ 0 & \text{if } m \text{ is odd}. \end{cases}$$

Moreover,

$$\left|\sum_{i=1}^{r} 2\cos m\theta_i - c_m r\right| \leqslant 4p^m 2^{\nu(N)} \sup_{f^2<4p^m} \psi(f) + 2f(N) + \delta_m(k), \tag{10}$$

where $\delta_m(k) = 0$ unless $k = 2$ in which case it is equal to $2p^{m/2}$.

Proof. The sum in question is

$$\mathrm{Tr}\, T'_{p^m} - \mathrm{Tr}\, T'_{p^{m-2}}$$

and the result is immediate from the discussion of the previous sections. □

Let us observe that the upper bound is

$$\ll p^{3m/2} 2^{\nu(N)} \log p^m + \sqrt{N} d(N). \tag{11}$$

There is a slightly different way of estimating A_2 that will be useful below in getting explicit constants. Let us consider the term $\mu(t, f, n)$ occurring in the trace formula. This term is easily seen to be

$$\leqslant \psi(N_f) M(t, n, NN_f).$$

Since

$$\psi(N_f) = N_f \prod_{p|N_f}\left(1 + \frac{1}{p}\right) \leqslant N_f \prod_{p|N}\left(1 + \frac{1}{p}\right) \leqslant 2^{\nu(N)} N_f.$$

As $N_f \leqslant f$, we deduce

$$A_2(n) \leqslant 4n^{k/2} \sigma(n) 4^{\nu(N)} \tag{12}$$

which implies

$$B_2(m) \leqslant 8p^{3m/2} 4^{\nu(N)}. \tag{13}$$

This means that (10) can be replaced by

$$16p^{3m/2} 4^{\nu(N)} + 2f(N) + \delta_m(k). \tag{14}$$

10. Effective version of Serre's theorem

In earlier sections, we described the tools necessary to obtain an effective version of Theorem 1. In what follows, we let $r = s(N, k)$. Let $[\alpha, \beta]$ be contained in the interval $[-1, 1]$. For a fixed prime p not dividing N, we want to estimate

$$\#\left\{1 \leqslant i \leqslant r\colon\ \frac{a_{p,i}}{2p^{\frac{k-1}{2}}} \in [\alpha, \beta]\right\}.$$

We let $\theta_i \in [0, \pi]$ be such that

$$\cos\theta_i = \frac{a_{p,i}}{2p^{\frac{k-1}{2}}}.$$

We choose a subinterval $I' = [\varphi_\beta, \varphi_\alpha]$ of $[0, \pi]$ such that if $\theta_i \in I'$, then

$$\cos\theta_i = \frac{a_{p,i}}{2p^{\frac{k-1}{2}}} \in [\alpha, \beta],$$

and conversely. Let

$$I_1 = \left[\frac{\varphi_\beta}{2\pi}, \frac{\varphi_\alpha}{2\pi}\right] \subseteq [0, 1/2].$$

Let $S^{\pm}_{M,1}(x)$ be the majorant and minorant Selberg polynomials for this interval. Now consider the interval

$$I_2 = \left[1 - \frac{\varphi_\alpha}{2\pi}, 1 - \frac{\varphi_\beta}{2\pi}\right] \subseteq [1/2, 1].$$

Let $S^{\pm}_{M,2}(x)$ denote the majorant and minorant Selberg polynomials for I_2. We consider the sequence $\pm\theta_i/2\pi$, $1 \leqslant i \leqslant r$ (modulo 1) and study its equidistribution in the unit interval. Since $\theta_i/2\pi \in I_1$ if and only if $-\theta_i/2\pi \in I_2$, we see that

$$\sum_{i=1}^{r} S^{-}_{M,1}(\pm\theta_i/\pi) \leqslant \#\{1 \leqslant i \leqslant r\colon\ \cos\theta_i \in [\alpha, \beta]\} \leqslant \sum_{i=1}^{r} S^{+}_{M,1}(\pm\theta_i/\pi)$$

and

$$\sum_{i=1}^{r} S^{-}_{M,2}(\pm\theta_i/\pi) \leqslant \#\{1 \leqslant i \leqslant r\colon\ \cos\theta_i \in [\alpha, \beta]\} \leqslant \sum_{i=1}^{r} S^{+}_{M,2}(\pm\theta_i/\pi).$$

Adding these two inequalities and denoting by c_m the limit

$$\lim_{r\to\infty} \frac{1}{r} \sum_{i=1}^{r} 2\cos m\theta_i,$$

we find upon using the estimates for $\widehat{S}^{\pm}_{M,i}(m)$ for $i = 1, 2$,

$$\left|N_I(r) - r\mu_p(I)\right| \leqslant \frac{r\|\mu_p\|}{M+1} + \sum_{1\leqslant|m|\leqslant M} \left(\frac{1}{M+1} + \min\left(\beta - \alpha, \frac{1}{\pi|m|}\right)\right) \left|\sum_{i=1}^{r} 2\cos m\theta_i - c_m r\right|,$$

where

$$N_I(r) = \#\{1 \leqslant i \leqslant r\colon\ \cos\theta_i \in [\alpha, \beta]\}.$$

We need to calculate the Weyl limits c_m and estimate

$$\sum_{i=1}^{r} 2\cos m\theta_i - c_m r.$$

But this is the content of Theorem 18.

We insert this estimate into Theorem 8 to obtain Theorem 2. Indeed, for the quantity in question, we get an upper bound using (11) of

$$\ll \frac{r}{M+1} + \left(p^{3M/2} 2^{\nu(N)} M \log p + d(N)\sqrt{N}\right) \log M.$$

Choosing $M = [c(\log kN)/\log p]$ for a sufficiently small constant c, we obtain Theorem 2.

For computational purposes, it may be convenient to have a sharper version of Theorem 2 with explicit constants.

We are now ready to prove the following theorem:

Theorem 19. *Let p be coprime to N. For an interval $[\alpha, \beta]$ contained in $[-1, 1]$, and any positive integer M,*

$$\left| \#\left\{1 \leqslant i \leqslant r\colon \frac{a_{p,i}}{2p^{\frac{k-1}{2}}} \in [\alpha, \beta]\right\} - \frac{k-1}{12}\psi(N)\frac{2(p+1)}{\pi} \int_{\alpha}^{\beta} \frac{\sqrt{1-x^2}}{(\sqrt{p} + \frac{1}{\sqrt{p}})^2 - 4x^2}\, dx \right|$$
$$\leqslant \frac{r}{M+1} + 4p^M 2^{\nu(N)} \sup_{f^2 < 4p^M} \psi(f) + 2f(N) + \delta_M(k),$$

where $\delta_M(k) = 0$ unless $k = 2$ in which case it is equal to $2p^{M/2}$.

Proof. This is immediate from the previous discussion. □

Remark 20. From the above equation, we can derive a new proof of Theorem 1. Dividing both sides of the equation by

$$\frac{k-1}{12}\psi(N),$$

we notice that the second error term goes to 0 as $N + k \to \infty$. Moreover, this equation is true for any positive integer M. Thus, as $M \to \infty$, the first error term tends to 0 and we retrieve Theorem 1 after appropriate changes of variables.

Since the above equation is true for any positive integer M, we now choose M such that

$$M + 1 = \left\lceil \frac{\frac{1}{a}\log k + \frac{1}{a}\log N}{\frac{3}{2}\log p} \right\rceil,$$

for any $a > 3$ of our choice. This proves Theorem 2.

Applying Theorem 9, the same argument gives

Theorem 21. *Let the notation be as in the previous theorem. For any function $f : [-2, 2] \to \mathbb{R}$ of bounded variation $\delta(f)$, we have*

$$\sum_{i=1}^{r} f\left(a_{p,i}/p^{(k-1)/2}\right) = s(N,k)\mu(f) + O\left(\delta(f)\frac{s(N,k)\log p}{\log kN}\right),$$

where the implied constant is absolute and effectively computable.

11. Hecke eigenvalues equal to a fixed value

When $\alpha = \beta$, we deduce

Theorem 22. *For a fixed α, the number of $i \leqslant r$ for which $\theta_i = \alpha$ is bounded by*

$$\frac{r}{M+1} + 4p^M 2^{\nu(N)} \sup_{f^2<4p^M} \psi(f) + 2f(N) + \delta_M(k),$$

for any positive integer value of M.

There are several corollaries one may deduce from this result. The first concerns the multiplicity of any given eigenvalue.

Corollary 23. *The multiplicity of any given eigenvalue is*

$$\ll \frac{s(N,k)\log p}{\log kN}.$$

Proof. This is immediate upon setting $M = c(\log kN)/\log p$, for a sufficiently small constant, in the previous theorem. □

If we use (14) in our derivation of Theorem 22, we get the bound

$$\frac{r}{M+1} + 16p^{3M/2}4^{\nu(N)} + 2f(N) + \delta_M(k).$$

Since $f(N) \leqslant \sqrt{N}d(N)$ and $\delta_M(k) \leqslant 2p^{M/2}$, this simplifies to

$$\frac{r}{M+1} + 17p^{3M/2}4^{\nu(N)} + 2\sqrt{N}d(N). \tag{15}$$

For computational purposes, it may be convenient to leave (15) in this form. On the other hand, it may also be useful to choose an optimal value of M to minimize the right-hand side, giving explicit constants. Both viewpoints will be useful as will be seen in the next two sections.

12. The prime level case

With a view to applications in the study of factorization of $J_0(N)$ as a product of $\mathbb{Q}$-simple abelian varieties, we study in this section the case $k = 2$ and N prime. We derive sharper estimates in this case. In the next section, we obtain similar results in the prime power case.

The following is easily deduced from Theorem 13.

Lemma 24. *If N is prime, then*

$$\frac{N}{12} - \frac{1}{2} \leqslant s(N,2) \leqslant \frac{N+1}{12}.$$

We also have the following refined estimates for the terms appearing in the Selberg trace formula:

Lemma 25. *If N is prime and $4p^m < N$, then $|A_2(p^m)| \leqslant 2\sigma(p^m)$. We also have $|B_3(m) - B_3(m-2)| \leqslant 2$ and $|B_4(m) - B_4(m-2)| \leqslant 2p^{m/2}$. Consequently, for $4p^m < N$, we have*

$$\left|\sum_{i=1}^{r} 2\cos m\theta_i - c_m r\right| \leqslant 10p^{m/2} + 2.$$

Proof. If $4p^m < N$, then all of the terms appearing in the sum defining $A_2(p^m)$ are less than N so that $N_f = 1$. Consequently, $\mu(t, f, p^m)$ is at most 2. Using Lemma 16, we obtain $|A_2(p^m)| \leqslant 2\sigma(p^m)$. The other two estimates involving B_3 and B_4 are equally immediate. Finally, we use the estimate

$$\sigma(p^m) = \frac{p^{m+1} - 1}{p - 1} \leqslant 2p^m,$$

to deduce the final estimate. $\square$

This allows us to deduce the following refinement of Theorem 22 in the case of $k = 2$ and prime level.

Theorem 26. *Let $k = 2$ and N be prime. For a fixed α, the number of $i \leqslant r$ for which $\theta_i = \alpha$ is bounded by*

$$\frac{r}{M+1} + 20p^{M/2} + 4$$

provided $4p^M < N$.

13. The prime power case

If N is a prime power, we can refine (14), so that the number of $i \leqslant r$ for which $\theta_i = \alpha$ is bounded by

$$\frac{r}{M+1} + 68p^{3M/2} + 2f(N).$$

If N is a prime power, it is easy to see that $f(N) \leqslant 2\sqrt{N}$. Thus, we obtain

$$\frac{r}{M+1} + 68p^{3M/2} + 4\sqrt{N}, \tag{16}$$

in the case that N is a prime power. This refinement will be useful in our study of factorizations of $J_0(N)$.

14. Explicit estimates and refinements

We now derive explicit estimates for the general weight k and level N. To this end, it will be useful to have the following lemmas in our discussion below.

Lemma 27. *For any $\alpha > 0$,*

$$\log x \leqslant \frac{x^\alpha}{\alpha e},$$

for $x \geqslant 1$.

Proof. The function

$$f(x) = \frac{\log x}{x^\alpha}$$

has derivative

$$\frac{x^{\alpha-1}(1-\alpha\log x)}{x^{2\alpha}}$$

which is negative if $x > e^{1/\alpha}$ and positive for $x < e^{1/\alpha}$. Thus, the function has a maximum at $x = e^{1/\alpha}$ and the result is now immediate. □

Lemma 28. *For any $\epsilon > 0$, the number of divisors $d(N)$ of N satisfies*

$$d(N) \leqslant C(\epsilon)N^\epsilon,$$

where

$$C(\epsilon) = \prod_{p<2^{1/\epsilon}} \left(1 + \frac{1}{\epsilon \log p}\right).$$

Proof. Writing $N = \prod_{p|N} p^\alpha$ we have

$$d(N)/N^\epsilon = \prod_{p|N} (\alpha+1)/p^{\alpha\epsilon}.$$

We break the product into two parts. The first part is over those p's for which $p < 2^{1/\epsilon}$ and the second part is over the complementary primes. In the second part, $p^\epsilon \geqslant 2$ so that $p^{\alpha\epsilon} \geqslant 2^\alpha$ and

$$\frac{\alpha+1}{p^{\alpha\epsilon}} \leqslant \frac{\alpha+1}{2^\alpha} \leqslant 1.$$

In the first part,

$$\frac{\alpha+1}{p^{\alpha\epsilon}} \leqslant 1 + \frac{\alpha}{p^{\alpha\epsilon}} \leqslant 1 + \frac{1}{\epsilon\log p}$$

since

$$\alpha\epsilon\log p \leqslant e^{\alpha\epsilon\log p} = p^{\alpha\epsilon}.$$

This completes the proof. □

In his classic paper on highly composite numbers, Ramanujan [21] gave the following bounds:

$$d(N) \leqslant \sqrt{3N}, \qquad d(N) \leqslant 8(3N/35)^{1/3}, \qquad d(N) \leqslant 96(3N/50050)^{1/4}$$

valid for all values of N. Nicolas and Robin [19] have shown that

$$d(N) \leqslant C^{\log N/\log\log N}$$

with $C = 2^{1.6}$. In particular, this implies

$$\nu(N) \leqslant \frac{\log N}{5\log 2} \quad \text{for } N \geqslant e^{1024}, \tag{17}$$

an estimate that will be useful below. If we use Ramanujan's second bound with exponent 1/3 and make crude estimates, it is easily seen that

$$2N^{1/2}d(N) \leqslant 48\frac{kN}{\log kN},$$

for all values of N.

Now let us consider (15) and the second term in it. Choosing $M = [(\log kN)/3\log p]$ and (17), we get that the second term is bounded by

$$9(kN)^{7/10}.$$

Now using Lemma 27, we see that this is bounded by

$$\frac{15kN}{\log kN}.$$

Putting everything together, we obtain

Theorem 29. *For a fixed α, the number of $i \leqslant r$ for which $\theta_i = \alpha$ is bounded by*

$$\frac{3s(N,k)}{\log kN} + 63\frac{kN}{\log kN},$$

provided $N \geqslant e^{1024}$.

We remark that these are very crude estimates and that finer estimates can be easily obtained with more care. Also, in certain cases, the estimates become substantially smaller. For example, the case when N is prime, leads to improved bounds as does the case when N is squarefree. For instance, in the latter case, the third term in (15) can be replaced by $2^{\nu(N)+1}$ since $f(N) = 2^{\nu(N)}$ in this case. Moreover, when $k = 2$, which is a case of special interest, further simplifications can be made.

15. Hecke eigenvalues of bounded degree

With the help of the results of the previous section, one may estimate for any $d \geqslant 1$, the number of eigenvalues $a_{p,i}$'s which are algebraic integers of degree d. We do so by first recording the following observation:

Proposition 30. *For a positive integer d, and a real number $M > 0$, the number of algebraic integers α of degree d and $H(\alpha) \leqslant M$ is at most*

$$C(d, M) := d\prod_{i=1}^{d}\left(2\binom{d}{i}M^i + 1\right),$$

where $H(\alpha)$ is the maximum of the absolute values of all conjugates of α.

Proof. Since α is an algebraic integer of degree d such that all its conjugates have absolute value less than or equal to M, the characteristic polynomial of α is of degree d and its coefficients are among a restricted set of integers. More precisely, if

$$f(x) = x^d + b_1 x^{d-1} + b_2 x^{d-2} + \cdots + b_d, \quad b_i \in \mathbb{Z},$$

is the minimal polynomial of α and $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$, say, are the conjugates of α, then by comparing the coefficients of

$$x^d + b_1 x^{d-1} + b_2 x^{d-2} + \cdots + b_d$$

and

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d),$$

and using the upper bound for the conjugates of α, we deduce that for every $1 \leqslant i \leqslant d$,

$$|b_i| \leqslant \binom{d}{i} M^i.$$

Since b_i is an integer, the number of possible values that b_i can take is

$$2\binom{d}{i} M^i + 1.$$

Thus, the characteristic polynomial of α is one among

$$\prod_{i=1}^{d} \left(2\binom{d}{i} M^i + 1\right)$$

possible polynomials. Therefore, the number of possible values that α can take under the given restrictions is less than or equal to

$$d \prod_{i=1}^{d} \left(2\binom{d}{i} M^i + 1\right). \qquad \square$$

For every $1 \leqslant i \leqslant r$, let $K_{p,i} = \mathbb{Q}(a_{p,i})$. Let $\alpha = a_{p,i}$ for some i such that $[K_{p,i} : \mathbb{Q}] = d$ where $d \geqslant 1$. Then, the conjugates α^ω of α are such that

$$\left|\alpha^\omega\right| \leqslant 2p^{\frac{k-1}{2}}.$$

Thus, taking

$$M = 2p^{\frac{k-1}{2}}$$

in Proposition 30, we deduce that $a_{p,i}$ can take at most l values, where

$$l = d \prod_{i=1}^{d} \left(2\binom{d}{i} \left(2p^{\frac{k-1}{2}}\right)^i + 1\right).$$

By combining the above information with Theorem 4, we deduce Theorem 5.

We now define

$$K_i := \mathbb{Q}\big(\{a_{n,i}\}_{(n,N)=1}\big).$$

K_i is a finite extension of $\mathbb{Q}$. For every $d \geqslant 1$, we define

$$s(N,k)_d := \#\big\{1 \leqslant i \leqslant r\colon\ [K_i : \mathbb{Q}] = d\big\}.$$

In Theorem 5 of [26], Serre shows that for every $d \geqslant 1$,

$$s(N,k)_d = \mathrm{o}\big(s(N,k)\big) \quad \text{as } N + k \to \infty.$$

For a fixed prime p not dividing N, if we let

$$s(N,k,p)_d = \#\big\{1 \leqslant i \leqslant r\colon\ \big[\mathbb{Q}\big(a_p(f_i)\big) : \mathbb{Q}\big] \leqslant d\big\},$$

then, clearly

$$s(N,k)_d \leqslant s(N,k,p)_d.$$

From the previous theorems, we can derive an upper bound for $s(N,k,p)_d$. The estimate for $s(N,k,p)_d$ has a factor of $p^{K_d} \log p$ in the numerator, where K_d is a positive integer depending on d. Thus, we can derive a non-trivial upper bound for $s(N,k)_d$ if we can find a sufficiently small prime p which does not divide N. How small is sufficiently small?

For N odd, we can choose $p = 2$ and deduce that for every $d \geqslant 1$,

$$s(N,k)_d \leqslant s(N,k,2)_d \leqslant d^2 \prod_{i=1}^{d} \left(2\binom{d}{i}\big(2^{\frac{k+1}{2}}\big)^i + 1\right)\left(3s(N,k)\frac{\log 2}{\log kN} + \frac{63kN}{\log kN}\right),$$

provided $N \geqslant e^{1024}$.

16. Dimensions of simple $\mathbb{Q}$-factors of $J_0(N)$

The results of the previous section have applications to the following question:

Let $J_0(N)$ be the Jacobian of the modular curve $X_0(N)$. Then, by the work of Shimura and Ribet (see [22]), $J_0(N)$ is $\mathbb{Q}$-isogenous to a product of $\mathbb{Q}$-simple abelian subvarieties,

$$J_0(N) \sim \prod_j A_j,$$

where, for every j, $E_j = \mathbb{Q} \otimes \mathrm{End}_{\mathbb{Q}}(A_j)$, and $[E_j : \mathbb{Q}] = \dim A_j$. From the work cited above, we note the following property:

Remark 31. The number of A_j's of dimension d is equal to $\frac{s(N,2)_d}{d}$.

As noted by Serre in [26], his equidistribution theory implies that there are finitely many values of N such that $J_0(N)$ is isogenous to a product of $\mathbb{Q}$-simple abelian varieties of bounded dimension. Our results lead to an immediate effective determination for every value of d. Indeed, in such a case, we have $s(N,2) = s(N,2)_d$ and for N odd, we obtain the inequality

$$s(N,2) \leqslant dC(d,2\sqrt{2})\left(3s(N,2)\frac{\log 2}{\log 2N} + \frac{126N}{\log 2N}\right)$$

from which an effective determination of N is easily obtained. One can extend this result when N is even also. This is done as follows.

We follow the reasoning on p. 89 of [26]. By the above calculation, we have shown that there is an effectively computable constant $C > 2$ such that if $p^* > C$ is prime, then $J_0(p^*)$ has a simple factor of dimension $> d$. Let p^* be the smallest prime $> C$. By Bertrand's postulate, $C < p^* < 2C$. Now let us consider $J_0(N)$. If $p^*|N$, then as $S(N,2)$ contains $S(p^*,2)$ and as this inclusion does not change the fields K_i, we see that $J_0(N)$ has a simple factor of dimension $> d$. If p^* is coprime to N, then by virtue of $p^* < 2C$, we can use the bound derived earlier to deduce that there is an effective bound for all N in general. This gives an effective bound in all cases. This proves Theorem 6.

Since we have been careful to be effective at every stage, we can write down an explicit (albeit humongous) estimate in the following way. Suppose that $J_0(N)$ decomposes as a product of $\mathbb{Q}$-simple abelian varieties of dimension at most d. We will bound all of the prime powers that can divide such an N. From estimate (16), we get

$$r \leqslant C(d,2\sqrt{3})\left(\frac{r}{M+1} + (68)3^{3M/2} + 4\sqrt{N}\right),$$

for any choice of M. Choosing $M+1 = 2C(d,2\sqrt{3})$, we get

$$\frac{r}{2} \leqslant C(d,2\sqrt{3})\big((68)3^{3C(d,2\sqrt{3})} + 4\sqrt{N}\big).$$

From Corollary 15, we know that $r \geqslant \frac{3N}{200}$, so that

$$\frac{3N}{400} - 4C(d,2\sqrt{3})\sqrt{N} \leqslant 68C(d,2\sqrt{3})3^{C(d,2\sqrt{3})}.$$

If

$$\frac{3\sqrt{N}}{400} - 4C(d,2\sqrt{3}) \geqslant C(d,2\sqrt{3}),$$

we obtain the bound

$$N \leqslant (68)^2 3^{6C(d,2\sqrt{3})}.$$

In other words, this proves

Theorem 32. *If $J_0(N)$ is isogenous over $\mathbb{Q}$ to a product of $\mathbb{Q}$-simple abelian varieties, then any prime power dividing N is bounded by*

$$\max\left((68)^2 3^{6C(d,2\sqrt{3})}, \frac{10^5}{9}C(d,2\sqrt{3})^2\right).$$

In the special case $d = 1$, the complete effective determination of N can be found in [5,32].

We now indicate how these ideas lead to the proof of Corollary 7. First suppose that N is odd. Let t be the largest dimension of the $\mathbb{Q}$-simple factor of $J_0(N)$. Then,

$$s(N,2) \leqslant \sum_{d\leqslant t} dC(d,2\sqrt{2})\left(s(N,2)\frac{\log 2}{\log 2N} + \frac{126N}{\log 2N}\right).$$

An easy estimation using Stirling's formula leads one to

$$\log 2N \ll C^{t^2},$$

for some constant $C > 0$. Thus, $t \gg \sqrt{\log\log N}$. This completes the proof in the case of N odd. For the general case, we write $N = 2^a N_0$, with N_0 odd. If $N_0 \gg N^\epsilon$ for some $\epsilon > 0$, then, as $J_0(N_0)$ is a subvariety of $J_0(N)$, we again deduce the result from the previous argument. If $N_0 \leqslant N^\epsilon$, then $2^a \gg N^{1-\epsilon}$. Letting t be the largest dimension of the $\mathbb{Q}$-simple factor of $J_0(2^a)$, we obtain as before

$$s\big(2^a, 2\big) \leqslant \sum_{d \leqslant t} dC(d, 2\sqrt{3})\left(s\big(2^a, 2\big)\frac{\log 3}{\log 2^{a+1}} + 126\frac{2^{a+1}}{\log 2^{a+1}}\right)$$

and arguing as before, we deduce the result.

Let us now consider the problem of determining all the prime values N for which $J_0(N)$ is isogenous to a product of elliptic curves defined over $\mathbb{Q}$. We can get sharper results if we proceed differently. For example, if we apply Theorem 26 with N an odd prime, $M = 6$, $p = 2$, we find using the lemmas and theorems of Section 12 that $N \leqslant 59081$.

A crude (but similar) estimation yields that if $J_0(N)$ is isogenous to a product of $\mathbb{Q}$-simple abelian varieties of dimension at most 2 and N is prime, then

$$N \leqslant 2^{215} 3(409) + 97.$$

17. Curves over finite fields

Let C be a curve of positive genus over the finite field $\mathbb{F}_q$ of q elements. As in [26], we denote by $g = g(C)$ the genus of C and $n(C, q^m)$ the number of points of C over $\mathbb{F}_{q^m}$. We have

$$n\big(C, q^m\big) = q^m + 1 - \sum_{i=1}^{g} \pi_i^m + \overline{\pi}_i^m,$$

where $\pi_1, \overline{\pi_1}, \ldots, \pi_g, \overline{\pi}_g$ are the eigenvalues of the Frobenius endomorphism acting on C. We set

$$x_i(C) = q^{-1/2}(\pi_i + \overline{\pi}_i), \quad i = 1, \ldots, g.$$

By a classical result of Weil, the x_i's belong to $\Omega = [-2, 2]$. We define $\theta_i(C) \in [0, \pi]$ by $x_i(C) = 2\cos\theta_i(C)$.

Now let C_r with $r = 1, 2, \ldots$, be a family of curves of genus g_r. We are interested in the distribution of the points $x_i(C_r)$, $i = 1, 2, \ldots, g_r$, as $r \to \infty$. This is equivalent to the study of the distribution of $\pm\theta_i(C_r)/2\pi \pmod 1$. By our earlier discussion, we must consider the sums

$$\sum_{i=1}^{g_r} 2\cos m\theta_i.$$

Thus, if the Weyl limits

$$c_m := \lim_{r\to\infty} \frac{1}{g_r} \sum_{i=1}^{r} 2\cos m\theta_i(C_r) \tag{18}$$

exist, and

$$\sum_m |c_m| < \infty, \tag{19}$$

then there is a measure μ with respect to which the $x_i(C_r)'s$ are equidistributed in Ω. Conversely, if these numbers are equidistributed with respect to some measure, then the above Weyl limits exist.

Actually, in this context, one has a sharper theorem. The second condition (19) is unnecessary. Indeed, in [26], it is shown that if $f(x)$ is a non-negative function, bounded and even on $[-1,1]$, and its Fourier coefficients c_m are $\leqslant 0$ for $m \neq 0$, then its Fourier series is absolutely convergent. In fact,

$$\sum_{m\neq 0} |c_m| \leqslant 1.$$

Serre deduces this via a clever use of the Féjer kernel. Applying this to our context, we see that

$$c_m = -\lim_{r\to\infty} \frac{n(C_r, q^m)}{g_r} \leqslant 0.$$

Thus, rewriting Proposition 5 and Theorem 8 of [26] with our refinements, we have

Theorem 33. *Assume that the limits* (18) *exist. Then,*

$$\sum_{m=1}^{\infty} \frac{c_m}{q^{m/2}} \leqslant 1.$$

Setting

$$F(x) = 1 - \sum_{m=1}^{\infty} \frac{c_m}{q^{m/2}} \cos mx,$$

and $\mu = \pi^{-1} F(x)\,dx$, *we have for any* $[\alpha, \beta] \subseteq [-2, 2]$,

$$\left| \#\{1 \leqslant i \leqslant g_r \colon x_i \in [\alpha, \beta]\} - g_r \int_\alpha^\beta \mu \right| \leqslant \frac{g_r \|\mu\|}{M+1} + 2 \sum_{1\leqslant m\leqslant M} \left(\frac{1}{M+1} + \min\left(b-a, \frac{1}{\pi m}\right)\right) \left| \sum_{i=1}^{g_r} e\big(m\theta_i(C_r)\big) - c_m g_r \right|.$$

In the case of $J_0(N)$ over $\mathbb{F}_p$, we have a family of curves whose genus $s(N,2)$ tends to infinity as N tends to infinity. The previous sections imply that there is a measure ν_p such that the angles of Frobenius are equidistributed with respect to this measure. Indeed, a direct calculation of the limits leads to an immediate determination of the measure, which (not surprisingly) turns out to be μ_p (defined earlier) so that we have for N coprime to p, the following estimate:

$$\left| \#\{1 \leqslant i \leqslant s(N,2)\colon\ x_i \in [\alpha, \beta]\} - s(N,2) \int_\alpha^\beta \mu_p \right| \ll \frac{s(N,2)\log p}{\log N},$$

where the implied constant is absolute and effectively computable.

18. The case of regular graphs

As in Serre [26], a graph X is a pair (V, E) with V consisting of vertices and E a set of "arrows" together with two maps: the "origin" map $\mathrm{o}: E \to V$ and the "inverse" map $E \to E$ given by $y \mapsto \bar{y}$. Thus, if we think of edges as ordered pairs of vertices and $y = (a, b)$ then $\mathrm{o}(y) = a$ and $\bar{y} = (b, a)$. We also define the "tail" of y, denoted $t(y) = \mathrm{o}(\bar{y})$. We say X is *regular* of degree k if $\forall v \in V$, the set of edges with origin v has size k. For suggestive reasons, we will write $k = q + 1$.

If m is a positive integer, a *walk* of length m is a sequence

$$\underline{y} = (y_1, \dots, y_m)$$

consisting of m edges $y_i \in E$ satisfying $t(y_i) = \mathrm{o}(y_{i+1})$ for $1 \leqslant i < m$. We define $\mathrm{o}(\underline{y}) = \mathrm{o}(y_1)$ and $t(\underline{y}) = t(y_m)$. A walk is *closed* if $\mathrm{o}(\underline{y}) = t(\underline{y})$. A walk is said to be *without backtracking* if $y_{i+1} \neq \overline{y_i}$ for $1 \leqslant i < m$. A closed walk is called a *circuit* if it is without backtracking and $y_m \neq \overline{y_1}$. In other words, $y_{i+1} \neq \overline{y_i}$ for all i modulo m.

If f_m is the number of closed walks of length m which are without backtracking, then it is not difficult to see that

$$f_m - C_m = \sum_{1 \leqslant i < m/2} (q-1) q^{i-1} C_{m-2i}. \tag{20}$$

Indeed, if $\underline{y} = (y_1, \dots, y_m)$ is a closed walk without backtracking, and this is not a circuit, then it must be of the form $y_1 \underline{z} \bar{y}_1$ where $z = (y_2, \dots, y_{m-1})$ is a closed walk without backtracking of length $m-2$. For a fixed $\underline{z}$, there are $q-1$ choices for y_1 if $\underline{z}$ is a circuit and q choices if $\underline{z}$ is not a circuit. Thus, we have the recursion

$$f_m - C_m = (q-1) C_{m-2} + q(f_{m-2} - C_{m-2}).$$

Iteration gives (20).

Now let X be as above, a regular graph of degree $q+1$. We let C_X be the group of 0-chains of X. That is, C_X is the $\mathbb{Z}$-module of functions on V with values in $\mathbb{Z}$. If $x \in V$, let δ_x be the function given by $\delta_x(u) = 1$ if $u = x$ and 0 otherwise. Then, the set of δ_x as x ranges over elements of V is a basis for C_X. The endomorphism $T: C_X \to C_X$ given by

$$T(\delta_x) = \sum_{y \in E:\ \mathrm{o}(y) = x} \delta_{t(y)}$$

enjoys a role analogous to the Hecke operator T_p. The matrix of T with respect to the basis $\delta_x : x \in V$ is called the *adjacency matrix* of X. Analogously, we define the operators $\Theta_m \in \mathrm{End}(C_X)$ by

$$\Theta_m(\delta_x) = \sum_{\underline{y}} \delta_{t(\underline{y})},$$

where the sum is over walks $\underline{y} = (y_1, \dots, y_m)$ without backtracking with origin x and length m. Clearly, $\Theta_1 = T$. Thus,

$$T\Theta_m = \Theta_{m+1} + \begin{cases} q+1 & \text{if } m = 1m \\ q\Theta_{m-1} & \text{if } m > 1. \end{cases}$$

We put $T' = T/\sqrt{q}$, and $\Theta'_m = \Theta_m/q^{m/2}$. Our goal is to study the equidistribution of the eigenvalues of the (normalized) adjacency matrix T'. It is clear that $\mathrm{Tr}(\Theta_m) = f_m$. We use this observation below.

The above recursion leads to the formal identity

$$\sum_{m=0}^{\infty} \Theta'_m t^m = \frac{1 - t^2/q}{1 - tT' + t^2}.$$

(Note that there is a typo in (104) of [26]. The T should be a T' in the formula.) As in [26], we can define $X_{n,q}(x)$ by the power series

$$\sum_{n=0}^{\infty} X_{n,q}(x) t^n = \frac{1 - t^2/q}{1 - xt + t^2}.$$

We also define $X_n(x)$ by

$$\sum_{n=0}^{\infty} X_n(x) t^n = \frac{1}{1 - xt + t^2}.$$

This is the generating function for the Chebychev polynomials of the second kind. An easy induction argument shows that

$$X_n(x) = \frac{\sin(n+1)\phi}{\sin\phi},$$

where $x = 2\cos\phi$. Clearly, $X_{n,q}(x) = X_n(x) - q^{-1} X_{n-2}(x)$ for $n \geqslant 2$. Thus, $\Theta'_m = X_{m,q}(T')$. If we let $Y_m(x) = X_m(x) - X_{m-2}(x)$ for $m \geqslant 2$, then as in [26], we deduce that

$$\mathrm{Tr}\big(Y_m(T')\big) = C_m q^{-m/2} - \begin{cases} (q-1)q^{-m/2}|V| & \text{if } m \text{ is even,} \\ 0 & \text{if } m \text{ is odd.} \end{cases} \tag{21}$$

This result gives us the determination of the requisite Weyl sums.

Indeed, the eigenvalues lie in the interval Ω_q. If we write the eigenvalues as x_i, with $1 \leqslant i \leqslant |V|$, then setting $\lambda_i = 2x_i/\omega_q$, we may write $\lambda_i = 2\cos\phi_i$ for some unique $\phi_i \in [0, \pi]$. The equidistribution of the x_i's is equivalent to the equidistribution of the ϕ_i's. To determine their equidistribution, we need to study the sums

$$\sum_i 2\cos m\phi_i.$$

With our notation above, this is the same as the study of

$$\sum_i Y_m(\lambda_i).$$

Now let X_i be a family of regular graphs of degree $k = q + 1$. Let T_i be the adjacency matrix of X_i. All the eigenvalues of T'_i lie in the interval $\Omega_q = [-\omega_q, \omega_q]$ where $\omega_q = q^{1/2} + q^{-1/2}$. This interval contains $[-2, 2]$. We let $\underline{x}_i$ be the family of eigenvalues of T'_i and view them as elements of Ω_q. Let $C_{m,i}$ be the number of circuits of X_i. We have

Theorem 34. *The following are equivalent.*

(a) *There is a measure ν_q on Ω_q such that the $\underline{x}_i$'s are equidistributed with respect to ν_q.*
(b) *For all $m \geqslant 1$, the limits*

$$\gamma_m := \lim_{i\to\infty} \frac{C_{m,i}}{|V_i|}$$

exist.

Suppose now that the limits exist and let $[\alpha,\beta] \subseteq \Omega_q$. Then, the number of eigenvalues of T_i that lie in $[\alpha,\beta]$ is equal to

$$|V_i| \int_{\alpha}^{\beta} \nu_q + \Delta,$$

where

$$|\Delta| \leqslant \frac{\|\nu_q\||V_i|}{M+1} + 2 \sum_{1\leqslant m\leqslant M} \min\left(\frac{1}{M+1} + \min\left(b-a, \frac{1}{\pi m}\right)\right) \left|\frac{C_{m,i} - \gamma_m|V_i|}{q^{m/2}}\right|.$$

Proof. The first part of the result is contained in [26]. The second part follows from our effective treatment of equidistribution theory. □

19. Concluding remarks

It would be interesting to further investigate the order of the error term in Theorem 2. If one could improve the error term substantially, then one can show that

$$s(N,k)_d \ll N^{\alpha}$$

with $\alpha < 1$. Serre asks [26, p. 89] if any $\alpha > 0$ is permissible. The case $d = 1$ and $k = 2$ corresponds to the counting of elliptic curves with conductor N. Indeed, thanks to the famous Shimura–Taniyama–Weil conjecture, now proved by the work of Wiles, Taylor–Wiles and Breuil–Conrad–Diamond–Taylor (see [2]), in the special case $k = 2$ and $d = 1$, estimating $s(N,k)_d$ is equivalent to counting the number of isogeny classes of elliptic curves defined over $\mathbb{Q}$ and of conductor N. In this connection, Brumer and Silverman [3] have shown that $s(N,2)_1 \ll N^{1/2+\epsilon}$ for any $\epsilon > 0$. This has been subsequently improved by various people. Lillian Pierce, in [20], has obtained a bound of the form $O(N^{27/56})$ and Helfgott and Venkatesh in [12] got the further improvement $O(N^{.22377+\epsilon})$. As indicated in [3], the celebrated Birch and Swinnerton–Dyer conjecture along with the generalized Riemann hypothesis for L-series attached to elliptic curves imply an estimate of $O(N^{\epsilon})$ for any $\epsilon > 0$.

Another avenue of investigation is to improve the constants in our estimates. This would have important consequences for numerical computation. For example, the effective determination of all values of N for which $J_0(N)$ is isogenous to a product of simple abelian varieties each of dimension $\leqslant 2$ has not been carried out. Our theorem gives an effective bound for N but it is another matter to actually determine all the finite values of N for which this holds.

An important direction for further work is the improvement of estimates in several contexts. For instance, substantial improvements in the error terms in the study of equidistribution of eigenvalues of T_p acting on $S(N,k)^{\mathrm{new}}$ can be derived. There are other natural subspaces of $S(N,k)$ on which T_p acts and one can derive equidistribution laws in these contexts as well. We have not discussed these questions here to keep the size of this paper to reasonable length. However, we plan to address these questions in [18].

Acknowledgments

Some of the results of this paper are contained in the second author's doctoral thesis [28]. We would like to thank Amir Akbary, Valentin Blomer, Ernst Kani, Peter Sarnak and Jean-Pierre Serre for their remarks on an earlier version of this paper. We also thank the referee for useful remarks.

References

[1] A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge Univ. Press, 1984.
[2] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises, J. Amer. Math. Soc. 14 (4) (2001) 843–939.
[3] A. Brumer, J. Silverman, The number of elliptic curves over $\mathbb{Q}$ of conductor N, Manuscripta Math. 91 (1996) 95–102.
[4] H. Cohen, A Course in Computational Algebraic Number Theory, Grad. Texts in Math., vol. 138, Springer-Verlag, 1993.
[5] H. Cohen, Sur les N tels que $J_0(N)$ soit $\mathbb{Q}$-Isogène à un produit de courbes elliptiques, preprint, available on http://www.ufr-mi.u-bordeaux.fr/~cohen.
[6] J.B. Conrey, W. Duke, D.W. Farmer, The distribution of the eigenvalues of Hecke operators, Acta Arith. 78 (4) (1997) 405–409.
[7] P. Deligne, La conjecture de Weil I, Inst. Hautes Études Sci. Publ. Math. 43 (1974) 273–307.
[8] P. Erdös, P. Turán, On a problem in the theory of uniform distribution I, Indag. Math. 10 (1948) 370–378;
P. Erdös, P. Turán, On a problem in the theory of uniform distribution II, Indag. Math. 10 (1948) 406–413.
[9] E.P. Golubeva, The distribution of the eigenvalues of Hecke operators, J. Math. Sci. 133 (6) (2006) 1622–1626.
[10] B. Gyires, Doubly ordered linear rank statistics, Acta Math. Acad. Sci. Hungar. 40 (1–2) (1982) 55–63.
[11] E. Halberstadt, A. Kraus, Courbes de Fermat: résultats et problèmes, J. Reine Angew. Math. 548 (2002) 167–234.
[12] H. Helfgott, A. Venkatesh, Integral points on elliptic curves and 3-torsion in class groups, J. Amer. Math. Soc. 19 (3) (2006) 527–550.
[13] M.N. Huxley, A note on polynomial congruences, in: Recent Progress in Analytic Number Theory, Durham, 1979, Academic Press, 1981, pp. 193–196.
[14] L. Kuipers, H. Niederreiter, Uniform Distribution of Sequences, John Wiley and Sons, 1974.
[15] C. Mauduit, J. Rivat, A. Sarkozy, On the pseudo-random properties of n^c, Illinois J. Math. 46 (1) (2002) 185–197.
[16] H.L. Montgomery, Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis, Conf. Board Math. Sci., vol. 84, Amer. Math. Soc., 1994.
[17] M. Ram Murty, Problems in Analytic Number Theory, second ed., Grad. Texts in Math., vol. 206, Springer-Verlag, 2007.
[18] M. Ram Murty, K. Sinha, Asymptotic equidistribution of eigenvalues of the Hecke operator T_p, in preparation.
[19] J.-L. Nicolas, G. Robin, Majorations explicites pour le nombre de diviseurs de N, Canad. Math. Bull. 26 (4) (1983) 485–492.
[20] L. Pierce, The 3-part of class numbers of quadratic fields, J. Lond. Math. Soc. (2) 71 (3) (2005) 579–598.
[21] S. Ramanujan, Highly composite numbers, Proc. London Math. Soc. (2) XIV (1915) 347–409.
[22] K. Ribet, Twists of modular forms and endomorphisms of abelian varieties, Math. Ann. 253 (1980) 43–62.
[23] E. Royer, Facteurs $\mathbb{Q}$-simple de $J_0(N)$ de grande dimension et de grand rang, Bull. Soc. Math. France 128 (2) (2000) 219–248.
[24] P. Sarnak, Statistical properties of eigenvalues of the Hecke operators, in: Analytic Number Theory and Diophantine Problems, Stillwater, 1984, in: Progr. Math., vol. 70, Birkhäuser, Basel, 1987, pp. 321–331.
[25] R. Schoof, M. van der Vlugt, Hecke operators and weight distribution of certain codes, J. Combin. Theory Ser. A 57 (1991) 163–186.
[26] J.-P. Serre, Répartition Asymptotique des Valeurs Propres de l'Operateur de Hecke T_p, J. Amer. Math. Soc. 10 (1) (1997) 75–102.
[27] F. Shahidi, Symmetric Power L-Functions for GL(2), in: CRM Proc. Lecture Notes, vol. 4, Amer. Math. Soc., 1994, pp. 159–182.
[28] K. Sinha, Effective equidistribution of eigenvalues of Hecke operators, PhD thesis, Queen's University at Kingston, 2006.
[29] R. Taylor, Automorphy for some ℓ-adic lifts of automorphic mod ℓ representations, II, in press.
[30] J.D. Vaaler, Some extremal functions in Fourier analysis, Bull. Amer. Math. Soc. 12 (1985) 183–216.
[31] A. Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2) 141 (3) (1995) 443–551.
[32] T. Yamauchi, On $\mathbb{Q}$-simple factors of Jacobian varieties of quotient modular curves, J. Ramanujan Math. Soc. 19 (3) (2004) 167–180.