MODULAR FORMS: EXAMPLE SHEET 1 – HINTS AND OUTLINE SOLUTIONS

DAVID LOEFFLER

Some of these solutions are based on the solutions that various brave audience members showed us in the examples class. Thanks to everyone who volunteered solutions and comments.

Exercises

Question 1. *Show that the action of* $\mathrm{SL}_2(\mathbb{R})$ *on* $\mathcal{H}$ *is transitive, and the stabiliser of* i *is the group* $\mathrm{SO}_2(\mathbb{R})$. *(Thus* $\mathcal{H}$ *is a quotient of the semisimple real Lie group* $\mathrm{SL}_2(\mathbb{R})$ *by a maximal compact subgroup.)*

Solution. To show transitivity: it is enough to show that for any $z \in \mathcal{H}$, there is some $\gamma \in \mathrm{SL}_2(\mathbb{R})$ such that $\gamma(i) = z$. But we showed this (in fact rather more than this) in Lemma 2.2.3. As for the stabiliser: since $\begin{pmatrix} a & b \\ c & d \end{pmatrix} i = \frac{(ac+bd)+(ad-bc)i}{c^2+d^2}$, if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Stab}_{SL_2(\mathbb{R})}(i)$, then $c^2 + d^2 = 1$ and $ac + bd = 0$. Together with $ad - bc = 1$, this implies that $a^2 + b^2 = 1$ and $ab + cd = 0$, so $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & c \\ b & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. □

Question 2. *Let* $\mathcal{L}$ *be the ring of holomorphic functions on* $\mathcal{H}$*, with the usual (weight 0) action of* $\mathrm{SL}_2(\mathbb{R})$. *Show that the function* $j_k : \mathrm{SL}_2(\mathbb{R}) \times \mathcal{H} \to \mathbb{C}$ *defined by* $j(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, z) = (cz + d)^k$ *satisfies*

$$j_k(\gamma_1\gamma_2, z) = j_k(\gamma_1, \gamma_2 z) \cdot j_k(\gamma_2, z).$$

Deduce that the weight k *action on* $\mathcal{L}$ *defined in lectures really is a right action, i.e.*

$$f|_k(\gamma_1\gamma_2) = (f|_k\gamma_1)|_k\gamma_2.$$

Solution. Elementary check. □

Question 3. *Complete the proof of Theorem 1.2.2 by showing that if* $z, z' \in \mathcal{D}$ *and* $\gamma z = z'$ *for some* $\gamma \in G = \mathrm{PSL}_2(\mathbb{Z})$ *with* $\gamma \neq 1$*, then one of the following holds:* $\mathrm{Re}\, z = \pm\frac{1}{2}$ *and* $\gamma = \begin{pmatrix} 1 & \mp 1 \\ 0 & 1 \end{pmatrix}$*;* $|z| = 1$ *and* $\gamma = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$*;* $z = z' = i$*; or* z *and* z' *are in the set* $\{\rho, 1 + \rho\}$ *where* ρ *is a cube root of unity. Find the elements of* $\mathrm{Stab}_G(i)$ *and* $\mathrm{Stab}_G(\rho)$*, and verify that they have order 2 and 3 respectively.*

Solution. It is helpful to draw the following diagram, illustrating the images of points in $\mathcal{D}$ under various elements of $\mathrm{PSL}_2(\mathbb{Z})$ with small coefficients.

We do not know *yet* that this is a tesselation – there could be some nasty $\gamma \in \mathrm{PSL}_2(\mathbb{Z})$ that maps $\mathcal{D}$ onto something overlapping itself – but it is easy to check that the transformations labelled on the graph above send $\mathcal{D}$ to the regions marked.

Now suppose we have γ, z, z' as above. Without loss of generality, we assume that $\operatorname{Im} z' \geq \operatorname{Im} z$. Then if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, we have $|cz + d| \leq 1$. If $z \in \mathcal{D}$, then $\operatorname{Im} z \geq \frac{\sqrt{3}}{2}$, so we must have $|c| < 2$. Thus $c = 0$ or $c = \pm 1$, and in each case it is clear that we must have $|d| < 2$ also.

It is easily seen that for each pair $c, d \in \mathbb{Z}$ with $\gcd(c, d) = 1$, the elements of $\mathrm{SL}_2(\mathbb{Z})$ with this as their bottom row correspond to transformations of the form $z \mapsto \gamma_0(z) + r$ for fixed γ_0 and varying integers $r \in \mathbb{Z}$.

Since -1 acts trivially, without loss of generality we may assume that either $c > 0$, or $c = 0$ and $d > 0$. Thus we must check the cases $(1, 0)$, $(1, \pm 1)$, and $(0, 1)$, and γ must be a translate of one of the transformations labelled above; and the only translates of the transformations labelled that have nonzero intersection with $\mathcal{D}$ are the labelled transformations themselves.

Now it is clear from the diagram that we have 9 possible cases where $\gamma\mathcal{D}$ and $\mathcal{D}$ have nontrivial intersection (corresponding to the 9 regions adjoining $\mathcal{D}$); in each case the overlap is contained in the boundary of $\mathcal{D}$; and for all but 3 of these the overlap is a point. For these 6 cases, either the overlap gives us an element γ with $\gamma\rho = 1 + \rho$, or an element with $\gamma(1 + \rho) = \rho$, or an element of the stabiliser of ρ or $1 + \rho$.

In particular, if $\gamma \in \mathrm{Stab}_{\mathrm{PSL}_2 \mathbb{Z}}(i)$, then γ must be either 1 or $z \mapsto \frac{-1}{z}$; while if $\gamma \in \mathrm{Stab}_{\mathrm{PSL}_2 \mathbb{Z}}\, \rho$, γ must be either the identity or one of the list of 6 elements studied above, and only two of them work. (The 6 elements are the 2 nontrivial elements of the stabiliser of each of ρ and $1 + \rho$, and 2 elements that send ρ to $1 + \rho$, and 2 that do the opposite.) □

Question 4. *Express* $\begin{pmatrix} 70 & 213 \\ 23 & 70 \end{pmatrix}$ *in terms of the generators* $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *and* $b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *of* $\mathrm{SL}_2(\mathbb{Z})$*.*

Solution. Use an iterative process: begin with the given matrix and multiply it on the right by a^{-1} – this subtracts a copy of the first column from the second. If we repeat the process of doing this until the bottom right entry is smaller than the bottom left one, then then multiply (again on the right) by b to swap the columns, then we are essentially performing Euclid's algorithm on the elements of the bottom row.

Since the original matrix was in $\mathrm{SL}_2(\mathbb{Z})$, the entries of the bottom row are coprime, so we must terminate with the bottom row being $(0, \pm 1)$. Since we never leave $\mathrm{SL}_2(\mathbb{Z})$, the top row must now be $(\pm 1, n)$ for some $n \in \mathbb{Z}$, and this is clearly in the subgroup generated by a and $b^2 = -1$. We have thus expressed the given matrix as a product of elements of $\mathrm{SL}_2(\mathbb{Z})$. In this case, if m is the given matrix, we find that $m = b^2 a^3 b a^{-23} b a^3$. □

Question 5. *Show that for* $k \geq 4$ *the sum defining the Eisenstein series* G_k*,*

$$G_k(z) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(m + nz)^k}$$

is absolutely convergent, locally uniformly in z*. Deduce that* $G_k(z)$ *is holomorphic and independent of the order of summation.*

Solution. Assume $\operatorname{Im} z > \epsilon$ for some $\epsilon > 0$; any compact subset of $\mathcal{H}$ is certainly contained in such a set.

Let us separate the terms into those with $n = 0$ and those with $n \neq 0$.

The $n = 0$ sum is just twice the usual series for $\zeta(k)$, independent of z which is clearly absolutely convergent (by the integral test, if you like).

The $n \neq 0$ sum is slightly more delicate. Let $w \in \mathcal{H}$ with $\operatorname{Im} w > \epsilon$ and consider

$$\sum_{m \in \mathbb{Z}} |m + w|^{-k}.$$

We note that $|m + w| \geq \min(|m + \operatorname{Re} w|, \operatorname{Im} w)$. The sum of this latter expression over $\mathbb{Z}$ splits into two sub-sums: the sum over terms where $\operatorname{Im} w$ dominates has $\leq 2 \operatorname{Im} w$ terms each equal to $(\operatorname{Im} w)^{-k}$, while the sum over the remaining terms is likewise bounded above by $C(\operatorname{Im} w)^{1-k}$ for some constant C depending only on ϵ, by comparison with an integral. Thus there is a constant C' (likewise depending only on ϵ) such that if $\operatorname{Im} w > \epsilon$ is at least some limit depending on C') we have $\sum_{m \in \mathbb{Z}} |m + w|^{-k} \leq C'(\operatorname{Im} w)^{1-k}$.

Hence the sum $\sum_{n\in\mathbb{Z},n\neq 0}\sum_{m\in\mathbb{Z}}|m+nz|^{-k}$ is convergent, uniformly in z in any region of the form $\{z\in\mathcal{H}|\operatorname{Im} z>\epsilon\}$, for any real number $k>2$, by comparison with the Riemann zeta function, which clearly implies what we need. (This argument actually proves slightly more: it shows that G_k is bounded as $\operatorname{Im} z\to\infty$, which implies that G_k is holomorphic at infinity.) □

Question 6. *Show that E_6 has a single simple zero at i, and E_4 a single simple zero at ρ where ρ is a cube root of unity; and neither has any other zeroes.*

Solution. Immediate from the valence formula. (One can prove independently that any modular form of weight not divisible by 4 must vanish at i, and any modular form of weight not divisible by 6 must vanish at ρ, since the corresponding lattices satisfy $L=iL$ and $L=\rho L$ respectively; but it is not clear from this that the zeros must be simple for E_4 and E_6.) □

Question 7. *Let f be a nonzero modular function of weight k. For simplicity, assume f has no zeros on the boundary of the fundamental domain $\mathcal{D}$, except possibly at the points i, ρ, $1+\rho$. Note that $\frac{\mathrm{d}f}{f}$ is a meromorphic differential on $\mathcal{H}$ with a simple pole at each zero or pole of f, with residue at z equal to $\operatorname{ord}_z f$. Consider the contour $\mathcal{C}$ illustrated below:*

Deduce the valence formula by finding the limit of the integral $\oint_{\mathcal{C}}\frac{\mathrm{d}f}{f}$ (as the height of the top horizontal line tends to ∞ and the radius of the three small arcs tends to zero) in two ways, first by using the residue theorem, and secondly by splitting up the integral into its component arcs.

Solution. Split the contour $\mathcal{C}$ into 8 arcs $\gamma_1\ldots\gamma_8$ as above. On the one hand, by the residue theorem

$$\oint_{\mathcal{C}}\omega=2\pi i\sum_{z\text{ inside }\mathcal{C}}\operatorname{Res}_z\omega=2\pi i\sum_{\substack{z\in\Gamma\backslash\mathcal{H}\\ z\neq i,\rho}}\operatorname{ord}_z f.$$

On the other hand, since $f(1+z)=f(z)$ it is clear that

$$\int_{\gamma_1}\omega+\int_{\gamma_3}\omega=0;$$

writing $\frac{f'(\rho+z)}{f(\rho+z)}=\sum_{n\geq -1}c_n z^n$ for some $c_n\in\mathbb{C}$, as the radius of the corner curves tends to 0 it is clear that

$$\int_{\gamma_4}\omega+\int_{\gamma_8}\omega=-\frac{2\pi i}{3}\operatorname{Res}_\rho\omega=-\frac{2\pi i}{3}\operatorname{ord}_\rho f$$

(with the minus sign being a consequence of traversing a negatively oriented arc), and similarly

$$\int_{\gamma_6}\omega=-\frac{2\pi i}{2}\operatorname{ord}_i f.$$

For the component near ∞, we use the substitution $q=e^{2\pi iz}$ to reduce the integral to

$$\int_{\mathcal{E}}\frac{f'(z(q))}{f(z(q))}\frac{\mathrm{d}z}{\mathrm{d}q}\mathrm{d}q$$

where $\mathcal{E}$ is a small circle around the origin in the q-plane, oriented clockwise; but if $f(z) = F(q)$, where F is meromorphic at 0, then $\frac{f'(z(q))}{f(z(q))}\frac{\mathrm{d}z}{\mathrm{d}q} = \frac{F'(q)}{F(q)}$ by the chain rule, so the integral reduces to

$$\int_{\mathcal{E}} \frac{F'(q)}{F(q)}\mathrm{d}q = -2\pi i \operatorname{ord}_0 F = -2\pi i \operatorname{ord}_\infty f.$$

So far k has made no appearance. The weight k magic, so to speak, is all in the integrals over γ_5 and γ_7. We make the change of variable $z = \frac{-1}{u}$ in the γ_7 integral.

$$\int_{\gamma_7} \frac{f'(z)}{f(z)}dz = -\int_{\gamma_5} \frac{f'(-1/u)}{f(-1/u)}\frac{\mathrm{d}z}{\mathrm{d}u}\mathrm{d}u.$$

(The minus sign is because the direction of the arc is reversed). We have $f(-1/u) = u^k f(u)$, and differentiating this, $1/u^2 f'(-1/u) = ku^{k-1}f(u) + u^k f'(u)$. Meanwhile $\frac{\mathrm{d}z}{\mathrm{d}u} = \frac{1}{u^2}$, so

$$\begin{aligned}\int_{\gamma_7} \omega &= \int_{\gamma_5} \frac{f'(-1/u)}{f(-1/u)} \cdot \frac{\mathrm{d}z}{\mathrm{d}u}\mathrm{d}u \\ &= \int_{\gamma_5} \frac{ku^{k+1}f(u) + u^{k+2}f'(u)}{u^k f(u)} \cdot \frac{1}{u^2}\mathrm{d}u \\ &= -k\int_{\gamma_5} \frac{\mathrm{d}u}{u} - \int_{\gamma_5} \frac{f'(u)}{f(u)}\mathrm{d}u \\ &= -k(\log i - \log \rho) - \int_{\gamma_5} \omega = \frac{2\pi i k}{12} - \int_{\gamma_5} \omega.\end{aligned}$$

(where we choose a branch of the logarithm so the branch cut doesn't cross γ_5).

So

$$\oint_{\mathcal{C}} \omega = 2\pi i \sum_{\substack{z \in \Gamma\backslash\mathcal{H} \\ z \ne i,\rho}} \operatorname{ord}_z f = 2\pi i \left(\frac{k}{12} - \frac{\operatorname{ord}_\rho f}{3} - \frac{\operatorname{ord}_i f}{2} - \operatorname{ord}_\infty f\right)$$

which is the valence formula. (Note that the restriction to f without poles on the boundary can clearly be dealt with, either by adding more semicircular arcs, or more subtly by multiplying by an appropriate rational function of j.) □

Question 8. *Give a careful proof of the claim made in the course of the proof of Prop 1.4.5: if L is a lattice in $\mathbb{C}$, and L' is a sublattice of index p^{n+1}, then the number of lattices L'' with $L \supset L'' \supset L'$ and $|L/L''| = p$ is $p+1$ if $L'' \subseteq pL$ and 1 otherwise.*

Solution. The structure theorem for finitely generated abelian groups states that any finitely generated abelian group is of the form

$$C_{d_1} \times C_{d_2} \times \cdots \times C_{d_k}$$

where C_n is the (additive) group $\mathbb{Z}/n\mathbb{Z}$ and the d_i are nonnegative integers with $d_i | d_{i+1}$.

Let us apply this to the finitely generated group L/L'. Lifting the generators of the cyclic factors of this finite group to elements of L, we deduce that L has a basis v_1, v_2 such that L' is the sublattice spanned by b_1v_1, b_2v_2 for two integers $v_1, v_2 \ge 0$ with $v_1|v_2$ and $v_1v_2 = p^{n+1}$.

It is clear that $L' \subseteq pL$ if and only if $v_1 > 1$. If this does hold, then any of the $p+1$ lattices L'' with $L \supset L'' \supset pL$ will do. If not, then clearly the only possibility is to take L'' to be the lattice spanned by v_1 and pv_2. □

Question 9. *Let $k = 24$. Calculate the q-expansions of a basis for the 3-dimensional space M_k, up to and including the q^6 term. Using the formulae for the Hecke operators in terms of q-expansions, compute the first 3 terms of the q-expansons of $T_2 f$ for each f in your basis, and hence find the matrix of T_2. Verify that the characteristic polynomial of T_2 is*

$$(x - 8388609)(x^2 - 1080x - 20468736).$$

(You will need a computer for this question. Feel free to do it how you like, but you might want to use the Sage worksheet linked from my web page.)

Solution. There are various bases for M_{24}. A natural choice is

$$\begin{aligned} F_0 = E_4^6 &= 1 + 1440q + 876960q^2 + 292072320q^3 + 57349833120q^4 + \dots \\ F_1 = E_4^3\Delta &= q + 696q^2 + 162252q^3 + 12831808q^4 + \dots \\ F_2 = \Delta^2 &= q^2 - 48q^3 + 1080q^4 + \dots \end{aligned}$$

We find that

$$\begin{aligned} F_0|_{24}T_2 &= 8388609F_0 - 12078720000F_1 + 1119744000000F_2 \\ F_1|_{24}T_2 &= 696F_1 + 20736000F_2 \\ F_2|_{24}T_2 &= F_1 + 384F_2 \end{aligned}$$

Although the Hecke algebra acts on the right, it's conventional to write matrices of linear operators on the left, so the matrix of T_2 in this basis would be

$$\begin{pmatrix} 8388609 & 0 & 0 \\ -12078720000 & 696 & 1 \\ 1119744000000 & 20736000 & 384 \end{pmatrix}.$$

This has the characteristic polynomial stated above. (Consequently the eigenforms in this example are defined over the splitting field of this polynomial, which is $\mathbb{Q}(\sqrt{p})$ where p is the rather elegant prime 144169. My PhD supervisor, teaching a course on p-adic modular forms, once pointed out that one can show for various theoretical reasons that the field which comes up here is a real quadratic field in which all primes $q < 23$ split, and it turns out that this is only the sixth smallest discriminant for which this occurs.) □

Question 10. *Show that if $k \geq 0$ is even, and $d = \dim M_k$, there are unique elements $f_0, \dots, f_{d-1}$ in M_k such that for $0 \leq i, j \leq d-1$, the coefficient of q^i in f_j is 1 if $i = j$ and 0 otherwise. Show also that the f_j are in $\mathbb{Z}[[q]]$, so they give a $\mathbb{Z}$-basis for the module of weight k modular forms with integral coefficients. (This basis is called the Victor Miller basis). Compute the first 5 terms of the q-expansion of each function in the Victor Miller basis for M_{24}.*

Solution. In this question, you are allowed to assume that Δ has integral coefficients. Now, we know that (by choosing various products of powers of E_4, E_6 and Δ, as in the previous question) we can always choose a basis $F_0, \dots, F_{d-1}$ such that $F_i \in q^i + q^{i+1}\mathbb{Z}[[q]]$.

We construct a new basis $f_0, \dots, f_d$ in the obvious way. Starting with F_0, we subtract an integer multiple of F_1 to kill its linear term, an integer multiple of F_2 to kill its q^2 term, and so on up to the q^{d-1} term. Call this f_0. Now we do the same treatment starting with F_1, killing terms from q^2 up to q^{d-1}, and call this f_1; and keep going until we have killed the coefficients of $q^1, \dots, q^{d-1}$.

(If one thinks of the q-expansions as the rows of matrix with d rows and ∞ columns, in some sense, then the F_i's are already in row echelon form, and we are transforming this into a reduced row echelon form, without losing integrality since all of the pivots are 1.)

For $k = 24$, if we start with the functions F_0, F_1, F_2 above, we find that

$$\begin{aligned} f_0 &= F_0 - 1440F_1 + 125280F_2 = 1 + 52416000q^3 + O(q^4) \\ f_1 &= F_1 - 696F_2 = q + 195660q^3 + O(q^4) \\ f_2 &= F_2 = q^2 - 48q^3 + O(q^4) \end{aligned}$$

I apologise if anyone thought I wanted the first five nonzero terms! I only wanted you to calculate the first nonobvious coefficient of each function in the VM basis. □

Question 11. *Show that the index of $\Gamma(N)$ in $\mathrm{SL}_2(\mathbb{Z})$ is*

$$N^3 \prod_{\substack{p|N \\ p \text{ prime}}} \left(1 - \frac{1}{p^2}\right).$$

Find similar formulae for $\Gamma_0(N)$ and $\Gamma_1(N)$.

Solution. We need the following useful lemma: the reduction map from $\mathrm{SL}_2(\mathbb{Z})$ to $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ is surjective for all N. This is known as the Strong Approximation Theorem for SL_2. I won't give a proof as this is part of a question on the second example sheet; suffice to say that it is false for GL_2, as I pointed out in the examples class.

Given the lemma, it is clear that $\Gamma(N)$ is exactly the kernel of the map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, so its index is exactly the size of $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Using the Chinese Remainder Theorem, both $N \mapsto |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})|$ and $N \mapsto N^3 \prod_{p|N}\left(1 - \frac{1}{p^2}\right)$ are weakly multiplicative functions of N (i.e. multiplicative for coprime arguments), so it is enough to check it for prime powers.

There are p^{2e} ways to choose the first column of a 2×2 matrix over $\mathbb{Z}/p^e\mathbb{Z}$, but p^{2e-2} are multiples of p. The others all do appear as the first column of some element of $\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$, since given any two integers in $\mathbb{Z}/p^e\mathbb{Z}$ which are not both multiples of p, we can lift them to coprime integers in $\mathbb{Z}$, and the result for $\mathbb{Z}$ is standard. So there are $p^{2e} - p^{2e-2}$ ways to pick the first column. For each of these first columns, the determinant map is a linear function of the entries of the second column; its image contains 1, by assumption, so its image is all of $\mathbb{Z}/p^e\mathbb{Z}$; hence the set of possible second columns giving determinant 1 has size p^e. Thus $|\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z}) = p^e(p^{2e} - p^{2e-2})$ as required.

Alternatively, as Barinder showed us in the examples class, one can easily see that $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ has order $(p^2-1)(p^2-p)$; SL_2 is the kernel of the surjective determinant homomorphism to $(\mathbb{Z}/p\mathbb{Z})^\times$, so $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$ has order $\frac{(p^2-1)(p^2-p)}{|(\mathbb{Z}/p\mathbb{Z})^\times|} = p^3 - p$; and for all $e \geq 1$, the natural homomorphism $\mathrm{SL}_2(\mathbb{Z}/p^{e+1}\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$ has kernel $1 + p^e R$ where R is the set of matrices over $\mathbb{Z}/p\mathbb{Z}$ with trace 0. Since R clearly has size p^3, this proves our result. The reason this works is essentially because the derivative of the determinant function at the identity matrix is the trace function, so for any 2×2 matrix M over $\mathbb{Z}$, $\det(1 + p^e M) = 1 + p^e \operatorname{Tr} M \bmod p^{2e}$.

One checks similarly that

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$$
$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)] = N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$$

□

Question 12. *Show that for any prime p, $\Gamma_0(p)$ has exactly 2 cusps. What can you say about $\Gamma_1(p)$?*

Solution. We note that for any $r, s \in \mathbb{Z}$ with $\gcd(r, s) = 1$, there exists $u, v \in \mathbb{Z}$ such that $\begin{pmatrix} r & u \\ s & v \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. This is a restatement of the standard fact that we can find u, v with $sv - ru = 1$.

It's clear that for $\gamma = \begin{pmatrix} a & b \\ pc & d \end{pmatrix} \in \Gamma_0(p)$, $\Gamma(\infty) = \frac{a}{pc}$ where a is invertible modulo p. Conversely if $\frac{r}{s} \in \mathbb{Q}$ is in lowest terms and $p|s$, then we can find an element of $\Gamma_0(p)$ which has first column $\begin{pmatrix} r \\ s \end{pmatrix}$

It's clear that 0 is not in this orbit. So let's show that if $\frac{r}{s} \in \mathbb{Q}$ is in lowest terms with $p \nmid s$, $\frac{r}{s}$ is in the orbit of 0. We use the above observation to construct an element of $\mathrm{SL}_2(\mathbb{Z})$ with second column $\begin{pmatrix} r \\ s \end{pmatrix}$; then this can be lifted to an element of $\mathrm{SL}_2(\mathbb{Z})$ as above, and since we may replace the u, v in the first column with $u - tr, v - ts$ for any t, and $p \nmid s$, we can arrange that $p \mid v$. Thus there is an element of $\Gamma_0(p)$ which maps 0 onto $\frac{r}{s}$.

The question for $\Gamma_1(p)$ is more difficult: there are $(p-1)$ cusps. A question on the second example sheet will show you an explicit set of representatives. □

Question 13. *Let f be weakly modular of some weight k and level $\mathrm{SL}_2(\mathbb{Z})$. Show that $z \mapsto f(Nz)$ is weakly modular of level $\Gamma_0(N)$. If f is a modular form, is $f(Nz)$?*

Solution. This is not difficult with the machinery we have available by now: we know that for any $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, $f|_k\alpha$ is weakly modular of weight k for $\alpha^{-1}\mathrm{SL}_2(\mathbb{Z})\alpha$, and modular if and only if f is. But it's easy to see that if $\alpha = \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$, then $(f|_k\alpha)(z) = N^{k-1}f(Nz)$, and $\alpha^{-1}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\alpha = \begin{pmatrix} a & b/N \\ Nc & d \end{pmatrix}$, so $\Gamma_0(N) \subseteq \alpha^{-1}\,\mathrm{SL}_2(\mathbb{Z})\alpha$. □

Harder Problems

Here I'll only give brief hints.

Question 14. *Show that j defines an element of the group cohomology $H^1(\mathrm{SL}_2(\mathbb{R}), \mathcal{L}^\times)$, where $\mathcal{L}^\times$ is considered as a right $\mathrm{SL}_2(\mathbb{R})$-module via the usual (weight 0) action. Is it a coboundary? (In other words, is there a nowhere vanishing function f on $\mathcal{H}$ such that*

$$j(\gamma, z) = f(\gamma z)/f(z)$$

for all $z \in \mathcal{H}, \gamma \in SL_2(\mathbb{R})$?) What if we restrict to $\gamma \in \mathrm{SL}_2(\mathbb{Z})$?

Solution. The cocycle condition is exactly what we checked in Question 2 above. It is clear that j is a coboundary if and only if there exists a nonwhere vanishing weakly modular function of weight k and level $\mathrm{SL}_2(\mathbb{R})$, which is absurd; but if we replace $\mathrm{SL}_2(\mathbb{R})$ with $\mathrm{SL}_2(\mathbb{Z})$, then the question whether j^k is a coboundary is equivalent to asking whether or not there exists a weakly modular function of weight k and level Γ with no zeroes or poles on $\mathcal{H}$, with no hypotheses at infinity.

It is easy to see that Δ is an example for weight 12, and thus any k that is a multiple of 12 will work. With a little work it is possible to construct examples in any even weight. (Hint: first show there exists a weakly modular function of weight k, and use j to push its zeroes and poles to ∞.) □

Question 15. *Show that any automorphism of $\mathcal{H}$ which is biholomorphic (holomorphic with holomorphic inverse) is given by an element of $PSL_2(\mathbb{R})$.*

Solution. Since $\mathrm{PSL}_2(\mathbb{R})$ acts transitively on $\mathcal{H}$, it is sufficient to check that every transformation fixing i is in $\mathrm{PSL}_2(\mathbb{R})$. One can write down an element of $\mathrm{PSL}_2(\mathbb{C})$ that maps $\mathcal{H}$ onto the open unit disc $\mathbb{D}$ and sends i to 0, and it's easy to check that the Moebius transformations of the disc that fix 0 are just rotations by unit complex numbers. This is called Schwarz's lemma and is immediate from the maximum modulus principle for analytic functions (which is itself immediate from the Cauchy integral formula). □

Question 16. *The elements $a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $b = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ satisfy $b^2 = (ba)^3 = 1$ in $\mathrm{PSL}_2(\mathbb{Z})$. Are these two relations a complete set of relations? (i.e. is $\mathrm{PSL}_2(\mathbb{Z})$ isomorphic to the free group on two generators quotiented by these two relations?)*

Solution. Let $\tilde{G}$ be the quotient of the free group on two elements a, b by the above two relations, so there is a surjective homomorphism $\tau : \tilde{G} \to G$, which we want to show is an isomorphism.

Let $w \in \tilde{G}$. Write w as a word in a and b. If w is not a power of a, then by repeatedly applying the relation $aba = ba^{-1}b$, which holds in $\tilde{G}$, we may put w in the form $a^{r_0}ba^{r_1}ba^{r_2}b\dots a^{r_k}b$, where $r_i \in \mathbb{Z}$ and $(-1)^j r_j > 0$ for $j \geq 1$, and $(-1)^k r_k > 1$.

Then it is clear that $(\tau(w))(\infty)$ is the rational whose continued fraction expansion is $[r_0, -r_1, r_2, \dots, (-1)^k r_k]$. Since every rational has a unique continued fraction expansion (once we rule out negative terms and degenerate cases ending in 1), we see that if $\tau(w)(\infty) = \infty$, then w is a^k for some k. Thus τ is an isomorphism, and the result follows. □

Question 17. *(a) Show (directly from the definition) that $\Delta = \frac{E_4^3 - E_6^2}{1728}$ has integer coefficients.*

(b) Prove Ramanujan's congruence for the coefficients of Δ: if $\Delta = \sum a_n q^n$, then $a_n = \sigma_{11}(n) \bmod 691$ for $n \geq 1$. (Hint: $\frac{B_{12}}{24} = -\frac{691}{65520}$.)

Solution. Part (a) is an elementary check: one expands out $(1 + 240A)^3 - (1 - 504B)^2$ and reduces mod 2^6 and mod 3^3, and in each case it reduces to an easy application of Fermat's little theorem. For part (b), we write E_{12} as a linear combination of E_4^3 and Δ (by matching the first two coefficients), and write out the resulting identity in the form $\sigma_{11}(n) = \lambda a_n + \mu b_n$ where b_n is the nth coefficient of E_4^3. Modulo 691, it turns out that λ is congruent to 1 and μ to 0, and since $b_n \in \mathbb{Z}$, the result follows. □

Question 18. *(a) Show that the graded ring $\mathcal{M}(\mathbb{Z})$ of modular forms whose q-expansions are in $\mathbb{Z}[[q]]$ is generated over $\mathbb{Z}$ by E_4, E_6, and Δ.*

(b) Let $p \geq 5$ be prime. Let $\mathcal{I}_p$ be the kernel of the natural map $\mathcal{M}(\mathbb{Z}) \to \mathbb{F}_p[[q]]$. Show that $\mathcal{M}(\mathbb{F}_p) = \mathcal{M}(\mathbb{Z})/\mathcal{I}_p$ is generated as an $\mathbb{F}_p$-algebra by the images of E_4 and E_6 (so we no longer need Δ). Take $p = 17$; show that the images Q and R of E_4 and E_6 satisfy $8Q^4 - 7QR^2 = 1$.

(c) Show that $\mathcal{M}/\mathcal{I}_{17}$ is isomorphic to $\mathbb{F}_p[Q, R]/(8Q^4 - 7QR^2 - 1)$. Deduce that if $f \in M_{k_1} \cap \mathcal{M}$ and $g \in M_{k_2} \cap \mathcal{M}$, and $f - g \in \mathcal{I}_{17}$, then $k_1 = k_2 \bmod 16$; in other words, elements of $\mathcal{M}/\mathcal{I}_{17}$ have well-defined weights modulo 16.

Solution. Part (a) is a restatement of things we already know. For part (b), if we are allowed to invert 2 and 3 then we can write Δ as a polynomial in E_4 and E_6. Now, E_{p-1} is 1 mod p, since the denominator of the Bernoulli number B_{p-1} is divisible by p. We can write E_{p-1} as a polynomial in E_4 and E_6; for $p = 17$, it turns out that the polynomial we get is the one above.

For part (c), the ideal $\mathcal{I}_{17}$ had better be prime, as it is the kernel of a map into an integral domain. The polynomial $8Q^4 - 7QR^2 - 1$ in $\mathbb{F}_{17}[Q, R]$ is irreducible – this is a finite check – so the ideal it generates is prime. Consequently if these ideals are not equal, $\mathcal{I}_{17}$ is a height 2 prime; in other words, both Q and R must be algebraic over $\mathbb{F}_{17}$. Hence Δ is algebraic over $\mathbb{F}_{17}$, which is absurd.

Clearly the above ideal is a graded ideal if weights are taken modulo 16, with Q and R weighted in the natural way; so modular forms modulo 17 have well-defined weights modulo 16. ☐

Question 19. *(a) Show that the weight 2 Eisenstein series*

$$G_2(z) = \sum_{m,n \in \mathbb{Z}^2} \frac{1}{(m + nz)^2}$$

is not absolutely convergent, but that if we choose the order of summation to be

$$\sum_{n \in Z} \left({\sum_{m \in \mathbb{Z}}}' \frac{1}{(m + nz)^2} \right)$$

(where the dash denotes that the $(0, 0)$ term is omitted), then it is convergent (locally uniformly in z), $G_2(z + 1) = G_2(z)$, and the q-expansion formula of proposition 1.3.4 is still valid.

(b) Show that

$$G_2(-1/z) = z^2 G_2(z) - 2\pi i z.$$

(Hint: If $\tilde{G}_2$ denotes the double sum with the opposite ordering of the variables, then $G_2(-1/z) = z^2\tilde{G}_2(z)$. Compare this double sum with the analogous sums $H, \tilde{H}$ whose (m, n) term is $\frac{1}{(m-1+nz)(m+nz)}$, again with the two possible orderings. The difference between G_2 and H is absolutely summable, so the "error" in changing the order of the variables is the same for G_2 and for H; but the H sum telescopes.)

Solution. We have $h_{mn} = \frac{1}{(m-1+nz)(m+nz)} = \frac{1}{m-1+nz} - \frac{1}{m+nz}$. Clearly this makes no sense if $(m, n) = (0, 0)$ or $(1, 0)$, so we must omit the $(1, 0)$ term too. Then we find that

$$\sum_{m=-R}^{R} \sum_{\substack{n=-S \\ (m,n) \neq (0,0),(1,0)}}^{S} h_{mn} = 2 + \sum_{n=-S}^{S} \left(\frac{1}{-R + nz} - \frac{1}{R + nz} \right).$$

If we let R tend to ∞, corresponding to summing over m first, then the bracketed term clearly vanishes, so the sum is 2. On the other hand, if we fix R and let S tend to ∞, we are dealing with the sum

$$2 - \frac{2}{z} \sum_{n \in \mathbb{Z}} \frac{1}{\frac{R}{z} + n} = 2 - \frac{2}{z} \left(\pi \cot \tfrac{\pi R}{z} \right)$$

(using a formula that came up in the proof of prop 1.3.5), and since if $\operatorname{Im} z > 0$, $\lim_{R \to \infty} \cot \frac{R}{z} = i$, we obtain $\tilde{H}(z) = 2 - \frac{2\pi i}{z}$.

(An alternative, and perhaps easier to find, argument is to compare $\frac{1}{m+nz}$ to the integral over the square $m \leq x \leq m+1$, $n \leq y \leq n+1$ of $\frac{1}{x+zy}$. One finds, again, that the difference is absolutely summable; and the double integral can be evaluated exactly whichever order of variables we choose, with the error in changing the order of limits in the double integral coming out as $\frac{2\pi i}{z}$. However, one has to be careful about screening out the region in which the poles lie.) ☐

Question 20. *Let* $F(z) = q\prod_{n\geq 1}(1-q^n)^{24}$*. Show that*

$$\frac{\mathrm{d}}{\mathrm{d}z}\log F(z) = \frac{6i}{\pi}G_2(z).$$

Deduce that $\log F(-1/z) - \log z^{12}F(z)$ *is constant. Set* $z = i$ *to deduce that the constant is 0, so* F *is a modular form of weight 12. Deduce that* $F = \Delta$*.*

Solution. This is an easy corollary of the transformation law for G_2 we established above. Once we know $F \in M_{12}$, checking the first two coefficients is enough to check that $F = \Delta$.

Incidentally, apologies for the typo in the original version (it originally said "deduce that the constant is 1"). ☐

Question 21. *(a) Show that if* $E_2(z) = G_2(z)/2\zeta(2) = 1 - 24\sum_{n\geq 1}\sigma_1(n)q^n$*, and* f *is any modular form of weight* k*, then* $\partial f = 12q\frac{\mathrm{d}f}{\mathrm{d}q} - kE_2 f$ *is a modular form of weight* $k+2$*. (This operator* ∂ *was introduced by Ramanujan.)*

(b) Deduce that if $f = \sum_{n\geq 0} a_n q^n$ *is a modular form of weight* k *with integral coefficients, and* p *is prime, then there exists a modular form* $g = \sum_{n\geq 0} c_n q^n$ *of weight* $k+p+1$ *such that* $c_n = na_n \bmod p$*. (So the operator* $\theta = q\frac{d}{dq}$ *preserves the space of mod* p *modular forms.)*

(c) Use this to give an extremely short proof that if a_n *is the* n*th coefficient of* Δ*,* $a_n = n\sigma_3(n) \bmod 7$*.*

Solution. For part (a), it is immediate that ∂f is preserved by $z \mapsto z+1$, and checking that it satisfies the weight $k+2$ transformation law for $z \mapsto -1/z$ is an elementary manipulation, given that we know how f and E_2 transform. It is clear that ∂f is holomorphic on $\mathcal{H}$ and has a convergent q-expansion on some neighbourhood of ∞ with no negative powers of q, so it is a modular form.

For part (b), we note that E_2 is congruent mod p to E_{p+1} – this is Fermat's little theorem for the coefficients of q^n with $n > 0$, and for the linear term it follows from Kummer's congruence which states that if $k \neq 0 \bmod (p-1)$, then $\frac{B_k}{k}$ is p-integral and depends only on $k \bmod (p-1)$. Similarly, one can check that E_{p-1} reduces to 1 mod p. We thus see that the weight $k+p+1$ form $E_{p-1}\partial f + kE_{p+1}f$ is congruent mod $p-1$ to $q\frac{\mathrm{d}f}{\mathrm{d}q}$.

For part (c), we find that θE_4 must be the mod 7 reduction of a modular form of weight 12, and by checking the mod 7 reductions of the first few coefficients of our basis elements of $M_{12}(\mathbb{Z})$ we deduce that $\theta E_4 = \Delta \bmod 7$, as required. ☐