# MODULAR FORMS EXAMPLE SHEET 3

1. Let $M_k(\mathbb{Z})$ be the space of modular forms of weight $k$ with integral $q$-expansions. Show that the graded ring:

$$\bigoplus M_k(\mathbb{Z})$$

is generated over $\mathbb{Z}$ by $E_4$, $E_6$, and $\Delta$.

This follows easily from the argument of problem 4 of example sheet 2; indeed, the $f_i$ constructed there are easily seen by induction to be integer polynomials in $E_4$, $E_6$, and $\Delta$, and any modular form with integral coefficients is an integral linear combination of the $f_i$.

2a. Show that the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective, for any $N > 1$.

Let $\gamma$ be a matrix in $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, and lift $\gamma$ to a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with entries in $\mathbb{Z}$, and $c$ nonzero. Then $ad - bc = 1 + kN$ for some $k$. In particular the gcd of $d, c$, and $N$ is 1. Let $t$ be the product of the primes that divide $c$ but not $d$. Then $d + tN$ is nonzero modulo all primes dividing $c$ (if $p$ divides $d$ then $p$ does not divide $tN$; if $p$ does not divide $d$ then it divides $tN$), so $c$ and $d + tN$ are relatively prime. Replacing $d$ with $d + tN$ we can thus assume that $c$ and $d$ are relatively prime.

Now choose $u, v$ such that $ud - vc = -k$, where $ad - bc = 1 + kN$. Then $\begin{pmatrix} a + uN & b + vN \\ c & d \end{pmatrix}$ is a lift of $\gamma$ with determinant 1.

2b. Show that the map $\mathrm{GL}_2(\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is not surjective, for any $N > 6$.

On determinants, the induced map is the map $\pm 1 \to (\mathbb{Z}/N\mathbb{Z})^\times$, which is clearly not surjective for $N > 6$.

3. Compute the matrix of the Hecke operator $T_2$ acting on $S_{24}$ with respect to the basis $E_4^3\Delta, \Delta^2$ of $S_{24}$, and show that its characteristic polynomial is irreducible. What does this mean about the eigenforms of level 24?

The computation of the polynomial is routine, if tedious: one uses the formula for $T_2$ on $q$-expansions to obtain the $q$ and $q^2$ coefficients of $T_2E_4^3\Delta$ and $T_2\Delta^2$; these suffice to express $T_2E_4^3\Delta$ and $T_2\Delta^2$ as linear combinations of $E_4^3\Delta$ and $\Delta^2$. The characteristic polynomial of the resulting matrix is $x^2 - 1080x - 20468736$; it is irreducible over $\mathbb{Q}$ since its discriminant is not a perfect square. This implies that the eigenforms of level 24 do not have integer coefficients, and come in a Galois conjugate pair.

4. Let $V$ be a *three* dimensional real vector space, and let $\mathcal{L}$ denote the space of lattices in $V$. For $a, b$ positive integers with $a$ dividing $b$, define a correspondence $T_{a,b}$ on $\mathcal{L}$ by letting $T_{a,b}L$ be the sum of the sublattices $L' \subset L$ such that $L/L'$ is isomorphic to $\mathbb{Z}/a \times \mathbb{Z}/b$.

4a. Show that if $(b, b') = 1$, then $T_{a,b}T_{a',b'} = T_{aa',bb'}$.
NOTATION: We will write $L' \subseteq_{a,b} L$ to mean that $L'$ is a sublattice of $L$ with $L/L'$ isomorphic to $\mathbb{Z}/a \times \mathbb{Z}/b$.

For arbitrary $a, b, a', b'$ we have:

$$T_{a,b}T_{a',b'}L = \sum_{L' \subseteq_{a',b'} L} \sum_{L'' \subseteq_{a,b} L'} L'',$$

and we may rewrite the latter as

$$\sum_{L''} C_{(a,b),(a',b')}(L, L''),$$

where $C_{(a,b),(a',b')}(L, L'')$ counts the number of lattices $L'$ such that $L'' \subseteq_{a,b} L' \subseteq_{a',b'} L$. (Or, equivalently, the number of subgroups $A$ of $L/L''$ such that $A$ is isomorphic to $\mathbb{Z}/a' \times \mathbb{Z}/b'$ and $(L/L'')/A$ is isomorphic to $\mathbb{Z}/a \times \mathbb{Z}/b$.)

If $b$ and $b'$ are relatively prime, then so are $ab$ and $a'b'$. We will show that in this case $C_{(a,b),(a',b')}(L, L'') = 1$ if $L'' \subseteq_{aa',bb'} L$, and zero otherwise. This will prove 4a.

First suppose there exists an $L'$ such that $L'' \subseteq_{a,b} L' \subseteq_{a',b'} L$. Then $L'/L''$ is a subgroup of $L/L''$ isomorphic to $\mathbb{Z}/a \times \mathbb{Z}/b$, and the quotient of $L/L''$ by this subgroup is isomorphic to $L'/L''$ and hence to $\mathbb{Z}/a' \times \mathbb{Z}/b'$. On the other hand, if $A$ is a finite abelian group, and $B$ is a subgroup of $A$ such that the orders of $B$ and $A/B$ are relatively prime, then $A$ is isomorphic to $A \times B/A$. (This follows from the fact that any abelian group is the product of its maximal subgroups of prime power order.) Thus $L/L''$ is isomorphic to $\mathbb{Z}/a \times \mathbb{Z}/b \times \mathbb{Z}/a' \times \mathbb{Z}/b'$, and the latter is isomporphic to $\mathbb{Z}/aa' \times \mathbb{Z}/bb'$.

On the other hand it is easy to see that there is a unique subgroup of order $a'b'$ in $\mathbb{Z}/aa' \times \mathbb{Z}/bb'$, consisting of all the elements of order dividing $a'b'$. Thus, for any $L'' \subseteq_{aa',bb'} L$, there is a unique intermediate $L'$ such that $L'' \subseteq_{a,b} L' \subseteq_{a',b'} L$.

4b. Fix a prime $p$, and express $T_{1,p^2}$, $T_{1,p^3}$, and $T_{p,p^2}$ as polynomials in $T_{1,p}$, $T_{p,p}$, and the "rescaling by $p$" operator $R_p$.

We compute $T_{1,p}^2$, $T_{1,p}T_{p,p}$, and $T_{1,p}T_{1,p^2}$ (in this order.)

First, $T_{1,p}^2 = \sum_{L''} C_{(1,p),(1,p)}(L'', L)L''$. If we have a lattice $L'$ such that $L'' \subseteq_{1,p} L' \subseteq_{1,p} L$, then $L''$ has index $p^2$ in $L$, so $L/L''$ is isomorphic to $\mathbb{Z}/p^2$ or $\mathbb{Z}/p$. The former has exactly one cyclic subgroup of order $p$; the latter has $p+1$. Thus $T_{1,p}^2 = T_{1,p^2} + (p+1)T_{p,p}$. (In particular, $T_{1,p^2} = T_{1,p}^2 - (p+1)T_{p,p}$.)

Next, $T_{1,p}T_{p,p} = \sum_{L''} C_{(1,p),(p,p)}(L'', L)L''$. If we have $L'$ such that $L'' \subseteq_{1,p} L' \subseteq_{p,p} L$, then $L/L''$ is isomorphic to $\mathbb{Z}/p \times \mathbb{Z}/p^2$ or $(\mathbb{Z}/p)^3$. (It cannot be isomorphic to $\mathbb{Z}/p^3$ as it has a quotient $L/L'$ that is not cyclic.) The former has $p+1$ subgroups $A$ of order $p$, but for only one such subgroup is the quotient $(\mathbb{Z}/p\times\mathbb{Z}/p^2)/A$ isomorphic to $\mathbb{Z}/p\times\mathbb{Z}/p$. Thus $c_{(1,p),(p,p)}(L'',L) = 1$ if $L/L''$ is isomorphic to $\mathbb{Z}/p\times\mathbb{Z}/p^2$. On the other hand, if $L/L''$ is isomorphic to $(\mathbb{Z}/p)^3$, then $L'' = R_pL$, there are $p^2+p+1$ subgroups of $L/L''$ of order $p$, and the quotient by any of those is $\mathbb{Z}/p\times\mathbb{Z}/p$. Thus $C_{(1,p),(p,p)}(L'',:) = p^2+p+1$ in this case, and we get $T_{1,p}T_{p,p} = T_{p,p^2} + (p^2+p+1)R_p$. (In particular $T_{p,p^2} = T_{1,p}T_{p,p} - (p^2+p+1)R_p$.)

As for $T_{1,p}T_{1,p^2}$, suppose we have $L'$ with $L'' \subseteq_{1,p} L' \subseteq_{1,p^2} L$. Then $L/L''$ is isomorphic to $\mathbb{Z}/p^3$ or $\mathbb{Z}/p\times\mathbb{Z}/p^2$. (It cannot be $(\mathbb{Z}/p)^3$ as it has a cyclic quotient of order $p^2$.) In the former case there is a unique intermediate $L'$; in the latter case there are $p$ intermediate $L'$ such that $L/L'$ is cyclic of order $p^2$. Thus $T_{1,p}T_{1,p^2} = T_{1,p^3} + pT_{p,p^2}$. From this we conclude that

$$T_{1,p^3} = T_{1,p}T_{1,p^2} - pT_{p,p^2} = T_{1,p}^3 - (p+1)T_{1,p}T_{p,p} - pT_{1,p}T_{p,p} + p(p^2+p+1)R_p.$$

In fact, one can show that every $T_{a,b}$ is a polynomial in $T_{(1,p)}$, $T_{(p,p)}$ and $R_p$ as $p$ varies, and these operators all commute!