MA4H9 Modular Forms: Problem Sheet 2 – Solutions

David Loeffler

December 3, 2010

This is the second of 3 problem sheets, each of which amounts to 5% of your final mark for the course. This problem sheet will be marked out of a total of 40; the number of marks available for each question is indicated. See the end of the sheet for some formulae that you may quote without proof.

You should hand in your work to the Undergraduate Office by ***3pm on Friday 3rd December****.*

1. [4 points] Let p be prime and $\tau \in \mathcal{H}$. Prove that the subgroups of $\mathbb{Z} + \mathbb{Z}\tau$ of index p are $p\mathbb{Z} + (\tau + j)\mathbb{Z}$, for $j = 0, \dots, p-1$, and $\mathbb{Z} + p\tau\mathbb{Z}$. Show that there are $p^2 + p + 1$ subgroups of index p^2, and give a list of these.

Solution: Let $\Lambda = \mathbb{Z} + \mathbb{Z}\tau$ and let Λ' be a subgroup of index p. Then $p\Lambda \subset \Lambda'$, and Λ' is determined by its image in $\Lambda/p\Lambda \cong (\mathbb{Z}/p\mathbb{Z})^2$, which is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^2$ of order p. There are two possibilities: either it is the subgroup generated by $(1, 0)$, or it contains a vector (a, b) with $b \neq 0$, in which case it also contains a vector of the form $(j, 1)$, and the value of j determines the subgroup uniquely. This gives the list of $j + 1$ possibilities above.

For subgroups of index p^2, the image of Λ' in $\Lambda'/p^2\Lambda \cong (\mathbb{Z}/p^2\mathbb{Z})^2$ is a subgroup of order p^2. This is either cyclic of order p^2, or isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$; the latter can only occur if $\Lambda' = p\Lambda$, since $(\mathbb{Z}/p^2\mathbb{Z})^2$ has only p^2 elements that are killed by p. So we must find $p^2 + p$ cyclic subgroups of order p^2 in $(\mathbb{Z}/p^2\mathbb{Z})^2$. The subgroup generated by $(j, 1)$ is cyclic of order p^2 for any j, and these are all distinct; this gives p^2 examples.

We also have subgroups of the form (j, p) with j invertible modulo p^2, but these are not all distinct, since $(1 + p) \cdot (j, p) = ((1 + p)j, p)$; using this relation, one may take the generator to be (j, p) with $1 \leq j \leq p - 1$, and this gives another $p - 1$ possibilities. Finally, there is the subgroup generated by $(1, 0)$.

These correspond to the lattices

$$\begin{gathered} p\mathbb{Z} + p\tau\mathbb{Z}, \\ p^2\mathbb{Z} + (\tau + j)\mathbb{Z} \quad (\text{for } 0 \leq j \leq p^2 - 1), \\ p^2\mathbb{Z} + (p\tau + j)\mathbb{Z} \quad (\text{for } 1 \leq j \leq p - 1), \\ \mathbb{Z} + p^2\tau\mathbb{Z}. \end{gathered}$$

(Note that there are other equally good choices of bases for these lattices.)

2. [4 points] Let p be prime and $j \geq 1$, and suppose $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ has q-expansion $\sum_{n \geq 0} a_n q^n$. Give a proof of the formula in Lemma 1.6.10,

$$T_{p^j}(f) = \left(\sum_{n \geq 0} a_{np^j} q^n \right) + p^{k-1} \left(\sum_{n \geq 0} a_{np^{j-1}} q^{np} \right) + \cdots + p^{j(k-1)} \left(\sum_{n \geq 0} a_n q^{p^j n} \right).$$

(Hint: Consider the operators U, V on the ring $\mathbb{C}[[q]]$ of formal power series defined by $U\left(\sum a_n q^n\right) = \sum a_{np} q^n$, $V\left(\sum a_n q^n\right) = p^{k-1} \sum a_n q^{np}$.)

Solution: The claim to be proven is that

$$T_{p^j}(f) = (U^j + VU^{j-1} + \cdots + V^{j-1}U + V^j)(f).$$

This is clear for $j = 0$ and $j = 1$. For $j \geq 2$ we have the following identity of operators:

$$T_{p^j} = T_p T_{p^{j-1}} - p^{k-1} T_{p^{j-2}} = (U + V)T_{p^{j-1}} - UVT_{p^{j-2}}.$$

If we assume the claim for $j-1$ and $j-2$, this is

$$(U+V)(U^{j-1} + VU^{j-2} + \cdots + V^{j-2}U + V^{j-1}) - UV(U^{j-2} + VU^{j-3} + \cdots + V^{j-3}U + V^{j-2})$$

which expands to

$$(U^j + UVU^{j-2} + UV^2U^{j-3} + \cdots + UV^{j-1}) + (VU^{j-1} + V^2U^{j-2} + \cdots + V^j) \\ - (UVU^{j-2} + UV^2U^{j-3} + \cdots + UV^{j-1}).$$

The terms in the first bracket all cancel with the terms in the last bracket except U^j, so the formula holds for j. Thus it is true for all j by induction.

3. [5 points] Let f be a normalised eigenform in $M_k(\mathrm{SL}_2(\mathbb{Z}))$ and p a prime. Let α and β be the roots of the polynomial $X^2 - a_p(f)X + p^{k-1}$.

   (a) Show that $a_{p^r}(f) = \alpha^r + \alpha^{r-1}\beta + \cdots + \alpha\beta^{r-1} + \beta^r$ for all $r \geq 0$.

   Solution: Let us write a_n for $a_n(f)$. The formula given is clearly valid for $r = 1$ and $r = 2$. Let us suppose that it holds for $r-1$ and $r-2$. Note that $\alpha + \beta = a_p(f)$ and $\alpha\beta = p^{k-1}$. Hence

   $$\begin{aligned} a_{p^r}(f) &= a_p a_{p^r} - p^{k-1} a_{p^{r-1}} \\ &= (\alpha+\beta)(\alpha^{r-1} + \cdots + \beta^{r-1}) - \alpha\beta(\alpha^{r-2} + \cdots + \beta^{r-2}) \end{aligned}$$

   This expression is clearly a sum of terms $\alpha^p\beta^q$ for pairs (s,t) with $s+t = r$. The pairs $(r,0)$ and $(0,r)$ appear once in the first bracket and not at all in the second bracket; all other pairs (p,q) appear twice in the first bracket and once in the second. Hence each term appears exactly once in the sum, so the formula is valid for r. Hence it is valid for all $r \geq 1$ by induction (and for $r = 0$ also, if we are careful in how we interpret the expression.)

   (b) Show that if $|a_p(f)| \leq 2p^{(k-1)/2}$, then $|\alpha| = |\beta| = p^{(k-1)/2}$.

   Solution: If this is the case, then $\alpha, \beta = \frac{a_p \pm i\sqrt{\Delta}}{2}$ where $\Delta = 4p^{k-1} - a_p^2 \geq 0$. Hence α, β are complex conjugates of each other, and in particular have the same absolute value. As their product is p^{k-1}, this common absolute value is $p^{(k-1)/2}$.

   (c) Show that if the hypothesis of part (b) holds, then $a_{p^r}(f) \leq (r+1)p^{r(k-1)/2}$ for all $r \geq 0$.

   Solution: If $|\alpha| = |\beta| = p^{(k-1)/2}$, then for any s, t with $s + t = r$, we have $|\alpha^s\beta^t| = p^{r(k-1)/2}$. Hence a sum of $(r+1)$ terms of this form has absolute value at most $(r+1)p^{r(k-1)/2}$, by repeated application of the triangle inequality.

   (d) Deduce that if the hypothesis of part (b) holds for all primes p, then $a_n(f) \leq d(n)n^{(k-1)/2}$ for all $n \in \mathbb{N}$, where $d(n) = \sigma_0(n)$ is the number of divisors of n.

Solution: Since both a_n and $d(n)n^{(k-1)/2}$ are functions of n that are multiplicative for coprime arguments, this follows from the case of n a prime power, which is part (c).

4. [4 points] Calculate the matrix of the Hecke operator T_2 acting on $S_{32}(\mathrm{SL}_2(\mathbb{Z}))$ (in a basis of your choice). Show that its characteristic polynomial is $x^2 - 39960x - 2235350016$. *(Hint: Use a computer to do the algebra!)*

Solution: A natural choice of basis is $f_1 = \Delta E_4^5$ and $f_2 = \Delta^2 E_4^2$. Computing the q-expansions up to degree q^4, we have

$$f_1 = q + 1176q^2 + 558252q^3 + 134859328q^4 + \dots$$
$$f_2 = q^2 + 432q^3 + 39960q^4 + \dots$$

Hence

$$T_2(f_1) = (1176q + 134859328q^2 + \dots) + 2^{31}(q^2 + \dots) = 1176q + 2282342976q^2 + \dots$$
$$T_2(f_2) = (q + 39960q^2 + \dots) + 2^{31}(q^4 + \dots) = q + 39960q^2 + \dots.$$

We deduce that $T_2(f_1) = 1176f_1 + 2280960000f_2$ and $T_2(f_2) = f_1 + 38784f_2$, so the matrix of T_2 is

$$\begin{pmatrix} 1176 & 1 \\ 2280960000 & 38784 \end{pmatrix}.$$

which does indeed have the stated characteristic polynomial. (Other choices of basis would, of course, give different matrices, but the same characteristic polynomial.)

5. [5 points] Let $N \geq 2$ and let $c, d \in \mathbb{Z}/N\mathbb{Z}$. We say that c and d are *coprime modulo* N if there is no $f \neq 0$ in $\mathbb{Z}/N\mathbb{Z}$ such that $fc = fd = 0$.

   (a) Show that if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, then c and d are coprime modulo N.

   Solution: Suppose $fc = fd = 0$ for some $f \in \mathbb{Z}/N\mathbb{Z}$. Then $f = f(ad - bc) = a(fd) - b(fc) = 0$, so f must be zero. Thus c and d are coprime mod N.

   (b) Show that for any pair (c, d) that are coprime modulo N, there exist $c', d' \in \mathbb{Z}$ such that $c' = c$ and $d' = d \pmod N$ and $\mathrm{HCF}(c', d') = 1$.

   Solution: Choose an arbitrary lift of c and d to $\mathbb{Z}$, and assume WLOG that $d \neq 0$. Let p be a prime dividing d. Then p cannot divide both N and c, since otherwise N/p would kill both c and d modulo N. For each such p, there exist λ_p such that $c + \lambda_p N$ is not divisible by p: if $p \nmid c$, we take $\lambda_p = 0$, and if $p \mid c$, then we can take $\lambda_p = 1$. By the Chinese remainder theorem we can find a $\lambda \in \mathbb{Z}$ such that $\lambda = \lambda_p \bmod p$ for each of the finitely many primes p dividing d. Then no prime can divide both $c + \lambda N$ and d, so $(c', d') = (c + \lambda N, d)$ is a coprime pair congruent to (c, d) modulo N.

   (c) Hence (or otherwise) show that the natural reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective for any $n \geq 2$.

   Solution: Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. By the previous part, we can find a lifting of c and d to a coprime pair of integers. Let us choose arbitrary lifts of a, b, and consider the matrix

$$\begin{pmatrix} a + \lambda N & b + \mu N \\ c & d \end{pmatrix}.$$

This has determinant $(ad - bc) + N(\lambda d - \mu c)$. Since $ad - bc = 1 \pmod N$, and c, d are coprime, we can find λ, μ such that $(ad - bc) + N(\lambda d - \mu c) = 1$. This gives a lifting of the original matrix to $\mathrm{SL}_2(\mathbb{Z})$.

(d) Give an example of an integer N and an element of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ which is not in the image of $\mathrm{GL}_2(\mathbb{Z})$.

Solution: Any element of $\mathrm{GL}_2(\mathbb{Z})$ has determinant ± 1, so its image modulo N has determinant $\pm 1 \pmod N$. So the matrix $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$ is not in the image of reduction.

6. [4 points] The *Sanov subgroup* of $\mathrm{SL}_2(\mathbb{Z})$ is the set S of all matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a = d = 1 \pmod 4$ and $b = c = 0 \pmod 2$.

(a) Show that S is indeed a subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Solution: Easy check. If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in S$, then $\gamma^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ is clearly in S. If γ' is another element of S, $\gamma\gamma' = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}$, and $ab' + bd'$ is even (because b and b' are) and $aa' + bc'$ is $1 \pmod 4$ (because $a = a' = 1 \pmod 4$, and bc' is a product of two even numbers and hence $0 \pmod 4$) and similarly for the other entries.
(Note that S is conjugate in $\mathrm{SL}_2(\mathbb{R})$, but not in $\mathrm{SL}_2(\mathbb{Z})$, to $\Gamma_1(4)$.)

(b) Show that S is a congruence subgroup, and determine its level.

Solution: S visibly contains $\Gamma(4)$, and it doesn't contain $\Gamma(2)$, so its level is 4.

(c) Show that S has index 12 in $\mathrm{SL}_2(\mathbb{Z})$.

Solution: This can be done by brute force, but it is easier to note that S is contained in $\Gamma(2)$, which has index $|\mathrm{SL}_2(\mathbb{F}_2)| = 6$ by the previous question; and S clearly has index 2 in $\Gamma(2)$, since if $\gamma \in \Gamma(2)$ then exactly one of γ and $-\gamma$ is in S.

7. [1 point] Show that $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ for any $N \geq 1$.

Solution: It's easy to see that the map $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$ mapping $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $d \pmod N$ is a group homomorphism, and its kernel is $\Gamma_1(N)$.

8. [3 points] Let Γ be an odd subgroup of $\mathrm{SL}_2(\mathbb{Z})$ (that is, $-1 \neq \Gamma$).

(a) Show that the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ is even.

Solution: Clearly we have $[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}] \in \mathbb{Z}$, and since Γ is odd, $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] = 2[\mathrm{PSL}_2(\mathbb{Z}) : \overline{\Gamma}]$.

(b) Show that there is no odd subgroup of index 2.

Solution: By elementary group theory, any subgroup of index 2 is normal. Hence it is the kernel of a homomorphism to $\{\pm 1\}$. Since $-1 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2$, the image of -1 in $\{\pm 1\}$ must be 1, so it is in Γ.

9. [3 points] Let f be a modular function of level $\mathrm{SL}_2(\mathbb{Z})$ (and some weight k) and let p be prime. Show that $f(pz)$ is a modular function of level $\Gamma_0(p)$, and calculate $v_{\Gamma_0(p),c}(f(pz))$ for the two cusps $c \in C(\Gamma_0(p))$. Hence show that $f(pz)$ is a modular form or cusp form if and only if f is.

Solution: Let f_p be the function $z \mapsto f(pz)$, for clarity of notation. We showed in class that f_p is weakly modular of level $\Gamma_0(p)$, so we need only check that it is meromorphic at the cusps. Recall that the cusps of $\Gamma_0(p)$ are ∞ and 0, with widths respectively 1 and p.

For ∞, we note that if $f(z) = \sum a_n q^n$, then $f_p(z) = f(pz) = \sum a_n q^{np}$. Thus $v_{\Gamma_0(p),\infty}(f_p) = p \cdot v_{\mathrm{SL}_2(\mathbb{Z}),\infty}(f)$.

To get the remaining term, we use the matrix $g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. We have $(f_p \mid_k g)(z) = z^{-k} f(-p/z) = z^{-k}(z/p)^k f(z/p) = p^{-k} \sum_n a_n (q_p)^n$, where $q_p = q^{1/p} = e^{2\pi i z/p}$. So we have $v_{\Gamma_0(p),0}(f_p) = v_{\mathrm{SL}_2(\mathbb{Z}),\infty}(f)$.

These are both obviously ≥ 0 or > 0 if and only if $v_{\mathrm{SL}_2(\mathbb{Z}),\infty}(f)$ is so, hence f_p is a cusp form or modular form if and only if f is so.

10. [2 points] Let $p \geq 3$ be prime. Show that for each cusp $c \in C(\Gamma_0(p))$, there are $\frac{p-1}{2}$ distinct cusps in $C(\Gamma_1(p))$ which are equivalent to c in $C(\Gamma_0(p))$.

Solution: Recall that $\Gamma_0(p)$ has just 2 cusps, ∞ and 0, and

$$\sum_{\substack{d \in C(\Gamma_1(p)) \\ d = c \in C(\Gamma_0(p))}} h_{\Gamma_1(p)}(d) = \left(\frac{d_{\Gamma_1(p)}}{d_{\Gamma_0(p)}} \right) h_{\Gamma_0(p)}(c).$$

Moreover, since $\Gamma_1(p)$ is normal in $\Gamma_0(p)$, for each $c \in C(\Gamma_0(p))$ all cusps of $\Gamma_1(p)$ equivalent to c have the same width. For the cusp ∞, we compute that $h_{\Gamma_1(p)}(\infty) = h_{\Gamma_0(p)}(\infty) = 1$; so every term on the left-hand side is 1, and their sum is

$$\frac{d_{\Gamma_1(p)}}{d_{\Gamma_0(p)}} = [\overline{\Gamma_0(p)} : \overline{\Gamma_1(p)}] = \tfrac{1}{2}[\Gamma_0(p) : \Gamma_1(p)] = \frac{p-1}{2}$$

(the $\frac{1}{2}$ because $\Gamma_0(p)$ is even and $\Gamma_1(p)$ is odd). So there are $\frac{p-1}{2}$ terms in the sum. Similarly, the cusp 0 has width p for both $\Gamma_0(p)$ and $\Gamma_1(p)$, so there are $\frac{p-1}{2}$ cusps of $\Gamma_1(p)$ that are $\Gamma_0(p)$-equivalent to 0 as well.

11. [2 points] Show that $\frac{1}{2}$ is an irregular cusp of $\Gamma_1(4)$, and calculate its width.

Solution: Let $\Gamma = \Gamma_1(4)$ and let g be the matrix $\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}$, so $g\infty = c = \frac{1}{2}$. We have $\pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma_c = P_\infty \cap g^{-1}\Gamma g$ if and only if $\pm g \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} g^{-1} \in \Gamma$. We calculate that

$$\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 1-2h & h \\ -4h & 1+2h \end{pmatrix}.$$

If $h = 1$ this is $\begin{pmatrix} -1 & 1 \\ -4 & 3 \end{pmatrix}$, which does not lie in $\Gamma_1(4)$, but its negative does. So $\frac{1}{2}$ is an irregular cusp, of width 1.
(It can be shown that all cusps of $\Gamma_1(N)$ are regular for any $N \neq 4$.)

12. [3 points] Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$, and let $g \in \mathrm{SL}_2(\mathbb{Z})$. Show that gi has nontrivial stabiliser in $\overline{\Gamma}$ if and only if $\pm g \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} g^{-1} \in \overline{\Gamma}$. Hence show that there exist points $z \in \mathcal{H}$ with $n_{\Gamma_0(N)}(z) = 2$ if and only if -1 is a square modulo N.

Solution: Since $\mathrm{Stab}_{\mathrm{PSL}_2(\mathbb{Z})}$ is the group of order 2 generated by $\pm \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\mathrm{Stab}_{\mathrm{PSL}_2(\mathbb{Z})}(gi)$ is the group of order 2 generated by $g \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} g^{-1}$. So gi stabiliser of order 2 in $\overline{\Gamma}$ if and only if $g \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} g^{-1} \in \overline{\Gamma}$; and any point of $\mathcal{H}$ that is not in the orbit of i has stabiliser in $\mathrm{PSL}_2(\mathbb{Z})$ of order 1 or 3, so it certainly cannot have stabiliser of order 2 in $\overline{\Gamma}$.

We calculate that for $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we have

$$g \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} g^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad+bc & -(a^2+b^2) \\ c^2+d^2 & -(ad+bc) \end{pmatrix}.$$

This lies in $\overline{\Gamma_0(N)}$ if and only if $c^2 + d^2 = 0 \bmod N$. I claim that if such a g exists, then both c and d are units mod N; this follows from the fact that no prime can divide both of c and d, and if $p \mid c$ and $p \mid N$, then $p \mid N - c^2 = d^2$, so $p \mid d$. Hence c^{-1} is defined mod N, and $(c^{-1}d)^2 = -1 \bmod N$. Conversely, if there is $x \in \mathbb{Z}$ such that $x^2 = -1 \bmod N$, then we can find $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ with $c = x$ and $d = 1 \bmod N$, and gi then has nontrivial stabiliser.

13. *(Non-assessed and for amusement only – I don't know the answer to this one)* Does there exist a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$ for which every cusp is irregular?

Solution: I still don't know the answer to this one.