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 x if $b^2-4ac=0 \pmod p$
- two solutions in x if b^2-4ac is a nonzero square mod p
- no solutions if b^2-4ac is not a square mod p

We complete the square: substituting $x=y-(2a)^{-1}b$ into the equation, we obtain:

$$ay^2-by+(4a)^{-1}b^2+by-(2a)^{-1}b^2+c=0$$

Multiplying through by $4a$ we get

$$4a^2y^2-b^2+4ac=0$$

or

$$(2ay)^2=b^2-4ac.$$

This clearly has the desired number of solutions in $2ay$ and hence in y (since a nonzero square mod p has exactly two square roots).

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 otherwise.

For each x, the number of y such that $y^2+y=P(x)$ is $1+\left(\frac{1+4P(x)}{p}\right)$ by part a). Summing over all x we obtain the formula given.

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

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

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

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

Mod 13, the nonzero squares are $1, 3, 4, 9, 12, 10$. (In particular -1 is a square mod 13.) Also note that

$$x^3 - x^2 - 10x - 20 \equiv (x - 10)(x^2 - 4x + 2) (\text{mod } 13).$$

- $x = 0$, $P(x) = -20$, $1 + 4P(x) = -79 = 12$. (Two y.)
- $x = 1$, $P(x) = 9$, $1 + 4P(x) = 37 = 11$. (Zero y.)
- $x = 2$, $P(x) = 16 = 3$, $1 + 4P(x) = 0$. (One y.)
- $x = 3$, $P(x) = 7$, $1 + 4P(x) = 29 = 3$. (Two y.)
- $x = 4$, $P(x) = -12 = 1$, $1 + 4P(x) = 5$. (Zero y.)
- $x = 5$, $P(x) = -35 = 4$, $1 + 4P(x) = 4$. (Two y.)
- $x = 6$, $P(x) = -4$, $1 + 4P(x) = -15 = 11$. (Zero y).
- $x = 7$, $P(x) = -69 = -4$, $1 + 4P(x) = -15 = 11$. (Zero y).
- $x = 8$, $P(x) = -68 = -3$, $1 + 4P(x) = -11 = 2$. (Zero y).
- $x = 9$, $P(x) = -47 = 5$, $1 + 4P(x) = 21 = 8$. (Zero y).
- $x = 10$, $P(x) = 0$, $1 + 4P(x) = 1$. (Two y.)
- $x = 11$, $P(x) = 79 = 1$, $1 + 4P(x) = 5$. (Zero y.)
- $x = 12$, $P(x) = 1$, $1 + 4P(x) = 5$. (Zero y.)

This gives $n_p = 2 + 0 + 1 + 2 + 0 + 2 + 0 + 0 + 0 + 0 + 2 + 0 + 0$, yielding $n_p = 9$. We thus have $p - n_p = 4$.

Expanding out the power series (using computer assistance, or by consulting the london modular forms database (lmfdb.org), we find that this is indeed equal to a_{13}!)

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 lecture.) [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.]

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 $w_1, \ldots, w_n$ 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.
Use the basis $w_1, \ldots, w_n$ to identify V with $\mathbb{R}^n$. Since L is discrete, the distance between two elements of L is bounded below, so there are only finitely many elements of L with coordinates in $[0, 1]$. On the other hand, given x in L, there exists y in L' such that $x - y$ has coordinates in $[0, 1]$. Thus L is generated by $w_1, \ldots w_n$ together with those elements of L with coordinates in $[0, 1]$. In particular L is finitely generated, and L/L' is finite. Thus L is isomorphic to $\mathbb{Z}^r$ for some r.

Since L/L' is finite we must have $r = n$; then there are $v_1, \ldots, v_n$ 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.

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 $|f(z)| < ce^{N(\operatorname{Im} z)}$ 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 ∞.

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

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 clearly has finite rank.

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 $E_4^3 = c_1E_{12} + c_2\Delta$. 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.

We must check that the coefficient of q^n in $E_4^3 - E_6^2$ is divisible by 1728 for all n; this amounts to checking that it is divisible by 2^6 and 3^3. The coefficient of q^n in E_4^3 is obtained by summing products of three coefficients of

$$E_4 = 1 + 240\Sigma_{n\geq 1}\sigma_3(n)q^n;$$

if more than one of these is not 1 then such a product is divisible by 240^2 and hence by 2^6. Thus the coefficient of q^n in E_4^3 is the sum of $3\cdot 240\sigma_3(n)$ and something divisible by 2^6. Similarly, the coefficient of q^n in E_6^2 is given by $-2\cdot 504\sigma_5(n)$, plus something divisible by 2^6. We must thus check that the sum $3\cdot 250\sigma_3(n) + 2\cdot 504\sigma_5(n)$ is always divisible by 2^6 and 3^3. Both 720 and 1008 are divisible by 2^4; factoring this out from the first term gives $45\sigma_3(n)+63\sigma_5(n)$, and we must show this is divisible by 4. 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.

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

Note that we have:

$$\gamma\begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} az+b \\ cz+d \end{pmatrix} = \begin{pmatrix} \gamma z \\ 1 \end{pmatrix} j(\gamma, z).$$

We thus have:

$$j(\gamma'\gamma, z)\begin{pmatrix} \gamma'\gamma z \\ 1 \end{pmatrix} = \gamma'\gamma\begin{pmatrix} z \\ 1 \end{pmatrix}$$

$$= \gamma' \begin{pmatrix} \gamma z \\ 1 \end{pmatrix} j(\gamma, z) = \begin{pmatrix} \gamma'\gamma z \\ 1 \end{pmatrix} j(\gamma', \gamma z) j(\gamma z).$$

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

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

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

We have:

$$\begin{aligned} (f|_{k,\gamma})_{k,\gamma'}(z) &= (f|_{k,\gamma}(\gamma' z) j(\gamma', z)^{-k} (\det \gamma')^{k-1} \\ &= f(\gamma\gamma' z) j(\gamma, \gamma' z) j(\gamma', z) (\det \gamma')^{k-1} (\det \gamma)^{k-1} \\ &= f(\gamma\gamma' z) j(\gamma\gamma', z) (\det \gamma\gamma')^{k-1} = f|_{k,\gamma\gamma'}(z). \end{aligned}$$