MODULAR FORMS EXAMPLE SHEET 1

1. Let V be a finite dimensional real vector space, and recall that a lattice in V is a closed discrete additive subgroup of V. Show that every lattice in V has the form $\mathbb{Z} \cdot v_1 + \mathbb{Z} \cdot v_2 + \cdots + \mathbb{Z} \cdot v_n$ for some linearly independent subset $v_1, \dots v_n$ of V.

Solution: Let L be a lattice in V; replacing V with the span of L we may assume that L spans V. Then L contains a basis $w_1, \dots, w_n$ of V. Let L' be the sublattice of L consisting of all the integer linear combinations of the w_i. We will show that L/L' is finite.

Claim 1: Let S be a closed discrete subset of a compact space X. Then S is finite.

Proof: For each s in S, there is a U_s open in x such that $U_s \cap S = \{s\}$. Let W be the complement of S in X; then W is open in X, and W, together with the U_s, cover S. It is clear that any subcover of this cover contains all the U_s. On the other hand X is compact, so there is a finite subcover; we must thus have S finite.

Claim 2: V/L' is compact.

Proof: The map that takes $r_1 w_1 + \dots r_n w_n$ to $(e^{2\pi i r_1}, \dots e^{2\pi i r_n})$ is a homeomorphism of V/L' onto $(S^1)^n$, where S^1 is the unit circle in the complex plane. Since S^1 is compact we are done.

Claim 3: L/L' is discrete and closed in V/L'.

Proof: Since L is discrete there exists an open subset U_0 of V such that $U_0 \cap L = \{0\}$. Then for $x \in L$ set $U_x = x + U_0$; note that U_x is open in V and $U_x \cap L = \{x\}$. Let $\pi : V \to V/L'$ be the quotient map, and let $\overline{U}_x$ be the subset $\pi(U_x)$ of V/L'. Then $\pi^{-1}(\overline{U}_x)$ is the disjoint union of U_{x+y}, for $y \in L'$. Thus $\overline{U}_x$ is open in V/L'. Moreover, $\pi^{-1}(\overline{U}_x) \cap L$ is equal to $\{x + y : y \in L'\}$, so $\overline{U_x} \cap L/L'$ is equal to the class $[x]$ of x modulo L'. Thus L/L' is discrete. Let W be the complement of L/L' in V/L'. Then $\pi^{-1}(W) = V \setminus L$, and so is open in V. Thus W is open in V/L', so L/L' is closed.

From these claims it follows immediately that L/L' is finite. In particular L is finitely generated, and so, by the classification of finitely generated abelian groups, L is isomorphic to $\mathbb{Z}^r$ for some r. Since L/L' is finite we must have $r = n$; then there are $v_1, \dots, v_n$ in V generating L. Since the span of the v_i contains the w_i, the v_i are a basis for V and hence linearly independent as required.

2. Show directly from the definition that there are no nonzero weakly modular functions of weight k for odd k, and that every modular form of weight zero is constant.

If f is weakly modular of weight k, for k odd, then for $\gamma = -\mathrm{Id}$ we have $f(\gamma z) = -f(z)$. But $\gamma z = z$, so we must have $f(z) = 0$. For the second claim, a modular form of f weight zero is holomorphic at infinity, and thus bounded as $\Im(z)$ approaches infinity, uniformly in $\Re(z)$. It follows that such a form is bounded on the fundamental domain D, and hence (since it is weight zero, hence invariant under $\mathrm{SL}_2(\mathbb{Z})$) on the entire upper half plane. We can regard f as a bounded function on $\mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$; since the latter is isomorphic to the complex plane, and bounded holomorphic functions on the complex plane are constant, f must be constant.

3. Let f be a weakly modular function, and g the unique function on the unit disk such that $f(z) = g(e^{2\pi iz})$. Show that g is meromorphic at zero if, and only if, there exists an integer N and a positive constant c such that such that $|f(z)| < ce^{N(\mathrm{Im}\, z)}$ for $\mathrm{Im}\, z >> 0$. Show that g is holomorphic at zero if we can take N to be zero, and that in this case $f(z)$ approaches $g(0)$ as $\mathrm{Im}\, z$ approaches ∞.

Let $q = e^{2\pi iz}$ be the coordinate on the upper half plane. The function g is meromorphic at zero if and only if $q^n g(q)$ is bounded near zero for some n. Making the change of variables $q = e^{2\pi iz}$, we see that this occurs if and only if $e^{2\pi inz} f(z)$ is bounded as $\Im(z)$ goes to infinity. As $|e^{2\pi inz}| = e^{-2\pi n\Im(z)}$ the first claim follows. Moreover, g is holomorphic if any only if we can take $n = 0$; in this case g extends to a well-defined function on the whole unit disc. As $\Im z$ approaches infinity, q approaches zero, and so $f(z)$ approaches $g(0)$ as claimed.

4. A lattice L in $\mathbb{C}$ is said to have *complex multiplication* if there is an $\alpha \in \mathbb{C} \setminus \mathbb{Z}$ such that $\alpha L \subseteq L$. Show that the lattice $L_{1,z}$ has complex multiplication if, and only if, z satisfies a quadratic polynomial P with integral coefficients. Show further that if this is the case, then the set of $\alpha \in \mathbb{C}$ with $\alpha L \subseteq L$ is an order in the number field $\mathbb{Q}(z)$.

Let $L = L_{1,z}$. We have $\alpha L \subseteq L$ if, and only if, α and αz lie in L. In this case we can write $\alpha = az + b$, $\alpha z = cz + d$. Then $az^2 + bz = cz + d$, so z satisfies a quadratic polynomial with integer coefficients (a is not zero as otherwise α would be an integer.) Conversely, if z satisfies such a polynomial, P, whose coefficients we may assume are relatively prime, then one checks easily that for any integers a, b, such that a is divisible by the leading coefficient of P, multiplication by $az + b$ takes L to a subset of L. Thus in this case, the set of α that take L to a subset of L is the subring $\mathbb{Z}[nz]$, where n is the leading coefficient of P; this is clearly an order in $\mathbb{Q}(z)$.

5a. Use the equations $E_8 = E_4^2$ and $E_{10} = E_4 E_6$ to deduce identities relating σ_3 and σ_7 in the first case, and σ_3, σ_5, and σ_9 in the second.

We have:

$$\begin{aligned}
E_4 &= 1 + 240\Sigma_{n\geq 1}\sigma_3(n)q^n \\
E_6 &= 1 - 504\Sigma_{n\geq 1}\sigma_5(n)q^n \\
E_8 &= 1 + 480\Sigma_{n\geq 1}\sigma_7(n)q^n \\
E_{10} &= 1 - 264\Sigma_{n\geq 1}\sigma_9(n)q^n \\
E_{12} &= 1 + \frac{24\cdot 2730}{691}\Sigma_{n\geq 1}\sigma_{11}(n)q^n
\end{aligned}$$

Comparing the coefficients of q^n we find that

$$\sigma_7(n) = 480\sigma_3(n) + 240^2\Sigma_{m=1}^{n-1}\sigma_3(m)\sigma_3(n-m).$$

$$264\sigma_9(n) = 504\sigma_5(n) - 240\sigma_3(n) - 240\cdot 504\Sigma_{m=1}^{n-1}\sigma_3(m)\sigma_5(n-m).$$

5b. Find constants c_1, c_2 such that $E_4^3 = c_1 E_{12} + c_2\Delta$. Conclude that if $\Delta(q) = \Sigma\tau(n)q^n$, then $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$. This is called "Ramanujan's congruence".

Considering the constant terms we find that $c_1 = 1$. Considering the q-coefficients gives the equation:

$$c_2 + \frac{24\cdot 2730}{691} = 720$$

from which we find that $c_2 = \frac{432000}{691}$. Substituing into the series expansions we find:

$$240\cdot 691\sigma_3(n) = 24\cdot 2730\sigma_{11}(n) + 432000\tau(n).$$

Reducing mod 691 yields the desired result.

6. Show (using the q-expansions for E_4 and E_6, and the identity $\Delta = \frac{1}{1728}(E_4^3 - E_6^2)$, that the q-expansion of Δ has integral coefficients.

The coefficient of q^n in $E_4^3 - E_6^2$ is given by $3\cdot 240\sigma_3(n) + 2\cdot 504\sigma_5(n)$, plus $-[504\sigma_5(n/2)]^2 + 3[240\sigma_3(n/2)]^2$ if n is even and $240^3\sigma_3(n/3)^3$ if n is divisible by 3. We must check that this sum is always divisible by 2^6 and 3^3. It is easy to see that the "extra" terms that arise if n is even or divisible by 3 are always divisible by 2^6. On the other hand, both 720 and 1008 are divisibly by 2^4; factoring this out from the first term gives $45\sigma_3(n) + 63\sigma_5(n)$. Modulo 4 we have d^3 and d^5 congruent for all d, so modulo 4 this is congruent to $\sigma_3(n) + 3\sigma_3(n)$ and is thus divisible by 4. We thus have divisibility by 2^6; divisibility by 3^3 is similar.