MODULAR FORMS EXAMPLE SHEET 1

1a. Let p be an odd prime. Show that the quadratic equation $ax^2+bx+c=0$ (a,b,c fixed in $\mathbb{Z}/p\mathbb{Z}$, a nonzero) has:

- exactly one solution in $\mathbb{Z}/p\mathbb{Z}$ if $b^2 - 4ac = 0 \pmod{p}$
- two solutions if $b^2 - 4ac$ is a nonzero square mod p
- no solutions if $b^2 - 4ac$ is not a square mod p

1b. Let $P(x)$ be a polynomial with integral coefficients. Show that the equation:

$$y^2 + y = P(x)$$

has exactly n solutions mod p in (x, y), where n is given by:

$$n = p + \sum_{x=0}^{p-1} \left(\frac{1 + 4P(x)}{p} \right),$$

where $\left(\frac{a}{p}\right)$ is zero if a is zero mod p, 1 if a is a nonzero square mod p, and -1 if a is not a square mod p.

1c. For $p = 13$, verify the claim made in the first lecture that $a_p = p - n_p$, where n_p is the number of pairs (x, y) mod p that satisfy

$$y^2 + y = x^3 - x^2 - 10x - 20$$

and a_p is the coefficient of q^p in the series:

$$q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2.$$

(Feel free to use computer assistance to compute a_p here; it can be done by hand but is somewhat intensive combinatorially.)

2. Let V be a finite dimensional real vector space, and recall that a lattice in V is a closed discrete additive subgroup of V that spans V over $\mathbb{R}$. 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 basis $v_1, \ldots v_n$ of V. (In particular, the lattices in $\mathbb{C}$ have the form claimed in .) [Hint: first show that such a lattice is a finitely generated abelian group. You will then need the fact that a finitely generated abelian group with no elements of finite order is isomorphic to $\mathbb{Z}^r$ for some r.]

3. Let f be a weakly modular function, and g the unique function on the unit disk such that $f(z) = g(e^{2\pi i z})$. 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 $|f(z)| < ce^{N(\operatorname{Im} z)}$ for $\operatorname{Im} z >> 0$. 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 $\operatorname{Im} z$ approaches ∞.

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 a subring of the number field $\mathbb{Q}(z)$ that has finite rank as a $\mathbb{Z}$-module.

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.

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".

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.

7a. For $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{GL}_2(\mathbb{R})^+$, define $j(\gamma, z) = cz + d$. Show that

$$j(\gamma'\gamma, z) = j(\gamma', \gamma(z)) j(\gamma, z).$$

7b. Show that for f a function on the upper half plane, one has

$$(f|_{k,\gamma})|_{k,\gamma'} = f|_{k,\gamma\gamma'},$$

where $f|_{k,\gamma}(z) = f(\gamma z) j(\gamma, z)^{-k} (\det \gamma)^{k-1}$.