Problem 1. Kernels of Hecke operators on $S_k(N, \chi)$ (50 points)

Throughout this problem we fix $N \in \mathbb{Z}_{\geq 1}$, $k \in \mathbb{Z}_{>2}$, a Dirichlet character $\chi$ of modulus $N$ for which $\chi(-1) = (-1)^k$, and we let $S_k(N, \chi) := S_k(\Gamma_0(N), \chi)$ and $S_k(N) := S_k(\Gamma_0(N))$.

For each positive integer $n$ define the sets

\[
\Delta_n(N) := \left\{ \left( \frac{a}{c} \right) \in \mathbb{M}_2(\mathbb{Z}) : c \equiv 0 \mod N, a \perp N, ad - bc = n \right\},
\]

\[
\Delta_n^*(N) := \left\{ \left( \frac{a}{c} \right) \in \mathbb{M}_2(\mathbb{Z}) : c \equiv 0 \mod N, d \perp N, ad - bc = n \right\},
\]

(which we note coincide when $n \perp N$), and the function

\[
K_n(z_1, z_2, \chi) := n^{k-1} \sum_{\alpha \in \Delta_n^*(N)} \overline{\chi}(d)j(\alpha, z_1)^{-k}(\alpha z_1 + z_2)^{-k},
\]

for $z_1, z_2 \in \mathbb{H} := \{ z \in \mathbb{C} : \text{Im}(z) > 0 \}$, with $j\left( \left( \frac{a}{c} \right), z \right) := cz + d$.

(a) Prove that $K_n$ satisfies the identity

\[
K_n(z_1, -\bar{z}_2, \chi) = (-1)^k \overline{K_n(-\bar{z}_1, z_2, \chi)},
\]

and that for any fixed $z_1, z_2 \in \mathbb{H}$ we have $K_n(z, z_2, \chi), K_n(z_1, z, \chi) \in S_k(N, \chi)$. Conclude that $K_n(z, z, \chi) \in S_{2k}(N)$ (no matter what $\chi$ is).

(b) Prove that for $n \perp N$ we also have the identities

\[
K_n(z_2, z_1, \chi) = \overline{\chi(n)} K_n(z_1, z_2, \chi),
\]

\[
K_n(z_1, -\bar{z}_2, \chi) = (-1)^k \overline{\chi(n)} K_n(z_2, -\bar{z}_1, \chi).
\]

If $\Delta_n(N) = \prod_{i=1}^r \Gamma_0(N)\alpha_i$ with $\alpha_i = \left( \frac{a_i}{c_i} \right)$, we may define the action of the Hecke operator $T(n)$ on $f \in S_k(N, \chi)$ via

\[
f|_k T(n) = n^{k/2-1} \sum_i \chi(a_i) f|_k \alpha_i.
\]

Recall that for $n \perp N$ we have $f|_k T(n) = \chi(n) f|_k T^*(n)$ (see Lecture 12), in which case we could also have defined this action using a decomposition of $\Delta_n^*(N)$ and replacing $\chi(a_i)$ with $\overline{\chi}(d_i)$ (but this is not true when $\gcd(n, N) > 1$).
(c) Derive the following explicit expression for the action of $T(n)$ on $f \in S_k(N, \chi)$:

$$f|_k T(n) = \frac{1}{n} \sum_{ad=n, a>0} \chi(a) a^k \sum_{0 \leq b < d} f(\frac{az+b}{d}).$$

(d) Let $q := q(z) = e^{2\pi i z}$. Show that if $f \in S_k(N, \chi)$ has $q$-expansion $f(z) = \sum_{m \geq 1} a_m q^m$ then $f|_k T(n)$ has $q$-expansion $\sum_{m \geq 1} b_m q^m$ where

$$b_m = \sum_{d \mid \gcd(m,n), d>0} \chi(d) d^{k-1} a_{mn/d^2}.$$ 

As in lecture, we will work with the inner product on the Hilbert space $L^2_0(\Gamma_0(N), \chi)$

$$\langle f, g \rangle := \int_{\Gamma_0(N) \backslash \mathbb{H}} f(z) \overline{g(z)} \text{Im}(z)^k dv(z).$$

which is equal to the Petersson inner product on $S_k(N, \chi) \subseteq L^2_0(\Gamma, \chi)$ multiplied by a factor of $\nu(\Gamma_0(N)/\mathbb{H}) = \frac{2}{\pi} \nu(N)$, where $\nu(N) := [\text{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N}(1 - \frac{1}{p})$.

We note the following identity, valid for $z_2 \in \mathbb{H}$ and $f \in S_k(N, \chi)$, which you are not required to prove:

$$\int_{\mathbb{H}} f(z_1)(z_1 + z_2)^{-k} \text{Im}(z_1)^k dv(z_1) = \frac{4\pi}{k-1} (i/2)^k f(-\bar{z}_2).$$

(e) Prove that for $f \in S_k(N, \chi)$ and $z_2 \in \mathbb{H}$ we have

$$\langle f(z), K_n(z, z_2, \chi) \rangle = \frac{4\pi}{k-1} (i/2)^k (f|_k T(n))(z_2).$$

If $T$ is a linear operator on a Hilbert space $H$ of functions $X \to \mathbb{C}$, we call $K(x, y)$ a kernel function for $T$ if $(Tf)(y) = \langle f(x), K_y(x) \rangle$ for all $f \in H$, with $K_y(x) := K(x, y) \in H$ for all $y \in X$ (so a kernel function for $H$ is a kernel function for the identity operator).

(f) Prove that

$$K_n(z_1, z_2) := \frac{k-1}{4\pi} (2i)^k K_n(z_1, -\bar{z}_2, \chi)$$

is the kernel function of the Hecke operator $T(n)$ on $S_k(N, \chi)$, and in particular, $K_1(z_1, z_2)$ is the kernel function of $S_k(N, \chi)$.

(g) Prove that for $n \perp N$ we have

$$\langle f|_k T(n), g \rangle = \chi(n) \langle f, g|_k T(n) \rangle$$

for all $f, g \in S_k(N, \chi)$, thus $T(n)$ is a $\chi$-Hermitian operator on $S_k(N, \chi)$.

(h) Let $f_1, \ldots, f_r$ be a basis of eigenforms for $S_k(N, \chi)$ normalized so $f_i|_k T(n) = a_n(f_i) f_i$ for $n \perp N$. Show that for $n \perp N$ we have

$$K_n(z_1, z_2) = \sum_{i=1}^r \overline{a_n(f_i)} \frac{f_i(z_1)}{\langle f_i, f_i \rangle} \bar{f}_i(z_2).$$

(i) Prove that for all $n$ (whether coprime to $N$ or not) we have

$$\text{tr}(T(n)|S_k(N, \chi)) = \int_{\Gamma_0(N) \backslash \mathbb{H}} K_n(z, z) \text{Im}(z)^k dv(z).$$
Problem 2. Dirichlet characters and Conrey characters (50 points)

Recall that a Dirichlet character is a totally multiplicative periodic function $\chi : \mathbb{Z} \to \mathbb{C}$; this means that $\chi(1) = 1$, $\chi(mn) = \chi(m)\chi(n)$ for all $m, n \in \mathbb{Z}$, and there exists a positive integer $q$ for which $\chi(n + q) = \chi(n)$ for all $n \in \mathbb{Z}$, in which case we say that $\chi$ is $q$-periodic. The least such $q$ is the period of $\chi$. A Dirichlet character of modulus $q$ is a $q$-periodic Dirichlet character for which $\chi(n) \neq 0$ if and only if $n \perp q$, equivalently the extension-by-zero of a character of $(\mathbb{Z}/q\mathbb{Z})^\times$.

(a) Show that a product of Dirichlet characters is a Dirichlet character, and that every Dirichlet character admits a unique factorization into Dirichlet characters whose periods are powers of distinct primes.

(b) Show that every Dirichlet character of period $q$ is a Dirichlet character of modulus $q$,

but not every $q$-periodic Dirichlet character is a Dirichlet character of modulus $q$,

and show that a Dirichlet character of modulus $q$ is also a Dirichlet character of modulus $q'$ for infinitely many distinct $q'$

Thus every Dirichlet character $\chi$ is the extension by zero of a group character, but

that group character is not uniquely determined unless the modulus is specified. If $\chi$ is

a Dirichlet character of modulus $q$ and $q'$ is a multiple of $q$, the extension-by-zero of the

projection of $\chi$ to $(\mathbb{Z}/q'\mathbb{Z})^\times$ is a Dirichlet character of modulus $q'$ with $\chi'(n) = \chi(n)$ for

all $n \perp q'$. We say that such a character $\chi'$ is induced by $\chi$. A Dirichlet character that

is not induced by any character other than itself is primitive.

(c) Show that for every Dirichlet character $\chi$ there is a minimal $c \in \mathbb{Z}_{>1}$ dividing the

period $q$ of $\chi$ for which $\chi(n + cm) = \chi(n)$ for all $n, n + cm \perp q$, called the conductor

of $\chi$, denoted $\text{cond}(\chi)$. Then show that the extension-by-zero $\chi'$ of the projection

of $\chi$ to $(\mathbb{Z}/c\mathbb{Z})^\times$ is the unique primitive Dirichlet character that induces $\chi$.

Dirichlet characters of conductor 1 are principal. The order of a Dirichlet character $\chi$ is the least $c \in \mathbb{Z}_{>1}$ such that $\chi^c$ is principal. The field of values $\mathbb{Q}(\chi) := \mathbb{Q}(\chi(\mathbb{Z}))$ is the number field obtained by adjoining all values of $\chi$ to $\mathbb{Q}$. The fixed field of a Dirichlet character of period $q$ is the subfield of $\mathbb{Q}(\zeta_q)$ fixed by all automorphisms $\zeta_q \mapsto \zeta_q^c$ for which $\chi(a) = 1$.

(d) Let $\chi$ be a Dirichlet character order $n$ and period $q$. Show that $\mathbb{Q}(\chi) = \mathbb{Q}(\zeta_n)$ and its fixed field is a cyclic extension of $\mathbb{Q}$ of degree $n$. Then show that the primitive character inducing $\chi$ has the same order, field of values, and fixed field as $\chi$ (even though it need not have the same period), and that the conductor $c := \text{cond}(\chi)$ is the least positive integer for which $\mathbb{Q}(\zeta_c)$ contains the fixed field of $\chi$.

The parity of a Dirichlet character $\chi$ is determined by the value of $\chi(-1) \in \{\pm1\}$; we call $\chi$ even if $\chi(-1) = 1$ and odd otherwise. Dirichlet characters $\chi$ and $\psi$ are Galois conjugates if $\psi = \sigma \circ \chi$ for some $\sigma \in \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The set of Galois conjugates of a Dirichlet character $\chi$ is its Galois orbit.

(e) Show that Galois conjugate Dirichlet characters necessarily have the same period, conductor, parity, order, fixed field, and field of values, and that if $\chi$ and $\psi$ are Galois conjugates, then the primitive characters that induce them are Galois conjugates.
(f) Show that if \( \chi \) is a Dirichlet character of modulus \( q \) and order \( e \) then the size of its Galois orbit is determined by the Euler \( \varphi \)-function \( \varphi(e) := \#(\mathbb{Z}/e\mathbb{Z})^\times \). Then show we can count Galois orbits of Dirichlet characters of modulus \( q \) via the formula

\[
\xi(q) := \sum_{e|\lambda(q)} \frac{\varphi(q,e)}{\varphi(e)},
\]

where \( \lambda(q) \) is the exponent of the group \((\mathbb{Z}/q\mathbb{Z})^\times\) (the least common multiple of the orders of its elements), and

\[
\varphi(q,e) := \#\{n \in (\mathbb{Z}/q\mathbb{Z})^\times : \text{ord}(n) = e\}
\]

counts the elements of \((\mathbb{Z}/q\mathbb{Z})^\times\) of order \( e \). Describe a polynomial-time algorithm to compute \( \xi(q) \), given the prime factorizations of \( q \) and \( \lambda(q) \), and use it to compute \( \xi(q) \) for \( q = 10^{100} \), \( q = 20! \), and \( q = N \), where \( N \) is your 9-digit student ID.

Conrey characters provide an explicit isomorphism between \((\mathbb{Z}/q\mathbb{Z})^\times\) and the group of Dirichlet characters of modulus \( q \). For each modulus \( q \in \mathbb{Z}_{\geq 1} \) and integers \( n, m \in \mathbb{Z} \) coprime to \( q \) we define the value \( \chi_q(n,m) \) of the Dirichlet character \( \chi_q(n,\cdot) \) associated to the image of \( n \) in \((\mathbb{Z}/q\mathbb{Z})^\times\) as follows.

- For each odd prime \( p \) let \( g_p \) be the least positive integer that is a primitive root modulo \( p^\ell \) for all \( p^\ell \), and for \( n = g_p^a \mod p^\ell \) and \( m = g_p^b \mod p^\ell \) coprime to \( p \) let
  \[
  \chi_{p^\ell}(n,m) := \exp\left(\frac{2\pi abi}{p^\ell}\right).
  \]
- We define \( \chi_2(1,1) = \chi_4(1,1) = \chi_4(3,1) = 1 \) and \( \chi_4(3,3) = -1 \), and for \( 2^e > 4 \), if \( n \equiv \epsilon_a 5^a \mod 2^e \) and \( m \equiv \epsilon_b 3^b \mod 2^e \) with \( \epsilon_a, \epsilon_b \in \{\pm 1\} \) then
  \[
  \chi_{2^e}(n,m) := \exp\left(2\pi i \left(\frac{(1-\epsilon_a)(1-\epsilon_b)}{8} + \frac{ab}{2^{e-2}}\right)\right).
  \]
- For general \( q \) with prime factorization \( q = p_1^{e_1} \cdots p_e^{e_e} \) we define \( \chi_q(m,n) \) to be the product of \( \chi_{p_i^{e_i}}(n,m) \), and let \( \chi_q(n,m) := 0 \) if either \( n \) or \( m \) is not coprime to \( q \).

(g) Show that one can take \( g_p \) to be the least positive integer that generates \((\mathbb{Z}/p^2\mathbb{Z})^\times\), but the least positive integer that generates \((\mathbb{Z}/p\mathbb{Z})^\times\) need not generate \((\mathbb{Z}/p^2\mathbb{Z})^\times\) (hint: consider \( p = 40487 \)).

The computation of \( \chi_{p^\ell}(n,m) \) requires computing discrete logarithms in \((\mathbb{Z}/p^\ell\mathbb{Z})^\times\) to obtain the values of \( a \) and \( b \) that are used in the formulas above. This problem can be efficiently reduced to a discrete logarithm problem in \( \mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times \), which makes it easy to compute values of \( \varphi_q(n,\cdot) \) as long as known of the primes \( p|q \) are too large. For large \( p \) there are subexponential-time algorithms for computing discrete logarithms in \( \mathbb{F}_p^\times \), but no polynomial-time algorithm is known. In most practical situations the values of \( q \) that arise are small enough (less than \( 10^{12} \), say) so that one can simply use a baby-steps giant-steps approach to obtain an \( \tilde{O}(\sqrt{p}) \) algorithm that is fast enough.

An attractive feature of Conrey characters is that most of the arithmetic invariants of \( \chi_q(n,\cdot) \) that one is interested in, including its order, parity, and conductor, can be computed very quickly (in polynomial-time), provided one knows the factorization of \( q \) and the factorization of \( p-1 \) for primes \( p|q \).
(h) Show that for $q = p_1^{e_1} \cdots p_r^{e_r}$ and $m,n \in \mathbb{Z}$ coprime to $q$ the following hold:

- $\chi_q(m,n) = \chi_q(n,m)$.
- $\chi_q(n,\cdot) = \prod_i \chi_{p_i^{e_i}}(n,\cdot) = \prod_i \chi_{p_i^{e_i}}(n \text{ mod } p_i,\cdot)$.
- $\operatorname{ord}(\chi_q(n,\cdot)) = \operatorname{lcm}_i \{\operatorname{ord}(\chi_{p_i^{e_i}}(n,\cdot))\}$, with $\operatorname{ord}(\chi_{p^{e}}(n,\cdot))$ the order of $n$ in $(\mathbb{Z}/p^e\mathbb{Z})^\times$.
- $\operatorname{cond}(\chi_q(\cdot,\cdot)) = \prod_i \operatorname{cond}(\chi_{p_i^{e_i}}(n,\cdot))$, where
  $$\operatorname{cond}(\chi_{p^e}(n,\cdot)) = \begin{cases} 1 & \text{ if } n \equiv 1 \text{ mod } p^e, \\ p^{a+2} & \text{ if } n \not\equiv \pm 1 \text{ mod } p^e \text{ and } p = 2, \\ p^{a+1} & \text{ otherwise,} \end{cases}$$
  with $a = v_p(\operatorname{ord}(\chi_{p^e}(n,\cdot)))$.
- The value field of $\chi_q(n,\cdot)$ is real if and only if $n^2 \equiv 1 \text{ mod } q$.
- The parity of $\chi_q(n,\cdot)$ can be computed via
  $$\chi_q(n,-1) = \begin{cases} \prod_{p | q} (\frac{n}{p}) & \text{ if } 4 \nmid q \\ \left(\frac{-1}{n}\right) \prod_{p | q} (\frac{n}{p}) & \text{ otherwise.} \end{cases}$$

where $p$ ranges over odd prime divisors of $q$ and $(\frac{a}{q})$ is the Legendre symbol.

(i) Give a polynomial-time algorithm to compute the parity, order, conductor of $\chi_q(n,\cdot)$, given the prime factorizations of $q$ and $p-1$ for primes $p|q$. Use it to compute the parity, order, conductor of $\chi_q(n,\cdot)$ for $q = 10^{100}$, $q = 20!$, and $q = N$, for the least $n > 1$ coprime to $q$, where $N$ is your 9-digit student ID.

Problem 3. The trace formula for $S_k(N,\chi)$ (50 points)

Fix $n,N \in \mathbb{Z}_{\geq 1}$, $k \in \mathbb{Z}_{\geq 2}$, and a Dirichlet character $\chi$ of modulus $N$ with $\chi(-1) = (-1)^k$.

Using the results of Problem 1 it is possible (but highly non-trivial) to derive the following explicit trace formula which appears in [2, Theorem 3].

$$\operatorname{tr}(T(n)|S_k(N,\chi)) = -\frac{1}{2} \sum_{t^2 \leq 4n} P_k(t,n) \sum_{u|N} H \left(\frac{4n-t^2}{u^2}\right) C(N,\chi,u,t,n)$$

$$- \frac{1}{2} \sum_{ad=n} \min(a,d)^{k-1} \Phi(N,\chi,a,d) + 2\delta_{k=2,\chi=1} \sigma_1(N,n).$$

where $t$ ranges over $\mathbb{Z}$ and $u,a,d$ range over $\mathbb{Z}_{\geq 1}$ and $P_k, H, C, \Phi, \delta, \sigma_1$ are defined by:

- $P_k(t,n)$ is the coefficient of $x^{k-2}$ in $(1 - tx + nx^2)^{-1} \in \mathbb{Z}[[x]]$.
  Equivalently, $P_k(t,n) = \frac{a^{k-1} - \tilde{a}^{k-1}}{\alpha - \tilde{\alpha}}$, where $\alpha, \tilde{\alpha} \in \mathbb{C}$ are the roots of $x^2 - tx + n$.

- $H(n)$ is the Hurwitz class number: $H(n) = 0$ unless $n \in \mathbb{Z}_{\geq 0}$ and $-n \equiv 0 \text{ mod } 4$, in which case $H(0) = -\frac{1}{2}$ and $H(-D)$ counts $\text{SL}_2(\mathbb{Z})$ equivalence classes of positive definite binary quadratic forms $ax^2 + bxy + cy^2$ of discriminant $b^2 - 4ac = D < 0$.

\[\text{[There is a minor error in [2, Lemma 4.5] that does not impact this theorem; see [1, A.2].}\]
Show that for any fixed \(\Phi(C,\delta)\) is the summing over the Galois orbit of \(Q\) that generate a number field with a running time that is quasilinear in \(k\) or \(t,n\) integers, but you are not required to prove this).

- \(C(N,\chi,u,t,n)\) is defined for \(u\mid N\) and \(u^2|(t^2 - 4n)\) with \(\frac{t^2 - 4n}{u^2} \equiv \Box \mod 4\) by

\[
S(N,u,t,n) := \{m \in \mathbb{Z} \cap [1,N] : m \perp N \text{ and } m^2 - tm + n \equiv 0 \mod Nu\}
\]

\[
B(N,\chi,u,t,n) := \frac{\psi(N)}{\psi(N/u)} \sum_{m \in S(N,u,t,n)} \chi(m)
\]

\[
C(N,\chi,u,t,n) := \sum_{a|u} \mu(a) B(N,\chi,u/a,t,n)
\]

where \(\psi(N) = [\Gamma(1) : \Gamma_0(N)] = N \prod_{p\mid N}(1 + \frac{1}{p})\) and \(\mu(a)\) is the Möbius function.

- \(\Phi(N,\chi,a,d)\) is defined by

\[
\Phi(N,\chi,a,d) = \sum_{rs=N, m=gcd(r,s)} \varphi(m) \chi(\hat{\alpha}_{r,s}(a,d))
\]

where \(\alpha_{r,s} : \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z} \to \mathbb{Z}/\lcm(r,s)\mathbb{Z}\) is the map determined by the CRT and \(\hat{\alpha}_{r,s}\) denotes any lift to \(\mathbb{Z}\), and \(\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times\) is Euler’s \(\varphi\)-function.

- \(\delta_{k=2,\chi-1} \in \{0,1\}\) is 1 iff \(k = 2\) and \(\chi\) is trivial, and \(\sigma_1(N,n) = \sum_{a|n,\perp N} \frac{n}{a} \in \mathbb{Z}\).

(a) Prove that \(\text{tr}(T(n)|S_k(N,\chi)) \in \mathbb{Q}(\chi)\), where \(\mathbb{Q}(\chi)\) is the value field of \(\chi\), and that summing over the Galois orbit of \(\chi\) yields an integer. Conclude that if \(f(z) = \sum a_n q^n\) is the \(q\)-expansion of a newform in \(S_k(N,\chi)\), then the \(a_n\) are algebraic numbers that generate a number field \(\mathbb{Q}(f)\) that contains \(\mathbb{Q}(\chi)\) (in fact the \(a_n\) are algebraic integers, but you are not required to prove this).

(b) Show that for any fixed \(t,n \in \mathbb{Z}\) with \(t^2 \leq 4n\), the function \(g(k) := P_k(t,n)\) defines a sequence of integers satisfying a second order linear recurrence. Use this to develop an algorithm to efficiently compute \(P_k(t,n)\) using only integer arithmetic, with a running time that is quasilinear in \(k \log(n)\) (assume that multiplying two \(b\)-bit integers take \(O(b \log b)\) time and adding two \(b\)-bit integers takes \(O(b)\) time).

(c) Show that \(C(N,\chi,u,t,n)\) is a multiplicative function of \(N\) that can be computed using the values of \(C(p^e,\chi^t,p^f,t,n)\), where \(v = v_p(N)\), \(a = v_p(u)\), and \(\chi^t\) is the Dirichlet character of modulus \(p^f\) that appears in the factorization of \(\chi\) into Dirichlet characters of prime power modulus, and give a similar argument for \(\Phi(N,\chi,a,d)\).
(d) By specializing the formula for $\text{tr}(T(n)|S_k(N))$ to $n = 1$ and $\chi = 1$, derive a formula for computing $\dim S_k(N) = \text{tr}(T(1)|S_k(N))$ that has the form

$$\dim S_k(N) = \frac{1}{12} w(k) \cdot \prod_{p^e \mid N} v(p, e) + \delta_{k=2},$$

where $w(k)$ and $v(p, e)$ are quadruples of integers, with the $v(p, e)$ multiplied point-wise, followed by a dot product with $v(k)$. Use your formula to compute $\dim S_k(N)$ for $k \in \{2, 10^{12}\}$ and $N = 10^{20}$, $N = 20!$, and $N$ equal to your 9-digit student ID.

(e) Recall from Lecture 15 that we have a decomposition

$$S_k(N) \simeq \bigoplus_{M \mid N} S_k^{\text{new}}(M) \oplus \sigma_0(N/M) \cdot S_k^N,$$

where $\sigma_0(n) = \sum_{d \mid n} 1$ counts the divisors of $n$. This implies

$$\dim S_k(N) = \sum_{M \mid N} \sum_{d \mid N} \dim S_k^{\text{new}}(M).$$

For each fixed $k$, part (d) implies that $\dim S_k(N)$ is a sum of multiplicative functions of $N$. Use Möbius inversion to express $\dim S_k^{\text{new}}(N)$ as a sum of multiplicative functions of $N$ to obtain a formula of the form

$$\dim S_k^{\text{new}}(N) = \frac{1}{12} w(k) \cdot \prod_{p^e \mid N} u(p, e) + \delta_{k=2} \cdot \mu(N),$$

where $w(k)$ and $u(p, e)$ are quadruples of integers as in (d), and give explicit formulas for $u(p, e)$. Then use your formulas to compute the dimension of $S_k^{\text{new}}(N)$ for the values of $k$ and $N$ used in (d).

(f) Note that $\text{tr}(T(n)|S_k(N, \chi)) = 0$ whenever $\chi(-1) \neq (-1)^k$, since $\dim S_k(N, \chi) = 0$. Show $C(N, \chi, u, t, n) = \chi(-1)C(N, \chi, u, -t, n)$ and $P_k(k, t, n) = (-1)^k P_k(k, -t, n)$, and conclude that if $\chi(-1) \neq (-1)^k$ then the double sum in the first line of the trace formula vanishes for $\chi(-1) \neq (-1)^k$.

Then show that $\Phi(N, \chi, -a, -d) = \chi(-1)\Phi(N, \chi, a, d)$ and conclude that if we replace $\Phi(N, \chi, a, d)$ with $(\Phi(N, \chi, a, d) + (-1)^k \Phi(N, \chi, -a, -d))/2$ in the trace formula it is then valid for all $\chi$, without any restriction on parity. By summing this generalized trace formula over all $\chi$ of modulus $N$, show that for $N \geq 5$ we have

$$\dim S_k(\Gamma_1(N)) = \frac{k-1}{24} \prod_{p^e \mid N} (p^{2e} - p^{2e-2}) - \frac{1}{4} \prod_{p^e \mid N} ((p^2 - 1) + e(p-1)^2)p^{e-2} + \delta_{k=2}.$$

**Problem 4. Survey**

Complete the following survey by rating each problem you attempted on a scale of 1 to 10 according to how interesting you found it (1 = “mind-numbing,” 10 = “mind-blowing”), and how difficult you found it (1 = “trivial,” 10 = “brutal”). Also estimate the amount of time you spent on each problem to the nearest half hour.
<table>
<thead>
<tr>
<th>Problem</th>
<th>Interest</th>
<th>Difficulty</th>
<th>Time Spent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Problem 1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem 2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem 3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please rate each of the following lectures that you attended, according to the quality of the material (1=“useless”, 10=“fascinating”), the quality of the presentation (1=“epic fail”, 10=“perfection”), the pace (1=“way too slow”, 10=“way too fast”, 5=“just right”) and the novelty of the material to you (1=“old hat”, 10=“all new”).

<table>
<thead>
<tr>
<th>Date</th>
<th>Lecture Topic</th>
<th>Material</th>
<th>Presentation</th>
<th>Pace</th>
<th>Novelty</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/22</td>
<td>Traces of Hecke operators</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/24</td>
<td>Modular abelian varieties</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4/29</td>
<td>Level structures on elliptic curves</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5/1</td>
<td>Modular curves</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Please feel free to record any additional comments you have on the problem sets and the lectures, in particular, ways in which they might be improved.

References
