PMATH 944: MODULAR FORMS

LECTURES GIVEN BY DR. C. STEWART AT THE UNIVERSITY OF WATERLOO, WINTER 2012

Lecture 1: Lattices and Elliptic Functions

Definition 1. *Let $\omega_1, \omega_2 \in \mathbb{C}\backslash\{0\}$ with $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$. A lattice in $\mathbb{C}$ is a set $L := \{n\omega_1 + m\omega_2 : n, m \in \mathbb{Z}\}$.*

It is easy to see that this is an additive subgroup of $\mathbb{C}$. Also, the representation of each element L is unique. Indeed, if $w \in L$ with $w = n_1\omega_1 + m_1\omega_2 = n_2\omega_1 + m_2\omega_2$ with $n_1, n_2, m_1, m_2 \in \mathbb{Z}$ with at least one of $n_1 \neq n_2$ or $m_1 \neq m_2$. Without loss of generality, suppose $n_1 \neq n_2$. Then $(n_1 - n_2)\omega_1 = (m_1 - m_2)\omega_2$, so that $\frac{\omega_1}{\omega_2} = \frac{m_1 - m_2}{n_1 - n_2} \in \mathbb{R}$, a contradiction, hence $n_1 = n_2$ and $m_1 = m_2$. Thus, each element of L is uniquely represented.

Definition 2. *An elliptic or doubly-periodic function f is a meromorphic function on $\mathbb{C}$ which is L-periodic for some lattice L, i.e. there exists some lattice L such that for every $z \in \mathbb{C}$ and $\omega \in L$, $f(z + \omega) = f(z)$.*

Suppose L is generated by complex numbers ω_1 and ω_2. We shall denote L by $L = [\omega_1, \omega_2]$. Further, for every $\alpha \in \mathbb{C}$, $\{\alpha + t_1\omega_1 + t_2\omega_2 : 0 \leq t_1, t_2 < 1\}$ is known as the fundamental parallelogram at α for the lattice, as in Figure 1. A doubly-periodic function is thus completely determined by its behaviour on the fundamental parallelogram at 0.
If f were entire, since the fundamental parallelogram is compact, f would be bounded on it. By L-periodicity, f is thus bounded on all of $\mathbb{C}$. By Liouville's theorem in complex analysis, this implies that f is constant. Therefore, the interesting cases are those functions that have poles.

Notice that if ω_1', ω_2' also generate $L = [\omega_1, \omega_2]$, we can find $a, b, c, d \in \mathbb{Z}$ such that $\omega_1' = a\omega_1 + b\omega_2$ and $\omega_2' = c\omega_1 + d\omega_2$, so we have the matrix equation $\binom{\omega_1'}{\omega_2'} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \binom{\omega_1}{\omega_2}$, and since ω_1 and ω_2 are also expressible in terms of ω_1' and ω_2', it follows that the matrix $A := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible. Since the entries are integers, $\det A^{-1} = \frac{1}{\det A} \in \mathbb{Z}$, so $ad - bc = \det A = \pm 1$. The set of 2×2 matrices with integer entries with this property is known as the modular group.
For any lattice L, we define the Weierstrass p-function of L, written $p(z)$ or $p_L(z)$, as

$$p(z) = \frac{1}{z^2} + \sum_{\omega \in L'} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right),$$

where $L' = L\backslash\{0\}$.
We claim that p is meromorphic and L-periodic. To do this, we will show that p converges uniformly on compact subsets. Let $K \subseteq \mathbb{C}$ be compact, thus bounded, so there exists $R > 0$ such that $K \subseteq D(0; R)$, the

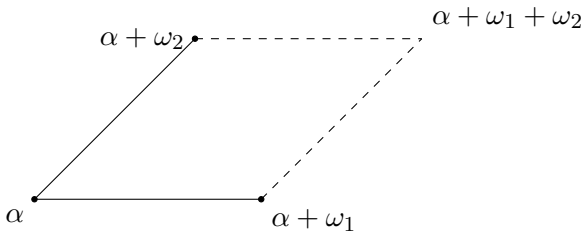

FIGURE 1. Fundamental Parallelogram for the Lattice $[\omega_1, \omega_2]$ at α

open disk of radius R centered at 0. Thus, for $\omega \in L$, if $|\omega| \geq 2R$, $|\omega| \geq 2|z|$ for every $z \in K$.
For $z \in K$, $|z - \omega| \geq |\omega| - |z| \geq |\omega| - \frac{1}{2}|\omega| = \frac{1}{2}|\omega|$ and

$$|z - 2\omega| \leq |z| + 2|\omega| \leq \frac{1}{2}|\omega| + 2|\omega| = \frac{5}{2}|\omega|$$

so it follows that

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{\omega^2 - z^2 + 2z\omega - \omega^2}{(\omega(z-\omega))^2}\right| = \frac{|z||z-2\omega|}{|\omega|^2|z-\omega|^2} \leq \frac{|z|\frac{5}{2}|\omega|}{\frac{1}{4}|\omega|^4} = \frac{10|z|}{|\omega|^3}.$$

Therefore, to show that the series converges uniformly on compact subsets, we need only show that $\sum_{\omega \in L'} \frac{1}{|\omega|^2}$ is absolutely convergent. Since $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$, there exists a $C > 0$ such that $|n_1\omega_1 + n_2\omega_2| \geq C(|n_1| + |n_2|)$. Since there are $4n + 2$ pairs (n_1, n_2) with $|n_1| + |n_2| = n$ (for each k amongst the $2n + 1$ numbers $\{0, \pm 1, \ldots, \pm n\}$, there are two solutions $m = \pm(n - |k|)$ with $|k| + |m| = n$), we see that

$$\sum_{\omega \in L'} \frac{1}{|\omega|^3} \leq \sum_{\substack{\omega = n_1\omega_1 + n_2\omega_2 \\ (n_1, n_2) \neq (0,0)}} \frac{1}{|n_1\omega_1 + n_2\omega_2|^3} \leq \sum_{n=1}^{\infty} \frac{4n+2}{C^3 n^3} < \infty.$$

Thus, p is converges uniformly on K so since K was arbitrary, it follows that p is meromorphic. Note that p has a double pole at every point of L and no others.

Further, observe that snce L is invariant under the transformation $\omega \mapsto -\omega$, the term

$$\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right) + \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right)$$

is invariant with respect to $z \mapsto -z$ as well, and therefore p, the sum of all such terms, is an even function, i.e. $p(z) = p(-z)$ for every $z \in \mathbb{C}$.
Is p L-periodic? Notice that $p'(z) = -2\sum_{\omega \in L} \frac{1}{(z-\omega)^3}$ since the series of derivatives of the terms converge uniformly on compact subsets, by comparison with p. This is clearly L-periodic. Thus, there exists a constant c_0 such that $p(z + \omega_1) = p(z) + c_0$ for every $z \in \mathbb{C}$. Take $z = -\frac{1}{2}\omega_1$. Then by the evenness of p,

$$p\left(-\frac{1}{2}\omega_1\right) = p\left(\frac{1}{2}\omega_1\right) = p(z + \omega_1) = p(z) + c_0 = p\left(-\frac{1}{2}\omega_1\right) + c_0$$

so that $c_0 = 0$. The analogous result holds for ω_2 and thus p is L-periodic.

Given a lattice L, the set of elliptic functions for the lattice forms a field. In fact, one can prove the field is generated over $\mathbb{C}$ by p and p'.

Let us now consider the power series expansions of p and p' around the origin.

$$\begin{aligned} p(z) &= \frac{1}{z^2} + \sum_{\omega \in L'} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right) = \frac{1}{z^2} + \sum_{\omega \in L'} \left(\frac{1}{\omega^2} \frac{1}{(1-\frac{z}{\omega})^2} - \frac{1}{\omega^2} \right) \\ &= \frac{1}{z^2} + \sum_{\omega \in L'} \left(\frac{1}{\omega^2} \left(1 + \frac{z}{\omega} + \left(\frac{z}{\omega}\right)^2 + \dots \right) - \frac{1}{\omega^2} \right) = \frac{1}{z^2} + \sum_{\omega \in L'} \left(\sum_{m=1}^{\infty} (m+1) \left(\frac{z}{\omega}\right)^m \right) \frac{1}{\omega^2} \\ &= \frac{1}{z^2} + \sum_{m=1}^{\infty} c_m z^m \end{aligned}$$

where $c_m = (m+1) \sum_{\omega \in L'} \frac{1}{\omega^{2+m}}$.
Note that $c_m = 0$ when m is odd, since p is an even function.

Notation. *For any lattice L and positive integer m we define*

$$s_m(L) := \sum_{\omega \in L'} \frac{1}{\omega^m}$$

whenever the sum converges (when the context is clear, we will write s_m).

Thus, in a neighbourhood of 0, we have

$$p(z) = \frac{1}{z^2} + \sum_{m=1}^{\infty} (2m+1) s_{2m+2} z^{2m} = \frac{1}{z^2} + 3s_n z^2 + 5s_6 z^4 + \dots$$

$$p'(z) = -\frac{2}{z^3} + \sum_{m=1}^{\infty} 2m(2m+1) s_{2m+2} z^{2m-1} = -\frac{2}{z^3} + 6s_4 z + 20 s_6 z^3 + \dots$$

Put $g_2 := g_2(L) = 60 s_4$ and $g_3 := g_3(L) = 140 s_6$.

Theorem 1. $p'(z)^2 = 4p(z)^3 - g_2 p(z) - g_3$

Proof. Consider the function $\phi(z)$ given by $\phi(z) := p'(z)^2 - 4p(z)^3 - g_2 p(z) - g_3$. Clearly, ϕ is elliptic since p' and p both are. Now consider ϕ in a neighbourhood of 0. Expanding each term in the definition of $\phi(z)$ in powers of z gives

$$\begin{aligned} p'(z)^2 &= \frac{4}{z^6} - \frac{24 s_4}{z^2} - 80 s_6 + \dots \\ -4p(z)^3 &= -\frac{4}{z^6} - \frac{36 s_4}{z^2} - 60 s_6 + \dots \\ g_2 p(z) &= \frac{60 s_4}{z^2} + 0 + \dots \\ g_3 &= 140 s_6. \end{aligned}$$

Thus, adding these terms gives $\phi(z) = 0+$ higher order powers of z, in a neighbourhood of 0. But ϕ is elliptic, so the poles of ϕ are in L if they exist, so there are no poles in any neighbourhood of 0, so ϕ is entire. Thus, by a remark we made above, ϕ is constant and thus identically 0. $\square$

Therefore, the points $(p(z), p'(z)) \in \mathbb{C}^2$ lies on the curve $y^2 = 4x^3 - g_2x - g_3$.

Lecture 2: Relationship between Lattices and Elliptic Curves

The quotient group $\mathbb{C}/L$ is abelian under addition. Define $E := \{(x, y) \in \mathbb{C}^2 : y^2 = 4x^3 - g_2x - g_3\} \cup \{\infty\}$. This is an elliptic curve. The map $\mathbb{C}/L \to E$ given by $z \mapsto (p(z), p'(z))$ is a group homomorphism. Thus, we can impose a group structure on the elliptic curve E in this way. In fact there is a geometric interpretation of the group structure on E adding points may be defined independently of the p-function. It turns out that if E has $g_2, g_3 \in \mathbb{Q}$ then adding points on E with rational coordinates results in a point with rational coordinates. Here, we suppose the point at infinity has rational coordinates (this is the identity element of the group of rational points on E).

Suppose $g_2, g_3 \in \mathbb{Q}$ and let $E(\mathbb{Q})$ denote the group of points on E with rational coordinates. Poincaré asked: is $E(\mathbb{Q})$ finitely generated?
In 1922, Mordell proved that it is. In 1930, Weil generalized the result in the following way:

Mordell-Weil Theorem. *Let $K/\mathbb{Q}$ be a field extension. If $g_2, g_3 \in K$ with $g_2^3 - 27g_3^2 \neq 0$ then $E(K)$ is finitely-generated.*

The proof is not constructive so there is no algorithm for computing generators.

One can find $g_2, g_3 \in \mathbb{Q}$ such that $g_2^3 - 27g_3^2 \neq 0$ for which the rank is positive and thus $E(\mathbb{Q})$ is infinite. However, by a result of Siegel, if $g_2, g_3 \in \mathbb{Q}$ with $g_2^3 - 27g_3^2 \neq 0$ then there are finitely many pairs $(x, y) \in E$ with integer coefficients. The analogous result on the field extension $K/\mathbb{Q}$ also holds, i.e. there are only finitely many pairs $(x, y) \in E$ where x, y are elements of the ring of integers of K.

It is possible to associate an L-function to an elliptic curve E. The L-function is an Euler product of local L-functions determined by examining E modulo p for each prime p. It follows from the work of Taylor and Wiles that the L-function can be analytically continued to all of $\mathbb{C}$. By a conjecture of Birch and Swinnwerton-Dyer, the order of the zero of L at $s = 1$ is the rank of $E(\mathbb{Q})$. This result is of interest because it allows one to characterize the global behaviour of an elliptic curve using local information.

Recall that $p(z)$ is an even function (and thus all of the terms in its Laurent series have positive power) so $p'(z)$ is an odd function. For any elliptic function f with respect to a lattice $L = [\omega_1, \omega_2]$ we can find a fundamental paralleogram P_α with $\alpha \in \mathbb{C}$ for which $P_\alpha = \{\alpha + t_1\omega_1 + t_2\omega_2 : 0 \leq t_1, t_2 \leq 1\}$ has no zeros or poles of f on its boundary, as in Figure 2. Note that $\oint_{\partial P_\alpha} f dz = 0$ (where given a set A, the notation ∂A refers to the boundary of the set A), since f is periodic so on parallel sides of the parallelogram we get the same points but different orientation. Since the set of elliptic functions is a field as remarked above, $\frac{f'}{f}$ is also elliptic and therefore by the argument principle, since P_α is a simple closed curve, it follows that

$$\sum_{z:f(z)=0} N(z) - \sum_{z:\frac{1}{f}(z)=0} P(z) = \oint_{\partial P_\alpha} \frac{f'}{f} dz = 0$$

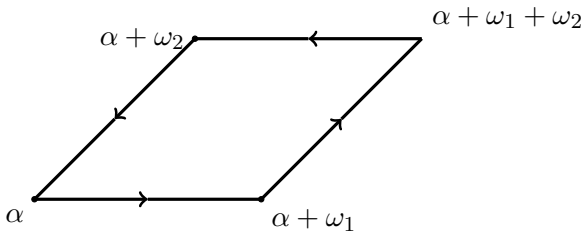

FIGURE 2. Path of Integration P_α

where $N(z)$ is the order of the zero z and $P(z)$ is the order of the pole z. Thus, the number of zeros of f counted with multiplicity is equal to the number of zeros counted with multiplicity.

By its series definition, $p'(z)$ has a pole of order 3 at every lattice point and no others. Therefore, there are 3 zeros (counted with multiplicity) of $p'(z)$ in P_0 counted with multiplicity.

Observe that $\frac{\omega_1}{2} \equiv -\frac{\omega_1}{2} \pmod{L}$ so $p'\left(\frac{\omega_1}{2}\right) = p'\left(-\frac{\omega_1}{2}\right)$ by periodicity. But p' is odd, so $p'\left(\frac{\omega_1}{2}\right) = -p'\left(-\frac{\omega_1}{2}\right)$ so $p'\left(\frac{\omega_1}{2}\right) = p'\left(-\frac{\omega_1}{2}\right) = 0$. Similarly, $p'\left(\frac{\omega_1}{2}\right) = 0$ and $p'\left(\frac{\omega_1+\omega_2}{2}\right) = 0$. Therefore, $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ and $\frac{\omega_1+\omega_2}{2}$ are zeros of p' of multiplicity one and there are no others.

Next, let $c \in \mathbb{C}$ and let $f(z) = p(z) - c$. Then f has a pole of order 2 (since p does) at every lattice point and no others. Thus, in any fundamental parallelogram, there will either be two distinct zeros of multiplicity 1 or one zero of multiplicity 2.
Suppose we have a zero of multiplicity 2 in P_0. Then that zero is a simple zero of p' hence it is one of $\frac{\omega_1}{2}$, $\frac{\omega_2}{2}$ or $\frac{\omega_1+\omega_2}{2}$. Thus, c is either $p\left(\frac{\omega_1}{2}\right), p\left(\frac{\omega_2}{2}\right)$ or $p\left(\frac{\omega_1+\omega_2}{2}\right)$. Note that if $c = p\left(\frac{\omega_1}{2}\right)$ then $\frac{\omega_1}{2}$ is the unique zero of f in P_0, and similarly for $\frac{\omega_2}{2}$ or $\frac{\omega_1+\omega_2}{2}$. The values of $p(z)$ at these three points are distinct. Indeed, suppose for example that $p\left(\frac{\omega_1}{2}\right) = p\left(\frac{\omega_2}{2}\right)$. Then $f\left(\frac{\omega_1}{2}\right) = f\left(\frac{\omega_2}{2}\right) = 0$, implying that f has more than one zero, a contradiction to our initial hypothesis.

Corollary 3. *$4p(z)^3 - g_2p(z) - g_3 = 4(p(z) - e_1)(p(z) - e_2)(p(z) - e_3)$, where $e_1 = p\left(\frac{\omega_1}{2}\right)$, $e_2 = p\left(\frac{\omega_2}{2}\right)$ and $e_3 = p\left(\frac{\omega_1+\omega_2}{2}\right)$, and e_1, e_2 and e_3 are distinct.*

Proof. The polynomial $q(x) = 4x^3 - g_2x - g_3$ has 3 distinct zeros, namely e_1, e_2 and e_3 as given in the statement, by theorem 1 which says that $q = p'$. The result follows. □

Consider $f(x) = 4x^3 - g_2x - g_3$. The discriminant D of f is $D = 4^4((e_1 - e_2)(e_2 - e_3)(e_1 - e_3))^2$. Further, $\text{Res}(f, f') = -4D$ so $D = 4^2(g_2^3 - 27g_3^2)$. Thus, if g_2 and g_3 came from a lattice L then $g_2^3 - 27g_3^2 \neq 0$ (for if $g_2^3 - 27g_3^2 = 0$, then the resultant is zero, implying that f has a repeated root, but as we just saw this is impossible).
We shall prove later that if $a, b \in \mathbb{C}$ and $a^3 - 27b^2 \neq 0$, there is a lattice L with $g_2(L) = a$ and $g_3(L) = b$.

Lecture 3: The Modular Group and its Action on the Upper Half Plane

Recall that

$$g_2(L) = 60 \sum_{\omega \in L'} \frac{1}{\omega^4} = 60 \sum_{(m,n)\neq(0,0)} \frac{1}{(m\omega_1 + n\omega_2)^4} = \frac{60}{\omega_2^4} \sum_{(m,n)\neq(0,0)} \frac{1}{\left(m\frac{\omega_1}{\omega_2} + n\right)^4},$$

for $L = [\omega_1, \omega_2]$. Similarly,

$$g_3(L) = 140 \sum_{\omega \in L'} \frac{1}{\omega^6} = \frac{140}{\omega_2^6} \sum_{(m,n)\neq(0,0)} \frac{1}{\left(m\frac{\omega_1}{\omega_2} + n\right)^6}.$$

Let H denote the upper half plane $H := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Define $G_k(z)$ for $k = 2, 3, \ldots$ by $G_k(z) = \sum_{(m,n)\neq(0,0)} \frac{1}{(mz+n)^{2k}}$ which is analytic in H. Further, the series converges uniformly on compact subsets of H to an analytic function on H. We now define $g_2(z)$ on H by $g_2(z) = 60G_2(z)$ and $g_3(z) = 140G_3(z)$ and $\Delta(z) = g_2^3(z) - 27g_3^2(z)$. Then $\Delta(z)$ is analytic and non-zero on H.

Definition 3. *The Special Linear Group $SL_2(\mathbb{R})$ is the set of 2×2 matrices with coefficients in $\mathbb{R}$ with determinant 1. We denote by $\pm I = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. The Projective Special Linear Group $PSL_2(\mathbb{R})$ is the quotient group $PSL_2(\mathbb{R}) := SL_2(\mathbb{R})/\{I, -I\}$.*

Definition 4. *The group $PSL_2(\mathbb{Z}) := SL_2(\mathbb{Z})/\{I, -I\}$ is known as the modular group.*

Let G be the modular group and let $g \in G$ with $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ (by this we mean the equivalence class modulo $\pm I$, but we shall abuse notation in this manner). Then g acts on H by $gz = \frac{az+b}{cz+d}$.

Remark. *Let $\mathcal{L}$ be the set of lattice on $\mathbb{C}$. For any lattice $L = [\omega_1, \omega_2]$ and an $\lambda \in \mathbb{C}\backslash\{0\}$ we can define the lattice $\lambda L := [\lambda\omega_1, \lambda\omega_2]$.*
Let k be a non-negative even integer. There is a bijection between the set of functions $F : \mathcal{L} \to \mathbb{C}$ which satisfy $F(\lambda L) = \lambda^{-k} F(L)$ for all $\lambda \in \mathbb{C}\backslash\{0\}$ and the set of functions $f : H \to \mathbb{C}$ such that $f(gz) = (cz + d)^k f(z)$ for all $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$.
To see this, let $\phi(F) = f$, where $f(z) = F([z, 1]) = F(L)$ for $L = [z, 1]$. Then

$$f(gz) = F([gz, 1]) = F\left(\left[\frac{az+b}{cz+d}, 1\right]\right) = F\left(\frac{1}{cz+d}\left[az+b, cz+d\right]\right) = (cz+d)^k F([az+b, cz+d])$$
$$= (cz+d)^k F([z,1]) = (cz+d)^k f(z)$$

where $[az + b, cz + d]$ is equal to the lattice $[z, 1]$ via the matrix g. Thus, ϕ is well-defined. It is easy to see that f is a bijection by definition.
For the sake of edification, let us see the other direction, i.e. suppose $f : H \to \mathbb{C}$ satisfies $f(gz) = (cz + d)^k f(z)$ for all $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$. For any $L = [\omega_1, \omega_2]$. We define $F(L) := \omega_2^{-k} f\left(\frac{\omega_1}{\omega_2}\right)$. Then

$$F(\lambda L) = F([\lambda\omega_1, \lambda\omega_2]) = (\lambda\omega_2)^{-k} f\left(\frac{\lambda\omega_1}{\lambda\omega_2}\right) = \lambda^{-k} F(L).$$

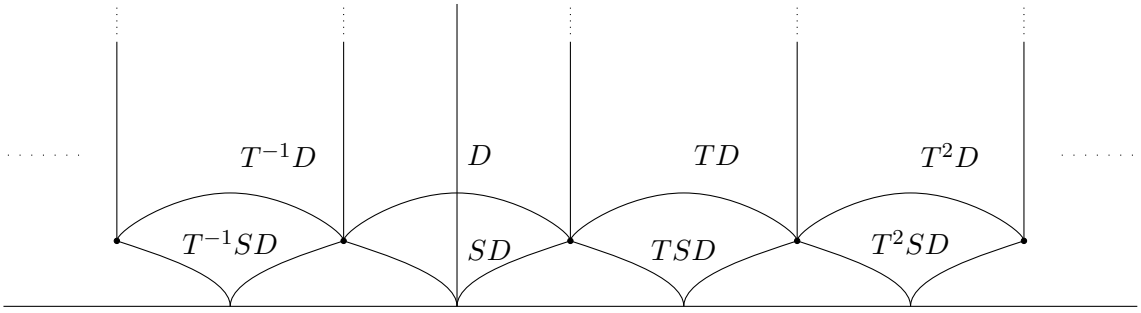

FIGURE 3. Covering $\mathbb{C}$ with Transformations of D

Note that F is invariant under the action of $PSL_2(\mathbb{Z})$ on L since the generators change. Recall that $\Delta(z) = g_2(z)^3 - 27g_3(z)^2$. We can check that $\Delta(gz) = (cz+d)^{12}\Delta(z)$.

LECTURE 4: THE ACTION OF THE MODULAR GROUP G ON H

Let $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ so that $Sz = -\frac{1}{z}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ so $Tz = z+1$. Notice that $S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{\{I, -I\}}$ and $(ST)^3 \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{\{I, -I\}}$.

Let D denote the set $D := \{z \in H : -\frac{1}{2} \leq \mathrm{Re}(z) \leq \frac{1}{2}, |z| \geq 1\}$. We'll prove that D is the fundamental domain of the modular group, i.e. the orbit of each element of G under the action of G contains an element of D. Further, if it contains 2 elements of D then these elements are on the boundary of D.

Theorem 2. *Let $G = SL_2(\mathbb{Z})/\{I, -I\}$.*

1. *For all $z \in H$ there exists $g \in G$ such that $gz \in D$.*
2. *Let $z_1, z_2 \in D$ with $gz_1 = z_2$ and $z_1 \neq z_2$ and $g \in G$. Then either $Re(z_1) = \pm\frac{1}{2}$ and $z_2 = z_1 \pm 1$ or $|z_1| = 1$ and $z_2 = -\frac{1}{z_1}$.*
3. *Let $z \in D$ and put $Stab_G(z) := \{g \in G : gz = z\}$. Then $Stab_G(z) = \{I\}$ if $z \in \{i, e^{\frac{\pi i}{3}}, e^{\frac{2\pi i}{3}}\}$. We have $Stab_G(i) = \{I, S\}$ and $Stab_G\left(e^{\frac{2\pi i}{3}}\right) = \{I, ST, (ST)^2\}$ and $Stab_G\left(e^{\frac{\pi i}{3}}\right) = \{I, TS, (TS)^2\}$.*
4. *G is generated by S and T.*

Proof. (1) Let G' be the subgroup of G generated by S and T. We will show that for all $z \in H$ there exists $g \in G'$ such that $gz \in D$. First, note that if $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ then

$$\begin{aligned} \mathrm{Im}(gz) = \mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \mathrm{Im}\left(\frac{(az+b)(c\overline{z}+d)}{|cz+d|^2}\right) &= \frac{1}{|cz+d|^2}\mathrm{Im}\left(ac|z|^2 + bd + adz + bc\overline{z}\right) \\ = \frac{1}{|cz+d|^2}\left(ad\mathrm{Im}(z) + bc\mathrm{Im}(\overline{z})\right) &= \frac{(ad-bc)\mathrm{Im}(z)}{|cz+d|^2} = \frac{\mathrm{Im}(z)}{|cz+d|^2} \end{aligned}$$

Next, observe that c and d are integers and $|cz+d| \to \infty$ as $\max(|c|, |d|) \to \infty$. Thus $\mathrm{Im}(gz)$ achieves a maximum for some $g \in G$.

Suppose $g \in G'$ is such that $\mathrm{Im}(gz)$ is maximal. We can then translate so that gz has real part in $\left[-\frac{1}{2}, \frac{1}{2}\right]$. In particular there exists an integer n with $-\frac{1}{2} \leq \mathrm{Re}(T^n gz) \leq \frac{1}{2}$ with unchanged imaginary part. We need to show that $|T^n gz| \geq 1$. Suppose that $|T^n gz| < 1$. Then applying S gives $|ST^n gz| > 1$ and $\mathrm{Im}(ST^n gz) > \mathrm{Im}(T^n gz) = \mathrm{Im}(gz)$, with $ST^n g \in G'$. Indeed, if $w = T^n gz$ so $|w| < 1$, then

$$\mathrm{Im}(Sw) = \mathrm{Im}\left(-\frac{1}{w}\right) = \mathrm{Im}\left(\frac{-\overline{w}}{|w|^2}\right) = \frac{1}{|w|^2}\mathrm{Im}(w) > \mathrm{Im}(w)$$

But then gz does not have maximal imaginary part, and this is a contradiction. It follows that $|T^n gz| \geq 1$ so that $g'z \in D$ for $g' = T^n g \in G'$.

(2) Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$ with $gz_1 = z_2$, $z_1, z_2 \in D$. Without loss of generality, assume $\mathrm{Im}(z_1) \leq \mathrm{Im}(z_2)$ (otherwise we can pick $z_2 = gz_1$ so $z_1 = g^{-1}z_2$ to make this the case). Since $\mathrm{Im}(gz_1) = \frac{1}{|cz+d|^2}\mathrm{Im}(z_1)$, we see that $|cz_1 + d| \leq 1$. Observe that if $\theta \in D$ then $\mathrm{Im}(\theta) \geq \frac{\sqrt{3}}{2}$ (since $\mathrm{Re}(\theta) \in \left[-\frac{1}{2}, \frac{1}{2}\right]$, then $\frac{\pi}{3} \leq z_1 \leq \frac{2\pi}{3}$). Thus,

$$1 \geq |cz_1 + d|^2 \geq \mathrm{Im}(cz_1 + d)^2 = c^2\mathrm{Im}(z_1)^2$$

and hence $|c| < 2$, so that $c = 0, 1$ or -1. If $c = 0$ then we have $a = d = \pm 1$ since $|cz_1 + d| \leq 1$ and $d \neq 0$ for the determinant to be non-zero. Then $gz_1 = z_1 \pm b$ hence is a translation by $\pm b$. Therefore the translation is either by 0,1 or -1 since $z_1, z_2 \in D$. If $b = 0$, $z_1 = z_2$, otherwise $\mathrm{Re}(z_1) = \pm\frac{1}{2}$ and $z_2 = z_1 \pm 1$.
If $c = 1$ then $d = 0, \pm 1$. If $d = 1$, $|cz_1 + d| = |z_1 + 1| \leq 1$. This is only possible if $z_1 + 1$ is on the arc of the unit disc (since $z_2 \in D$ so $|z_2| \geq 1$ as well), and since $z_1 \in D$, $z_1 = \mathrm{e}^{\frac{2\pi i}{3}}$. Further, if $d = -1$, then $|cz_1 + d| = |z_1 - 1| \leq 1$ so similarly $z_1 = \mathrm{e}^{\frac{\pi i}{3}}$. Finally, if $d = 0$, $|z_1| \leq 1$ so $|z_1| = 1$ $\frac{az_1 - 1}{z_1} = a - \frac{1}{z_1}$ ($-bc = 1$ so $b = -1$). But then $\left|\frac{1}{z_1}\right| = 1$. Thus, either $a = 0$ and $gz_1 = -\frac{1}{z_1}$ or $a = 1$ and by the reasoning above, $-\frac{1}{z_1} = \mathrm{e}^{\frac{2\pi i}{3}}$ i.e. $z_1 = \mathrm{e}^{\pi i + \frac{4\pi i}{3}} = \mathrm{e}^{\frac{\pi i}{3}}$ and if $a = -1$, $z_1 = \mathrm{e}^{\frac{2\pi i}{3}}$. Finally, if $c = -1$, the same analysis works by taking $(a, b, c, d) \mapsto (-a, -b, -c, -d)$.

(3) By the analysis in (2), if $z_1 \in D$ and $gz_1 = z_1$, then $|cz_1 + d| = 1$. If $c = 1$ then $d = 0, 1, -1$. If $c = 1$, $d = 0$ then $|z_1| = 1$ and $b = -1$. Since $gz_1 = z_1$, $\frac{az_1 - 1}{z_1} = a - \frac{1}{z_1} = z_1$ hence since $|z_1| = 1$, we have $a = 0$ hence $z = i$, or $a = 1$ so that $z_1^2 - z_1 + 1 = 0$ so $z_1 = \mathrm{e}^{\frac{\pi i}{3}}$ or $a = -1$ so $z_1 = \mathrm{e}^{\frac{2\pi i}{3}}$. Similarly, if $c = 1$ and $d = 1$ then since $|cz_1 + d| = |z_1 - 1| \leq 1$ we find that $z_1 = \mathrm{e}^{\frac{2\pi i}{3}}$. Further, if $c = 1$ and $d = -1$, $z_1 = \mathrm{e}^{\frac{\pi i}{3}}$. To conclude, $\mathrm{Stab}_G(i) = \{1, S\}$, $\mathrm{Stab}_G\left(\mathrm{e}^{\frac{2\pi i}{3}}\right) = \{1, ST, (ST)^2\}$, $\mathrm{Stab}_G\left(\mathrm{e}^{\frac{\pi i}{3}}\right) = \{1, TS, (TS)^2\}$.

(4) Let $g \in G$ and let $z_0 \in \mathrm{Int}(D)$. Then $gz_0 \in H$. By our proof of (1), there exists $g' \in G'$ generated by S and T such that $g'gz_0 \in D$. Since $z_0 \in \mathrm{Int}(D)$, it cannot be any of the options in (2) so $g'gz_0 = z_0$, but since the stabilizer is trivial in this case, $g'g = I$. Thus, $g = (g')^{-1} \in G'$, so $G \subseteq G'$. □

In fact $\langle S, T; S^2 = I, (ST)^3 = I \rangle$ is a presentation for G. In other words, G is a free product of a cyclic group of order 2 and one of order 3.

Definition 5. *A meromorphic function on H satisfying $f(z) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right)$ for all $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ is said to be <u>weakly modular</u> of weight $2k$.*

Remark. *Observe that* $\frac{d(gz)}{dz} = \frac{1}{(cz+d)^2}$, *hence if* f *is weakly modular of weight* $2k$ *then* $f(z)(dz)^k = f(gz)(d(gz))^k$. *Since* S *and* T *generate* G, *to check whether* f *is weakly modular, we need only check:*

(1) $f(z) = f(Tz) = f(z+1)$
(2) $f(z) = z^{-2k} f\left(\frac{-1}{z}\right)$

Let $U := \{z \in \mathbb{C} : |z| < 1\}$ and $U^* = U \backslash \{0\}$. Let $q : H \to U^*$, $q(z) = \mathrm{e}^{2\pi i z}$. Given a weakly modular function $f : H \to \mathbb{C}$ we can define $f^* : U^* \to \mathbb{C}$ by $f^*(q(z)) = f^*\left(\mathrm{e}^{2\pi i z}\right) = f(z)$, since f is periodic (and thus $f(z) = f(z+1)$). Note that $f^* \circ q = f$ and $q^{-1}(z) = \frac{\log(z)}{2\pi i}$ for some branch of the logarithm.
Since f is meromorphic on H, f^* is meromorphic on U^*. If f^* extends to a meromorphic function on U then we say that f is meromorphic at infinity. Similarly, if f is analytic on H and f^* extends to an analytic function on U, we say that f is analytic at infinity.

Suppose that f is not identically zero, that it is weakly modular of weight $2k$ and meromorphic at infinity. Then it has only finitely many zeros and finitely many poles in D. For suppose that there were infinitely many zeros in D. Then the origin would be an accumulation point of zeros for f^*, hence f^* would be identically zero. Similarly, if there are infinitely many poles in D, the origin would be an accumulation point of poles for f^* would not be meromorphic.

Definition 6. *A weakly modular function is said to be* modular *if it is meromorphic at infinity.*

Definition 7. *A* modular form *is a modular function that is analytic on* H *and analytic at infinity.*

Definition 8. *A modular form is called a* cusp form *if it is 0 at infinity.*

Lectures 5 and 6: Relating the Weight of a Modular Function to the Orders of Zeros and Poles

For any $z_0 \in H$ and f modular, define $\mathrm{ord}_{z_0}(f)$ to be the integer n such that $\frac{f(z)}{(z-z_0)^n}$ is analytic and non-zero in a neighbourhood of z_0. Suppose f is of weight $2k$. Let $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be in the modular group. Since $f(z) = (cz+d)^{-2k} f(gz) = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right)$, we see that $\mathrm{ord}_{z_0}(f) = \mathrm{ord}_{gz_0}(f)$. We define $\mathrm{ord}_\infty(f) := \mathrm{ord}_0(f^*)$.
Lt $D' = D \backslash (A_1 \cup A_2)$ where $A_1 := \{z \in D : \mathrm{Re}(z) = \frac{1}{2}\}$ and $A_2 := \{z \in D : |z| = 1, \mathrm{Re}(z) > 0\}$, as in Figure 4.

Theorem 3. *Let* f *be a modular function of weight* $2k$ *which is not identically zero. Then*

$$ord_\infty(f) + \frac{1}{2} ord_i(f) + \frac{1}{3} ord_{e^{\frac{2\pi i}{3}}}(f) + \sum_{\substack{z_0 \in D' \\ z_0 \neq i, e^{\frac{2\pi i}{3}}}} ord_{z_0}(f) = \frac{k}{6}$$

Proof. We'll first prove this under the assumption that f has no zeros or poles on the boundary of D.
In this case, we consider a path Γ given by $ABCDE$ in Figure 5 where $B = \mathrm{e}^{\frac{2\pi i}{3}}$, $C = i$, $D = \mathrm{e}^{\frac{\pi i}{3}}$ and D and E have real part $\frac{1}{2}$. Further, A and E have the same imaginary part chosen large enough that the

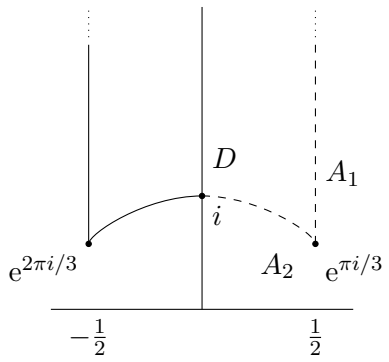

FIGURE 4. The Region $D' = D\backslash(A_1, \cup A_2)$

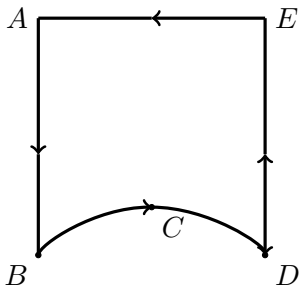

FIGURE 5. Path of Integration Γ

region enclosed by Γ contains all of the zeros and poles of f (since f is meromorphic and thus can only have finitely many of each). By the argument principle, we have

$$\frac{1}{2\pi i}\int_\Gamma \frac{f'(z)}{f(z)}dz = \sum_{z_0 \in D'} \mathrm{ord}_{z_0}(f)$$

Notice that $\frac{f'(Tz)}{f(Tz)}d(Tz) = \frac{f'(z)}{f(z)}dz$, so

$$\frac{1}{2\pi i}\int_A^B \frac{f'(z)}{f(z)}dz = -\frac{1}{2\pi i}\int_D^E \frac{f'(z)}{f(z)}dz$$

Next, observe that S transforms the arc BC to the arc DC. Also, note that $f(Sz) = z^{2k}f(z)$ since f is modular of weight $2k$. Therefore,

$$\frac{f'(Sz)}{f(Sz)}d(Sz) = \frac{2kz^{2k-1}f(z) + z^{2k}f'(z)}{z^{2k}f(z)}dz = \left(\frac{2k}{z} + \frac{f'(z)}{f(z)}\right)dz$$

Thus,

$$\int_B^C \frac{f'(z)}{f(z)}dz + \int_C^D \frac{f'(z)}{f(z)}dz = \int_B^C \left(\frac{f'(z)}{f(z)} - \frac{2k}{z} - \frac{f'(z)}{f(z)}\right)dz = -2k\int_B^C \frac{dz}{z}$$

Make a chance of variables under $z = \mathrm{e}^{i\theta}$ then

$$\int_B^C \frac{dz}{z} = \int_{\frac{2\pi}{3}}^{\frac{\pi}{2}} \frac{i\mathrm{e}^{i\theta}}{\mathrm{e}^{i\theta}} d\theta = \int_{\frac{2\pi}{3}}^{\frac{\pi}{2}} i d\theta = -\frac{\pi i}{6}$$

Thus, $\frac{1}{2\pi i}\left(\int_B^C \frac{f'(z)}{f(z)}dz + \int_C^D \frac{f'(z)}{f(z)}dz\right) = \frac{-2k}{2\pi i}\frac{-\pi i}{6} = \frac{k}{6}$.

Finally, we consider $\frac{1}{2\pi i}\int_E^A \frac{f'(z)}{f(z)}dz$. To evaluate it we change variables by $q = \mathrm{e}^{2\pi i z}$. Suppose that the segment $EA = \{\lambda + iM : -\frac{1}{2} \leq \lambda \leq \frac{1}{2}\}$ for some $M > 0$. As we traverse from E to A we move along a circle in the q-plane of radius $\mathrm{e}^{-2\pi M}$ in the negative (clockwise) direction.

We have $f^*(q) = f(z)$ and f^* is analytic and non-zero in the disc of radius $\mathrm{e}^{-2\pi M}$ except perhaps at the origin. Thus

$$\frac{1}{2\pi i}\int_E^A \frac{f'(z)}{f(z)}dz = -\frac{1}{2\pi i}\int_C \frac{(f^*(q))'}{f^*(q)}dq$$

where C is the path in the counterclockwise direction given by the circle of radius $\mathrm{e}^{-2\pi M}$. By the argument principle,

$$\frac{1}{2\pi i}\int_C \frac{(f^*(q))'}{f^*(q)}dq = \mathrm{ord}_0(f^*) = \mathrm{ord}_\infty(f).$$

Therefore, in the case that f has a no zeroes or poles on the boundary,

$$\mathrm{ord}_\infty(f) + \sum_{z_0 \in D'} \mathrm{ord}_{z_0}(f) = \frac{k}{6}$$

We now consider the possibility that we have zeroes or poles on the boundary of D. Note that we have only finitely many zeroes or poles so they are all isolated.

Suppose first that we have a zero or pole with $\mathrm{Re}(z) = -\frac{1}{2}$ amd $z \neq \mathrm{e}^{\frac{2\pi i}{3}}$. We modify the contour Γ by introducing a small semi-circle around z and a corresponding semicircle around Tz. We make the semicircle sufficiently small that the circle it determines encloses no other zeros or poles of f and that its endpoints are strictly within the segment AB.

The integerals along AB and DE cancel as before. In fact for each zero or pole of f and AB apart from $\mathrm{e}^{\frac{2\pi i}{3}}$, we introduce such a semicircle and the result holds.

Next, suppose z_2 is a zero or pole of f on the segment BC and different from $\mathrm{e}^{\frac{2\pi i}{3}}$ and i. We modify the contour Γ by introducing semicircles around z_2 for which the circle determined strictly inside BC. We also modify the contour by the image of the semicircle under S. Letting the radius of the semicircle tend to 0 we again find the contribution of the integral from B to D to be $\frac{k}{6}$. We can do this in general for any zero or pole on the interior of BC by making a similar modification.

It remains to consider the possibility of a pole or zero for f at $\omega = \mathrm{e}^{\frac{2\pi i}{3}}$ and i. We modify Γ by introducing a small arc around ω and a corresponding arc around $\mathrm{e}^{\frac{\pi i}{3}}$. Thus, the arc C is part of a circle around ω chosen so that that disc determined by the circle contains no other zeros or poles of f. We will let the radius r of the disc tend to 0. Let C_1 be the set of points $\omega + r\mathrm{e}^{i\theta}$ where θ varies from $\frac{\pi}{2}$ to α where α depends on r. Assume now that $f(z) = (z-\omega)^t g(z)$ where g is analytic and non-zero in a neighbourhood of ω. So t is the order of f at ω (of either a pole or a zero). On C_1, $z - \omega = r\mathrm{e}^{i\theta}$, so

$$\frac{f'(z)}{f(z)} = \frac{t}{z-\omega} + \frac{g'(z)}{g(z)}$$

Thus,

$$\frac{1}{2\pi i}\int_{C_1}\frac{f'(z)}{f(z)}dz = \frac{1}{2\pi i}\int_{C_1}\left(\frac{t}{z-\omega}+\frac{g'(z)}{g(z)}\right)dz = \frac{1}{2\pi i}\int_{\frac{\pi}{2}}^{\alpha}\frac{t}{re^{i\theta}}ire^{i\theta}d\theta + \frac{1}{2\pi i}\int_{\frac{\pi}{2}}^{\alpha}ire^{i\theta}\frac{g'(\omega+re^{i\theta})}{g(\omega+re^{i\theta})}d\theta$$
$$= \frac{1}{2\pi}\int_{\frac{\pi}{2}}^{\alpha}td\theta + \frac{1}{2\pi}\int_{\frac{\pi}{2}}^{\alpha}re^{i\theta}\frac{g'(\omega+re^{i\theta})}{g(\omega+re^{i\theta})}d\theta$$

Letting $r\to 0$, the second term vanishes and the first terms tends to

$$\lim_{r\to 0}\frac{t}{2\pi}\int_{\frac{\pi}{2}}^{\alpha(r)}d\theta = \frac{t}{2\pi}\lim_{r\to 0}\left(\alpha(r)-\frac{\pi}{2}\right) = -\frac{t}{2\pi}\frac{\pi}{3} = -\frac{t}{6}$$

Similarly, $\int_{C_2}\frac{f'(z)}{f(z)}dz = -\frac{t}{6}$, hence the contribution over C_1 and C_2 is $-\frac{t}{3}$, where C_2 is the reflection of the set of points in C_1 on the other side of the imaginary axis.
Finally, we consider the case when f has a zero or pole at i. Say $f(z) = (z-i)^l g(z)$ with $g(z)$ analytic and non-zero in a neighbourhood of i. We introduce a small semicircle of radius r around i to the contour Γ. Choose r sufficiently small that no other zeros of poles of f are inside the disc of radius r around i. Arguing as before we find a contribution of $-\frac{t}{2}$ to the integral. □

Consider the series $\sum_{n\in\mathbb{Z}}\frac{1}{(z-n)^2}$ and let $f(z)$ be the function of z on $\mathbb{C}$ determined by the series. Any compact subset $K\subseteq\mathbb{C}$ lies inside a disc of radius T around 0. If we remove from the series the terms $\frac{1}{(z-n)^2}$ with n at most T in absolute value, the remaining series converges uniformly on K since $\sum_n\frac{1}{n^2}$ converges. Therefore, $\sum_{n\in\mathbb{Z}}\frac{1}{(z-n)^2}$ converges uniformly on compact subsets to a meromorphic function $f(z)$ on $\mathbb{C}$. The integers are double poles of residue 0 since in a neighbourhood of n, f is of the form $\frac{1}{(z-n)^2}$ plus an analytic function. There are no other poles of f.
Let $g(z) = \left(\frac{\pi}{\sin\pi z}\right)^2$. Notice that g has a double pole at each integer and no other poles. Further, in a neighbourhood of 0,

$$\left(\frac{\pi}{\sin\pi z}\right)^2 = \left(\frac{\pi}{\pi z-\frac{1}{6}(\pi z)^3+\dots}\right)^2 = \frac{1}{z^2}\left(1-\frac{\pi z}{6}+\dots\right)^{-2} = \frac{1}{z^2}+\frac{\pi^2}{3}+\dots$$

so $\left(\frac{\pi}{\sin\pi z}\right)^2-\frac{1}{z^2} = \frac{\pi^2}{3}+\dots$.
Note that $f(z)-g(z)$ is analytic in a neighbourhood of 0 and by periodicity in a neighbourhood of each integer. Thus, $f(z)-g(z)$ is analytic on $\mathbb{C}$.
Notice that if $z = x+iy$ with $x,y\in\mathbb{R}$ then

$$\frac{1}{|z-n|^2} = \frac{1}{|(x-n)+iy|^2}\to 0$$

as $y\to\infty$. Further,

$$|\sin\pi z| = \frac{1}{2}\left|e^{i\pi z}-e^{-i\pi z}\right| = \frac{1}{2}\left|e^{i\pi x}e^{-\pi y}-e^{-i\pi z}e^{\pi y}\right|\to\infty$$

as $|y|\to\infty$.
Thus, $f(z)-g(z)\to 0$ uniformly as $|y|\to\infty$. Therefore, $f(z)-g(z)$ is a bounded analytic function and so is a constant by Liouville's theorem.
Further, the constant is 0 hence $f(z) = g(z)$ on $\mathbb{C}$.

Now observe that $\left(\frac{\pi}{\sin \pi z}\right)^2 - \frac{1}{z^2} = \sum_{\substack{n\in\mathbb{Z}\\ n\neq 0}} \frac{1}{(z-n)^2}$, which in a neighbourhood of 0 is an analytic function $\frac{\pi^2}{3}$. Letting $z \to 0$, we see that $2\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{3}$.
Now consider

$$F(z) = \frac{1}{z} + \sum_{\substack{n\in\mathbb{Z}\\ n\neq 0}} \left(\frac{1}{z-n} + \frac{1}{n}\right)$$

Using the fact that $\sum_{n=1}^{\infty} \frac{1}{n^2}$ converges, we see that the series defining F converges uniformly on compact subsets to a meromorphic function on $\mathbb{C}$. Thus, the series of derivatives converges uniformly on compact subsets to the derivative of the function. Thus,

$$-\sum_{n\in\mathbb{Z}} \frac{1}{(z-n)^2} = -\left(\frac{\pi}{\sin \pi z}\right)^2 = \frac{d}{dz}(\pi \cot \pi z)$$

Thus, $F(z) - \pi \cot \pi z$ is a constant.
Notice that by definition, $F(-z) = -F(z)$. Further, $\pi \cot \pi z$ is an odd function. Thus, $F(z) - \pi \cot \pi z$ is an odd function. Since it is constant, it must be 0. Thus, $F(z) = \pi \cot \pi z$. Therefore,

$$\pi \cot \pi z = \frac{1}{z} + \sum_{n\neq 0} \left(\frac{1}{z-n} + \frac{1}{n}\right)$$

Now since $\frac{1}{z-n} + \frac{1}{n} + \frac{1}{z+n} - \frac{1}{n} = \frac{2z}{z^2-n^2}$, we have

$$\pi \cot \pi z = \frac{1}{z} + \sum_{n\geq 1} \frac{2z}{z^2-n^2}$$

Lecture 7: Series Expansions for $g_2(z)$ and $g_3(z)$ on H

We'll now extablish the q-expansions for g_2 and g_3.

Lemma 1. *If $z \in H$ and $n \in \mathbb{N}$ then*

$$\sum_{m\in\mathbb{Z}} \frac{1}{(m+nz)^4} = \frac{8\pi^4}{3} \sum_{r=1}^{\infty} r^3 e^{2\pi r n z}$$
$$\sum_{m\in\mathbb{Z}} \frac{1}{(m+nz)^6} = -\frac{8\pi^6}{15} \sum_{r=1}^{\infty} r^5 e^{2\pi r n z}$$

Proof. We start with the expansion

$$\pi \cot \pi z = \frac{1}{z} + \sum_{\substack{m\in\mathbb{Z}\\ m\neq 0}} \left(\frac{1}{z+m} - \frac{1}{m}\right)$$

Let $q = \mathrm{e}^{2\pi i z}$. If $z \in H$, $\mathrm{Im}(z) > 0$ and thus $|q| < 1$. Hence,

$$\pi \cot \pi z = \pi \frac{\cos \pi z}{\sin \pi z} = \pi i \frac{\mathrm{e}^{\pi i z} + \mathrm{e}^{-\pi i z}}{\mathrm{e}^{\pi i z} - \mathrm{e}^{-\pi i z}} = \pi i \frac{q+1}{q-1} = -\pi i (q+1) \sum_{r=0}^{\infty} q^r = -\pi i \left(1 + 2\sum_{r=1}^{\infty} q^r\right)$$

Thus, if $z \in H$ then

$$\frac{1}{z} + \sum_{\substack{m \in \mathbb{Z} \\ m \neq 0}} \left(\frac{1}{z+m} - \frac{1}{m} \right) = -\pi i \left(1 + 2 \sum_{r=1}^{\infty} q^r \right)$$

Differentiating repeatedly with respect to z to give terms with denominators in powers of 4 and powers of 6 using the identity $\frac{dq}{dz} = 2\pi i q$ results in the series

$$-(3!) \sum_{m \in \mathbb{Z}} \frac{1}{(z+m)^4} = -(2\pi i)^4 \sum_{r=1}^{\infty} r^3 \mathrm{e}^{2\pi i z}$$

$$-(5!) \sum_{m \in \mathbb{Z}} \frac{1}{(z+m)^6} = -(2\pi i)^6 \sum_{r=1}^{\infty} r^5 \mathrm{e}^{2\pi i z}$$

Substituting nz in the place of z proves the result. □

Define the Riemann Zeta function $\zeta(z)$ by the series $\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}$ for $\mathrm{Re}(z) > 1$. The zeta function may be analytically continued to all of $\mathbb{C}$ with the exception of a simple pole at $z = 1$. It is conjectured that all zeros of $\zeta(z)$ in $\mathrm{Re}(z) > 0$ have $\mathrm{Re}(z) = \frac{1}{2}$. This is the Riemann Hypothesis.

Put, for z in a neighbourhood of 0,

$$\frac{z}{\mathrm{e}^z - 1} = \sum_{k=0}^{\infty} \frac{b_k}{k!} z^k$$

Notice that $b_0 = 1$ and $b_1 = -\frac{1}{2}$ by differentiating the left side and setting $z = 0$. Further, observe that

$$\frac{-z}{\mathrm{e}^{-z} - 1} - 1 + \frac{-z}{2} = \frac{z\mathrm{e}^z}{\mathrm{e}^z - 1} - 1 - \frac{z}{2} = \frac{z(\mathrm{e}^z - 1)}{\mathrm{e}^z - 1} + \frac{z}{\mathrm{e}^z - 1} - 1 - \frac{z}{2} = \frac{z}{2} + \frac{z}{\mathrm{e}^z - 1} - 1$$

so that $\frac{z}{\mathrm{e}^z - 1} - 1 + \frac{z}{2}$ is an even function. Thus, $b_{2k+1} = 0$ for $k \in \mathbb{N}$. We now put $b_{2k} = (-1)^{k+1} B_k$ for $k \in \mathbb{N}$. We can write

$$\frac{z}{\mathrm{e}^z - 1} = 1 - \frac{z}{2} + \sum_{k=1}^{\infty} (-1)^{k+1} B_k \frac{z^{2k}}{(2k!)}$$

The numbers $\{B_k\}_{k=1}^{\infty}$ are called Bernoulli numbers. We have $B_1 = \frac{1}{6}$, $B_2 = \frac{1}{30}$, $B_3 = \frac{1}{42}$ and so forth.

Theorem 4 (Euler)**.** *Let $k \in \mathbb{N}$. Then*

$$\zeta(2k) = \frac{2^{2k-1} B_k \pi^{2k}}{(2k)!}$$

Proof. We have

$$\frac{z}{\mathrm{e}^z - 1} + \frac{z}{2} = 1 + \sum_{k=1}^{\infty} (-1)^{k+1} B_k \frac{z^{2k}}{(2k)!}$$

Write $z = 2iu$ to get

$$\frac{2iu}{\mathrm{e}^{2iu} - 1} + iu = 1 - \sum_{k=1}^{\infty} B_k \frac{2^k u^k}{(2k)!} \tag{1}$$

Recall for $z \in H$,

$$\pi z \cot \pi z = 1 + 2\sum_{n=1}^{\infty} \frac{z^2}{z^2 - n^2}$$

Thus,

$$\begin{aligned} u \cot u &= 1 - 2\sum_{n=1}^{\infty} \frac{u^2}{\pi^2 n^2 - u^2} = 1 - 2\sum_{n=1}^{\infty} \frac{u^2}{\pi^2 n^2} \frac{1}{1 - \left(\frac{u}{\pi n}\right)^2} \\ &= 1 - 2\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \left(\frac{u^2}{\pi^2 n^2}\right)^k = 1 - 2\sum_{k=1}^{\infty} \left(\frac{u^2}{\pi^2}\right)^k \sum_{n=1}^{\infty} \frac{1}{n^{2k}} \\ &= 1 - 2\sum_{k=1}^{\infty} \frac{u^{2k}}{\pi^{2k}} \zeta(2k) \end{aligned}$$

Also, (1) has the form

$$\frac{2iu}{\mathrm{e}^{iu} - 1} + iu = iu\left(\frac{\mathrm{e}^{iu} + 1}{\mathrm{e}^{iu} - 1}\right) = u \cot u = 1 - 2\sum_{k=1}^{\infty} \frac{u^{2k}}{\pi^{2k}} \zeta(2k)$$

Thus we need only compare this to (1) to establish the result. □

Thus, $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$, $\zeta(6) = \frac{\pi^6}{945}$ and so forth.

Theorem 5. *If $z \in H$ then*

$$\begin{aligned} g_2(z) &= \frac{4\pi^4}{3}\left(1 + 240\sum_{k=1}^{\infty} \sigma_3(k) e^{2\pi i k z}\right) \\ g_3(z) &= \frac{8\pi^6}{27}\left(1 - 504\sum_{k=1}^{\infty} \sigma_5(k) e^{2\pi i k z}\right) \end{aligned}$$

where $\sigma_r(k) = \sum_{d|k} d^r$ for $r \in \mathbb{N}$.

Proof. For $z \in H$,

$$\begin{aligned} g_2(z) &= 60 \sum_{(m,n)\neq(0,0)} \frac{1}{(m+nz)^4} = 60\left[\sum_{\substack{m\in\mathbb{Z}\\ m\neq 0}} \frac{1}{m^4} + \sum_{n=1}^{\infty}\sum_{m\in\mathbb{Z}} \left(\frac{1}{(m+nz)^4} + \frac{1}{(m-nz)^4}\right)\right] \\ &= 60\left[2\zeta(4) + 2\sum_{n=1}^{\infty}\sum_{m\in\mathbb{Z}} \frac{1}{(m+nz)^4}\right] = 60\left[\frac{\pi^4}{45} + \frac{16\pi^4}{3}\sum_{n=1}^{\infty}\sum_{r=1}^{\infty} r^3 \mathrm{e}^{2\pi i r n z}\right] \end{aligned}$$

by Lemma 1. By counting all of the indices r and n such that the products $rn = k$ are constant, we can simply index by k and count all of the divisors r of k. Counting in this manner produces

$$g_2(z) = \frac{4\pi^4}{3}\left[1 + 240\sum_{k=1}^{\infty} \mathrm{e}^{2\pi i k z} \sum_{r|k} r^3\right] = \frac{4\pi^4}{3}\left[1 + 240\sum_{k=1}^{\infty} \sigma_3(k) \mathrm{e}^{2\pi i k z}\right]$$

Similarly, for $g_3(z)$ we have

$$g_3(z) = 140 \sum_{(m,n)\neq(0,0)} \frac{1}{(m+nz)^6} = 140 \left[\sum_{\substack{m\in\mathbb{Z}\\ m\neq 0}} \frac{1}{m^6} + \sum_{n=1}^{\infty} \sum_{m\in\mathbb{Z}} \left(\frac{1}{(m+nz)^6} + \frac{1}{(m-nz)^6} \right) \right]$$
$$= 140 \left[2\zeta(6) + 2\sum_{n=1}^{\infty} \sum_{m\in\mathbb{Z}} \frac{1}{(m+nz)^6} \right] = 140 \left[\frac{2\pi^6}{945} - \frac{16\pi^6}{15} \sum_{n=1}^{\infty} \sum_{r=1}^{\infty} r^5 \mathrm{e}^{2\pi i r n z} \right]$$

again by Lemma 1. By a similar argument as above, evaluating the double infinite series as a sum over divisor sums gives the desired result. □

Notice that g_2 and g_3 are analytic on H and analytic and non-zero at infinity. In particular, $\mathrm{ord}_\infty g_2 = 0 = \mathrm{ord}_\infty g_3$ so g_2 and g_3 are modular forms.
g_2 has weight 4 and g_3 has weight 6. By Theorem 3,

$$\mathrm{ord}_\infty g_2 + \frac{1}{3}\mathrm{ord}_{\mathrm{e}^{2\pi i/3}} g_2 + \frac{1}{2}\mathrm{ord}_i g_2 + \sum_{\substack{z_0\in D'\\ z_0\neq i, \mathrm{e}^{2\pi i/3}}} \mathrm{ord}_{z_0} g_2 = \frac{1}{3}$$

since here $k = 2$. However, since g_2 is analytic, it has no poles so all of these orders are non-negative integers. This equality can only be satisfied if g_2 has a simple zero at $\mathrm{e}^{\frac{2\pi i}{3}}$ and no others in D'. Similarly,

$$\mathrm{ord}_\infty g_3 + \frac{1}{3}\mathrm{ord}_{\mathrm{e}^{2\pi i/3}} g_3 + \frac{1}{2}\mathrm{ord}_i g_3 + \sum_{\substack{z_0\in D'\\ z_0\neq i, \mathrm{e}^{2\pi i/3}}} \mathrm{ord}_{z_0} g_3 = \frac{1}{2}$$

since here $k = 3$. By the same argument as above, g_3 has a simple zero at i and no others in D'.

Lecture 8: The Δ function and Related Fourier Expansions

Recall that $\Delta(z) = g_2(z)^3 - 27g_3(z)^2$.

Theorem 6. *For $z \in H$*

$$\Delta(z) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) e^{2\pi i n z}$$

where $\tau(1) = 1$, $\tau(2) = -24$ etc. The function $\tau : \mathbb{N} \to \mathbb{Z}$ is called the Ramanujan τ-function.

Proof. Put

$$A := A(z) = \sum_{n=1}^{\infty} \sigma_3(n) \mathrm{e}^{2\pi i n z}$$
$$B := B(z) = \sum_{n=1}^{\infty} \sigma_5(n) \mathrm{e}^{2\pi i n z}$$

Then by theorem 5,

$$\Delta(z) = g_2(z)^3 - 27g_3(z)^2 = \frac{64\pi^{12}}{27}\left((1+240A)^3 - (1-504B)^2\right)$$
$$= \frac{64\pi^{12}}{27}\left(12^2(5A+7B) + 12^3(100A^2 - 147B^2 + 8000A^3)\right) \tag{2}$$

But $5A+7B = \sum_{n=1}^{\infty}(5\sigma_3(n) + 7\sigma_5(n))\mathrm{e}^{2\pi inz}$ and

$$5d^3 + 7d^5 = d^3(5+7d^2) \equiv d^3(2+d^2) \pmod 3 \equiv 0 \pmod 3$$

since 0 and 1 are the only quadratic residues modulo 3, and if $d^2 \equiv 0$, then $3|d$ so $d^3 \equiv 0 \pmod 3$, and if $d^2 \equiv 1 \pmod 3$ then $2 + d^2 \equiv 0 \pmod 3$. Similarly, $5d^3 + 7d^5 \equiv 0 \pmod 4$ since the only quadratic residues modulo 4 are 0 and 1.
Thus, $12|(5A+7B)$ so that 12^3 divides both coefficients in the brackets in (2) and thus all of the coefficients of the Fourier expansion in z (or the power series expansion in $q = \mathrm{e}^{2\pi iz}$) are integers. Thus

$$\Delta(z) = \frac{64\pi^{12}}{27}\left(12^3\sum_{n=1}^{\infty}\tau(n)\mathrm{e}^{2\pi inz}\right) = (2\pi)^{12}\sum_{n=1}^{\infty}\tau(n)\mathrm{e}^{2\pi inz}$$

where $\tau(n)$ was defined to be the coefficient of the resulting Fourier series. It follows that $\tau(n) \in \mathbb{Z}$ for all $n \in \mathbb{N}$. □

By Theorem 6, $\Delta(z)$ is a modular function that has a zero at infinity and is thus a cusp form.
In particular, note that $\mathrm{ord}_\infty\Delta = 1$, since $\tau(1) = 1$ and by transforming Δ into its q expansion, the lowest order term in q has exponent 1, and thus the q-expansion has order 1 at $q = 0$.
By Theorem 3,

$$1 + \frac{1}{3}\mathrm{ord}_{\mathrm{e}^{2\pi i/3}}\Delta + \frac{1}{2}\mathrm{ord}_i\Delta + \sum_{\substack{z_0 \in D' \\ z_0 \neq i, \mathrm{e}^{2\pi i/3}}} \mathrm{ord}_{z_0}\Delta = 1$$

Since Δ is analytic, all of these orders are non-negative integers, and therefore they must all be equal to 0 as we saw at the end of Lecture 7. Thus, Δ does not vanish at all on H.

Ramanujan's τ-function satisfies a number of congruence relations. For example,

$$\tau(n) \equiv n\sigma_3(n) \pmod 7,\ \tau(n) \equiv n^2\sigma_7(n) \pmod{27},\ \tau(n) \equiv \sigma_{11}(n) \pmod{691}$$

all proved by Ramanujan. The first few values of $\tau(n)$ are $\tau(1) = 1$, $\tau(2) = -24$, $\tau(3) = 252$, $\tau(4) = -1472$, $\tau(5) = 4830$, $\tau(6) = -6048$ and so forth. Lehmer conjectured that $\tau(n)$ is non-zero for all positive integers n. He checked this to be true for $n < 10^{11}$.
It is not so difficult to show that $\tau(n) = O(n^6)$ since Δ is modular of weight 12 (another way to see this is consider the growth rate of the functions $\sum_{n\leq x}\sum_{d|n} d^r$ for $r = 3$ and $r = 5$). In fact, it follows from work of Deligne that for each $\epsilon > 0$, $\tau(n) = O\left(n^{\frac{11}{2}+\epsilon}\right)$.
We also have the product expansion due to Jacobi, which is the content of Theorem 14:

$$\sum_{n=1}^{\infty}\tau(n)\mathrm{e}^{2\pi inz} = \mathrm{e}^{2\pi iz}\prod_{n=1}^{\infty}\left(1 - \mathrm{e}^{2\pi inz}\right)^{24}$$

Lecture 9: The $j(z)$ Function

Can we have a **modular form** of weight 0? Suppose f were a modular form of weight 0 which is not identically zero. Then by Theorem 3,

$$\mathrm{ord}_\infty f + \frac{1}{3}\mathrm{ord}_{\mathrm{e}^{2\pi i/3}} f + \frac{1}{2}\mathrm{ord}_i f + \sum_{\substack{z_0 \in D' \\ z_0 \neq i, \mathrm{e}^{2\pi i/3}}} \mathrm{ord}_{z_0} f = 0.$$

Thus, f has no zeros or poles in H. Suppose that f is non-zero for some $z_0 \in D'$ say $f(z_0) = c$. Then $g(z) = f(z) - c$ is a modular form of weight zero and has a zero at z_0. Thus, $g(z)$ must be identically zero, so $f(z)$ is constant.
Can we have a **modular function** of weight zero which is not identically zero? Yes.
Indeed, put $J(z) = \frac{g_2(z)^3}{\Delta(z)}$ and $j(z) = 12^3 J(z)$. Since $\Delta(z)$ is analytic and non-zero in H and $g_2(z)$ is a modular form then $J(z)$ is analytic in H and has a simple pole at ∞. Further, $\Delta(z)$ is modular of weight 12, as is $g_2(z)^3$ so $J(z)$ is a modular function of weight 0.
What is the Fourier expansion of $J(z)$?

Theorem 7.

$$j(z) = 12^3 J(z) = e^{-2\pi i z} + 744 + \sum_{n=1}^{\infty} c(n) e^{2\pi i n z}$$

where $c(n) \in \mathbb{Z}$ for all $n \in \mathbb{N}$.

Proof. Put $x = \mathrm{e}^{2\pi i z}$ and let P_1, P_2 and P_3 denote power series expansions in x with integer coefficients. We have from Theorem 5

$$g_2(z) = \frac{64\pi^{12}}{27}(1 + 720x + x^2 P_1)$$

From Theorem 6, $\Delta(z) = (2\pi)^{12}(x - 24x^2 + x^3 P_2)$. Thus,

$$j(z) = \frac{12^3 \cdot 64\pi^{12}}{27 \cdot 2^{12}\pi^{12}} \left(\frac{1}{x} \left(\frac{1 + 720x + x^2 P_1}{1 - 24x + x^2 P_2} \right) \right) = \frac{1}{x}(1 + 720x + x^2 P_1)(1 + L + L^2 + \ldots)$$

where $L(z) = 24x - x^2 P_2$. Here if the series diverges, one can analytically continue it at the point of divergence.
Thus, $j(z) = \frac{1}{x}(1 + 744x + x^2 P_3)$ where P_3 has integer coefficients as required. □

The first values of $c(n)$ are: $c(0) = 744$, $c(1) = 2^2 \cdot 3^3 \cdot 1823$, $c(2) = 2^{11} \cdot 5 \cdot 2099$. We have the following congruences for example:

$$\begin{aligned} n \equiv 0 \pmod{2^a} &\text{ implies that } c(n) \equiv 0 \pmod{2^{3a+2}} \\ n \equiv 0 \pmod{3^a} &\text{ implies that } c(n) \equiv 0 \pmod{3^{2a+3}} \\ n \equiv 0 \pmod{11^a} &\text{ implies that } c(n) \equiv 0 \pmod{11^a} \\ (n+1)c(n) \equiv 0 \pmod{24} & \end{aligned}$$

for $n, a \in \mathbb{N}$.
In 1932, Peterson proved that

$$c(n) \sim \frac{\mathrm{e}^{4\pi\sqrt{n}}}{\sqrt{2} n^{\frac{3}{4}}}.$$

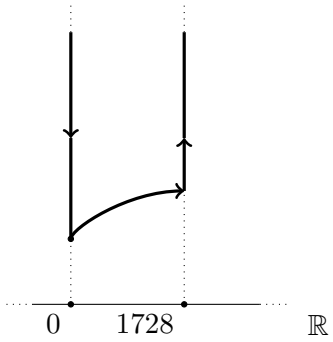

FIGURE 6. The contour of Γ that j maps to the real line.

Theorem 8. *$j(z)$ defines a bijection from D' to $\mathbb{C}$ (or equivalently H/G to $\mathbb{C}$).*

Proof. Let $\lambda \in \mathbb{C}$. Put $f_\lambda(z) = 12^3 g_2^3(z) - \lambda\Delta(z)$. Note that f_λ is a modular form of weight 12. Note that by Theorems 5 and 6, $\operatorname{ord}_\infty f_\lambda = 0$.
By theorem 3 with $k = 6$

$$\operatorname{ord}_\infty f_\lambda + \frac{1}{3}\operatorname{ord}_{e^{2\pi i/3}} f_\lambda + \frac{1}{2}\operatorname{ord}_i f_\lambda + \sum_{\substack{z_0 \in D' \\ z_0 \neq e^{2\pi i/3}, i}} \operatorname{ord}_{z_0} f_\lambda = 1.$$

Notice that if n_1, n_2 and n_3 are non-negative integers with $n_1 + \frac{1}{2}n_2 + \frac{1}{3}n_3 = 1$, then (n_1, n_2, n_3) is either $(1, 0, 0)$, $(0, 2, 0)$ or $(0, 0, 3)$. Thus, there is exactly one zero in D', say z_1 such that

$$j(z_1) = 12^3 \frac{g_2^3(z_1)}{\Delta(z_1)} = \frac{f_\lambda(z_1)}{\Delta(z_1)} + \lambda = \lambda$$

so j is surjective. Since $D' \subseteq \mathbb{C}$, it follows that j is injective as well and thus a bijection. □

Let us look more closely at the mapping $j : D' \to \mathbb{C}$. First, note that $j\left(e^{\frac{2\pi i}{3}}\right) = 0$ since $g_2 = 0$ there, and $j(i) = 12^3 = 1728$ since $g_3 = 0$ there and thus $\Delta(i) = g_2^3(i)$.
Next, observe that $j(z) = \overline{j(-\overline{z})}$. Indeed, if $z = u + iv$ for $u, v \in \mathbb{R}$ then

$$e^{2\pi i z} = e^{-2\pi v} \cdot e^{2\pi i u} = e^{-2\pi i \overline{z}} = e^{-(2\pi i(u - iv))} = e^{-2\pi v} \cdot e^{-2\pi i u} = \overline{e^{2\pi i z}}.$$

Thus, since $j(z)$ is representable by a Fourier expansion with real coefficients, it follows that every exponential term has this form so the claim follows.
Since $j(z + 1) = j(z)$ for $z \in H$, we have $j\left(-\frac{1}{2} + iv\right) = j\left(\frac{1}{2} + iv\right)$. Further, $\overline{-\left(\frac{1}{2} + iv\right)} = -\frac{1}{2} + iv$ so

$$j\left(-\frac{1}{2} + iv\right) = j\left(\overline{\frac{1}{2} + iv}\right) = j\left(\frac{1}{2} - iv\right) = \overline{j\left(-\frac{1}{2} + iv\right)}$$

since $\frac{1}{2} - iv = -\overline{\left(\frac{1}{2} - iv\right)}$. Thus, $j\left(-\frac{1}{2} + iv\right) \in \mathbb{R}$ for all $v > 0$. Further, $j(z) = j\left(-\frac{1}{z}\right)$ since it is modular of weight 0, so for $\beta \in \mathbb{T}$, $-\frac{1}{\beta} = -\overline{\beta}$ and thus $j(\beta) = j(-\overline{\beta})$ and so by our identity, $j(\beta) = \overline{j(-\overline{\beta})}$ so again $j(\beta) \in \mathbb{R}$. Further, if $z = iv$, $j(iv) = \overline{j(iv)}$ so $j(iv) \in \mathbb{R}$.
Thus, j maps the contour Γ, pictured in Figure 6 to the real line. Since j has a pole at infinity the contour is mapped to all of the real line.

Recall that for any lattice L,

$$g_2(L) = g_2([\omega_1, \omega_2]) = 60 \sum_{\omega \in L'} \frac{1}{\omega^4} = 60 \sum_{(m,n) \neq (0,0)} \frac{1}{(m\omega_1 + n\omega_2)^4}$$

Now for $z \in H$, $g_2(z) = 60 \sum_{(m,n)\neq(0,0)} \frac{1}{(mz+n)^4}$. Thus, $g_2([\omega_1, \omega_2]) = \frac{1}{\omega_2^4} g_2\left(\frac{\omega_1}{\omega_2}\right)$.

Theorem 9. *Let $a, b \in \mathbb{C}$ with $a^3 - 27b^2 \neq 0$. There exist complex numbers ω_1 and ω_2 with $\frac{\omega_1}{\omega_2} \notin \mathbb{R}$ for which $g_2([\omega_1, \omega_2]) = a$ and $g_3([\omega_1, \omega_2]) = b$.*

Proof. Since $J : D' \to \mathbb{C}$ is a bijection there exists a $\tau \in D'$ for which $J(\tau) = \frac{a^3}{a^3 - 27b^2}$.
Let us first assume $a, b \neq 0$. Since $a \neq 0$, $J(\tau) \neq 0$ so

$$\frac{J(\tau) - 1}{J(\tau)} = \frac{27b^2}{a^3} \tag{3}$$

Recall that $g_3([\omega_1, \omega_2]) = \frac{1}{\omega_2^6} g_3\left(\frac{\omega_1}{\omega_2}\right)$ and $g_2([\omega_1, \omega_2]) = \frac{1}{\omega_2^4} g_2\left(\frac{\omega_1}{\omega_2}\right)$. Since

$$\frac{J(\tau) - 1}{J(\tau)} = \frac{27 g_3(\tau)^2}{g_2(\tau)^3} \tag{4}$$

Now let $\omega_2 \in \mathbb{C}$ such that

$$\omega_2^2 = \frac{a}{b} \frac{g_3(\tau)}{g_2(\tau)} \tag{5}$$

and put $\omega_1 = \tau\omega_2$ so that

$$\frac{g_3([\omega_1, \omega_2])}{g_2([\omega_1, \omega_2])} = \frac{\frac{1}{\omega_2^6} g_3(\tau)}{\frac{1}{\omega_2^4} g_2(\tau)} = \frac{1}{\omega_2^2} \frac{g_3(\tau)}{g_2(\tau)} = \frac{b}{a} \tag{6}$$

From (5) we find that

$$\left(\frac{g_3(\tau)}{g_2(\tau)}\right)^2 = \omega_2^4 \left(\frac{b}{a}\right)^2$$

and similarly for a cube. Comparing (3) and (4) we find that

$$a = \frac{1}{\omega_2^4} g_2(\tau) = g_2([\omega_1, \omega_2])$$

By (6), $b = g_3([\omega_1, \omega_2])$. This proves the result when $ab \neq 0$.
Suppose $ab = 0$. Since $a^3 - 27b^2 \neq 0$, it follows that either $a = 0$ and $b \neq 0$ or $a \neq 0$ and $b = 0$. Let us first assume that $a = 0$. Choose ω_2 to be a complex number for which $g_3\left(\mathrm{e}^{2\pi i/3}\right) = b\omega_2^6$. Observe that $\omega_2 \neq 0$ since $g_3\left(\mathrm{e}^{2\pi i/3}\right) \neq 0$.
We then put $\omega_1 = \mathrm{e}^{2\pi i/3}\omega_2$. We have

$$g_3([\omega_1, \omega_2]) = \frac{1}{\omega_2^6} g_3\left(\frac{\omega_1}{\omega_2}\right) = b$$
$$g_2([\omega_1, \omega_2]) = \frac{1}{\omega_2^4} g_2\left(\mathrm{e}^{2\pi i/3}\right) = 0 = a$$

Finally, assume that $b = 0$. Choose $\omega_2 \in \mathbb{C}$ such that $g_2(i) = a\omega_2^4$ and $\omega_1 = i\omega_2$. Then

$$g_3([\omega_1, \omega_2]) = \frac{1}{\omega_2^6} g_3\left(\frac{\omega_1}{\omega_2}\right) = \frac{1}{\omega_2^6} g_3(i) = 0 = b$$
$$g_2([\omega_1, \omega_2]) = \frac{1}{\omega_2^4} g_2(i) = a$$

as required. □

Therefore, given any elliptic curve $y^2 = 4x^2 - ax - b$ with $a, b \in \mathbb{C}$ and $a^3 - 27b^2 \neq 0$ there is a lattice L and a p-function associated with this lattice L such that $(p(z), p'(z))$ gives a parametrization of the curve (see Lecture 2).

Lecture 10: Vector Spaces of Modular Forms of Fixed Weight

For any non-negative integer k let $\mathcal{M}_k$ denote the set of modular forms of weight $2k$. One can check that $\mathcal{M}_k$ is a vector space over $\mathbb{C}$.
Let $\mathcal{M}_k^o$ denote the subspace of $\mathcal{M}_k$ given by the cusp forms. Define the map $h : \mathcal{M}_k \to \mathbb{C}$ such that $h(f) = f(\infty)$. Then h is a linear functional and the kernel of h is $\mathcal{M}_k^o$. Thus, the dimension of $\mathcal{M}_k$ over $\mathcal{M}_k^o$ is at most 1 (by the First isomorphism theorem, the domain vector space quotiented by the kernel of the functional is isomorphic to the range, $\mathbb{C}$, which has vector space dimension one over itself). Further, for $k \geq 2$,

$$G_k(z) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m+nz)^{2k}}$$

is a modular form of weight $2k$. By the same proof as theorem 5, $G_k(0) = 2\zeta(2k) \neq 0$. Thus $\mathcal{M}_k \cong \mathcal{M}_k^o \oplus \mathbb{C}G_k$ for $k \geq 2$.

Theorem 10. (1) *$\mathcal{M}_k = \{0\}$ for $k < 0$ and $k = 1$.*

(2) *$\Delta(z)$ is an element of M_6^o and multiplication by Δ gives an isomorphism of $\mathcal{M}_{k-6}$ into $\mathcal{M}_k^o$ for $k \in \mathbb{Z}$.*

(3) *For $k = 0, 2, 3, 4, 5$, $\mathcal{M}_k$ is a dimension one vector space generated by $1, G_2, G_3, G_4, G_5$ respectively.*

Proof. (1) If f is a modular function of weight $2k$

$$\mathrm{ord}_\infty f + \frac{1}{2}\mathrm{ord}_i f + \frac{1}{3}\mathrm{ord}_{e^{2\pi i/3}} f + \sum_{\substack{z_0 \in D' \\ z_0 \neq i, e^{2\pi i/3}}} \mathrm{ord}_{z_0} f = \frac{k}{6}$$

If $f \in \mathcal{M}_1$ we would have a sum of the form $n_1 + \frac{n_2}{2} + \frac{n_3}{3} = \frac{1}{6}$ with $n_1, n_2, n_3 \in \mathbb{N}_0$ and this is impossible. The case $k < 0$ is incoherent for a non-zero modular form which is everywhere analytic.
(2) $\Delta \in \mathcal{M}_6^o$ since Δ is a cusp form of weight 12. Notice that the map ψ given by $\psi : \mathcal{M}_{k-6} \to \mathcal{M}_k^o$ with $\psi(f) = \Delta f$ is a linear map. It suffices to show that ψ is invertible. Given $g \in \mathcal{M}_k^o$ put $f = \frac{g}{\Delta}$. Notice that f is weakly modular of weight $2k - 12$. Since Δ is analytic and non-zero in H and it has a simple zero at ∞ and $g \in \mathcal{M}_k$, f is analytic and one-to-one and at infinity

$$\mathrm{ord}_\infty f = \mathrm{ord}_\infty g - \mathrm{ord}_\infty \Delta = \mathrm{ord}_\infty g - 1 \geq 0$$

since g is a cusp form. Thus, $f \in \mathcal{M}_{k-6}$. Thus, ψ is invertible so the result follows.
(3) By (1), $\mathcal{M}_k = \{0\}$ for $k < 0$ and $k = 1$. Then by (2), $\mathcal{M}_k^o = \{0\}$ for $k = 0, 1, 2, 3, 4, 5$ since it is the isomorphic image of $\mathcal{M}_k$ for $k - 6 < 0$. Thus, $\dim \mathcal{M}_k = 1$ for $k = 0, 1, 2, 3, 4, 5$, since by the first isomorphism theorem, the quotient space $\mathcal{M}_k/\mathcal{M}_k^o$ has dimension 1, and the kernel of ψ, $\mathcal{M}_k^o$ is trivial. Note that $1, G_1, G_2, G_3, G_4, G_5$ are non-zero elements of $\mathcal{M}_0, \mathcal{M}_2, \mathcal{M}_3, \mathcal{M}_4, \mathcal{M}_5$ respectively. Thus, (3) follows. □

Notice that for $k > 0$,

$$\dim \mathcal{M}_k = \begin{cases} \lfloor \frac{k}{6} \rfloor & \text{if } k \equiv 1 \pmod 6 \\ \lfloor \frac{k}{6} \rfloor + 1 & \text{otherwise} \end{cases}$$

since the result holds for $k = 0, 1, 2, 3, 4, 5$ and then using part b), the dimension increases by one. The congruence 1 modulo 6 is special since $\mathcal{M}_1 = \{0\}$ as in a).

Corollary 4. *A basis for $\mathcal{M}_k$ is given by $\{g_2^a g_3^b : a, b \in \mathbb{Z}, a, b \geq 0, 2a + 3b = k\}$.*

Proof. We will first show that $g_2^a g_3^b$ with $2a + 3b = k$, $a, b \geq 0$ generate $\mathcal{M}_k$. This is certainly true for $j \leq 3$ since G_2 is a scalar multiple of g_2 and G_3 of g_3.
We now argue by induction. Let (a_1, b_1) be a pair of non-negative integers with $2a_1 + 3b_1 = k$. Observe that $g_2^{a_1} g_3^{b_1}$ is a modular form of weight $2k$.
By theorem 5, $g_2^{a_1} g_3^{b_1}$ is not a cusp form so $g_2^{a_1} g_3^{b_1}$ is a non-zero element of $\mathcal{M}_k/\mathcal{M}_k^o$ and this is of dimension 1. Thus, if $f \in \mathcal{M}_k$, then there exists a $\lambda \in \mathbb{C}$ such that $f - \lambda g_2^{a_1} g_3^{b_1} \in \mathcal{M}_k^o$. By part b) of Theorem 10, $f - \lambda g_2^{a_1} g_3^{b_1} = \Delta h$ for $h \in \mathcal{M}_{k-6}$. By the inductive hypothesis, we can express h as an expansion of products $g_2^c g_3^d$, $2c + 3d = k - 6$ with $\Delta = g_2^3 - 27 g_3^2$, each term of which give resulting products of weight $2k$. To show this is a basis, suppose there exist scalars $\lambda_{a,b}$ not all zero in $\mathbb{C}$ such that

$$f(z) = \sum_{\substack{2a+3b=k \\ a,b \geq 0}} \lambda_{a,b} g_2^a g_3^b = 0.$$

Since $g_2(i)$ is non-zero, letting $z \to i$, we see that f has a zero of finite order at i which gives a contradiction. (This follows since by complex analysis we can write $f(z) = (z - i)^m g(z)$, $g(z) \neq 0$ in a neighbourhood of i for some m). □

Theorem 11. *f is a modular function of weight 0 if and only if f is a rational function of j.*

Proof. ($\Leftarrow$) Immediate.
($\Rightarrow$) Let f be a modular function of weight zero. Let $p_1, \ldots, p_k$ be the poles of f in D' repeated with multiplicity. Then

$$f_1 = f \prod_{i=1}^{k} (j(z) - j(p_i))$$

is analytic.
Next note that for some non-negative integer n, $f_2 = \Delta^n f_1$ is analytic at ∞. Therefore f_2 is a modular form of weight $12n$ and can be written as a $\mathbb{C}$-linear combination of $g_2^a g_3^b$ where $a, b \geq 0$ and $2a + 3b = 6n$. Thus, it suffices to show that $\frac{g_2^a g_3^b}{\Delta^n}$ is a rational function of j.

We have $\frac{a}{3}+\frac{b}{2}=n$. Thus, $a=3l$ and $b=2m$ for $l,m\in\mathbb{N}_0$.
Consider now

$$\frac{g_2^a g_3^b}{\Delta^n}=\left(\frac{g_2^3}{\Delta}\right)^l\left(\frac{g_3^2}{\Delta}\right)^m=\left(\frac{j}{1728}\right)^l\left(\frac{g_3^2}{\Delta}\right)^m=\left(\frac{j}{1728}\right)^l\left(\frac{g_2^3-\Delta}{1728\Delta}\right)^m$$
$$=\left(\frac{j}{1728}\right)^l\left(\frac{j}{27\cdot 1728}-\frac{1}{27}\right)^m$$

so the result follows. □

Let $d\in\mathbb{N}$ and $\theta\in\mathbb{Q}\left(\sqrt{-d}\right)$ with $\mathrm{Im}(\theta)>0$. Then $j(\theta)$ is an algebraic number. On the other hand, if θ is an algebraic number and θ is not in such a field, $j(\theta)$ is transcendental.

Lecture 11: Brief Review of Algebraic Number Theory

Let K be a finite extension of $\mathbb{Q}$ and let R be the ring of algebraic integers in K. Recall that $\alpha\in R$ if its minimal polynomial over $\mathbb{Z}$ is monic.
In general we do not have unique factorization into irreducibles in R up to reordering in units. For example, in $\mathbb{Q}(\sqrt{-5})$, $9=3\cdot 3=(2+\sqrt{-5})(2-\sqrt{-5})$, 3, $2\pm\sqrt{-5}$ being irreducibles in R for $\mathbb{Q}(\sqrt{-5})$.
However, we do have unique factorization of ideals of R (it takes some work to prove this).
In particular, given $\alpha\in R$ the principal ideal generated by α can be factored into prime ideals uniquely up to order.
Recall that a fractional ideal is a set of the form $\frac{1}{\beta}I$ with $\beta\in R$ and $I\subseteq R$ an ideal. We can define an equivalence relation $\sim$ on the fractional ideals of R by $I_1\sim I_2$ if and only if there exists nonzero $\alpha,\beta\in R$ such that $\alpha I_1=\beta I_2$.
We can define multiplication of equivalence classes by multiplication of representatives. This turns the set of equivalence classes into a finite Abelian group. The order of the group, denoted by h or $h(K)$ is known as the class number of K. If the class number is one, we recover unique factorization of elements of R up to multiplication by units, as every ideal is then principal, and by an elementary result of algebra, principal ideal domains are unique factorization domains.
It is not known but widely believed that there are infinitely many real quadratic extensions of $\mathbb{Q}$ with class number one. For imaginary quadratic extensions, the situation is different. It was known for many years that if $d\in\mathbb{N}$, $\mathbb{Q}(\sqrt{-d})$ has class number one then $\mathbb{Q}(\sqrt{-d})=\mathbb{Q}(\sqrt{-D})$ where $D=1,2,3,7,11,19,43,67$ or 163.
Gauss asked for a complete determination of all such imaginary extensions. Heilbronn proved in 1934 that there could be at most one more such field. In 1966-67 Baker and, independently, Stark proved the list above is complete. (In 1952, Heegner gave an essentially correct proof that was disregarded).

Recall, for $k\geq 2$

$$G_{2k}(L)=G_{2k}([\omega_1,\omega_2])=\sum_{(m,n)\neq(0,0)}\frac{1}{(m\omega_1+n\omega_2)^{2k}}$$

and that $g_2(L)=60G_4(L)$ and $g_3(L)=140G_6(L)$.

Theorem 12. *$G_{2k} = G_{2k}(L)$ is expressible as a polynomial in g_2 and g_3 with rational coefficients. Put $b_n = (2n+1)G_{2n+2}$ then $b_1 = \frac{g_2}{20}$ and $b_3 = \frac{g_3}{28}$ and*

$$(2n+3)(n-2)b_n = 3\sum_{k=1}^{n-2} b_k b_{n-1-k}$$

for $n \geq 3$.

Proof. Recall from the equation prcedding Theorem 1

$$p(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}z^{2n} = \frac{1}{z^2} + \sum_{n=1}^{\infty} b_n z^{2n}$$

and $p''(z) = 6p(z)^2 - \frac{g_3}{2}$. Comparing coefficients on both sides gives the result. □

Lecture 12: Complex Multiplication

Let $L = [\omega_1, \omega_2]$ be a lattice. If f is an L-periodic meromorphic function which is even then it can be shown that f is a rational function in terms of $p(z)$. Let $\beta \in \mathbb{C}$ and suppose that $p(\beta z)$ is L-periodic. In this case $p(\beta z) = \frac{g \circ p(z)}{h \circ p(z)}$ where g, h are polynomials over $\mathbb{C}$.

When does this happen? Certainly this holds if $n \in \mathbb{N}$. We can show that $p(nz) = \frac{g \circ p(z)}{h \circ p(z)}$ where g has degree n^2 and h has degree $n^2 - 1$.

If $\beta \in \mathbb{C}\backslash\mathbb{Z}$ and $p(\beta z)$ is L-periodic then we say that E_L, the elliptic curve associated with L, has complex multiplication or CM. If this happens we have

$$\beta\omega_1 = r\omega_1 + s\omega_2$$
$$\beta\omega_2 = t\omega_1 + u\omega_2$$

with $r, s, t, u \in \mathbb{Z}$. Thus

$$\begin{pmatrix} \beta - r & -s \\ -t & \beta - u \end{pmatrix}\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

so the determinant of the matrix is zero. Thus, β is a root of the quadratic polynomial $(x-r)(x-u) - st$. Thus, β is a root of a quadratic monic polynomial. Since $\beta \notin \mathbb{Z}$ we see that it is of degree 2 over $\mathbb{Q}$. Further, since $\beta = r + s\left(\frac{\omega_2}{\omega_1}\right)$, $s \neq 0$, and since $\frac{\omega_2}{\omega_1} \notin \mathbb{R}$ we see that β determines an imaginary quadratic extension. Notice that if E admits addition and multiplication by β_1 and β_2 then it does so by $\beta_1 \pm \beta_2$ and by $\beta_1\beta_2$ respectively.

In fact, the set of all elements β for which E admits complex multiplication is a subring of $\mathbb{Q}(\sqrt{-d})$ for some $d \in \mathbb{N}$.

E admits CM by the ring of algebraic integers of $\mathbb{Q}(\sqrt{-d})$ if and only if it admits complex multiplication by β where

$$\beta = \begin{cases} \sqrt{-d} & \text{if } d \equiv 1 \pmod 4 \\ \frac{1+\sqrt{-d}}{2} & \text{if } d \not\equiv 1 \pmod 4 \end{cases}$$

Suppose $L = [\omega_1, \omega_2]$ and $E = E_L$ is the elliptic curve associated with L, we define $j(E) = j(L) = j\left(\frac{\omega_2}{\omega_1}\right)$. Notice that if L_1 and L_2 are lattices with $L_1 = \lambda L_2$ then $j(L_1) = j(L_2)$.

Using this, one can show that

$$h(-d) = |\{j(E) : E \text{ is an elliptic curve with CM by the ring of algebraic integers of } \mathbb{Q}(\sqrt{-d})\}|$$

We shall now show that $j(E) = j(L) = j\left(\frac{\omega_2}{\omega_1}\right)$ is algebraic when E admits CM by β, where $\{1, \beta\}$ is an integral basis for $\mathbb{Q}(\sqrt{-d})$.
Notice that by scaling L we may suppose that $g = g_2 = g_3$. This does not change $j(E)$ as we showed above. By theorem 12,

$$p(z) = \frac{1}{z^2} + \frac{gz^2}{20} + \frac{gz^4}{28} + P_6(g)z^6 + P_8(g)z^8 + \dots$$

where $P_6(g)$ and $P_8(g)$ are polynomials in g with rational coefficients.
Further,

$$p(\beta z) = \frac{1}{\beta^2 z^2} + \frac{g\beta^2 z^2}{20} + \dots$$

We have

$$p(\beta z) = \frac{f_1(p(z))}{f_2(p(z))}$$

with f_1, f_2 coprime polynomials in $\mathbb{Q}[x]$. In fact, we may suppose that $f_i \in \mathbb{Q}(\beta)[x]$ for $i = 1, 2$ and that f_1, f_2 are coprime. Thus, by examining the power series expansion of the latter equation we see that the coefficient of z^a for a an odd integer is 0. But the coefficient of z^a is a polynomial $P_a(x, y) \in \mathbb{Q}[x, y]$ evaluated at $x = g$ and $y = \beta$. Note that the polynomials $P_a(x, y)$ are not all identically zero since if we vary β then there must exist a $\beta \in \mathbb{C}\backslash\mathbb{Q}(\sqrt{-d})$ such that the equality does not hold for if it did it would contradict the statement above that $\beta \in \mathbb{Q}(\sqrt{-d})$ for some $d \in \mathbb{N}$ is a necessary condition.
For fixed β there is a polynomial $P_a(x, y)$ which is not identically zero such that $P_a(x, \beta)$ is not identically zero. This follows since as we vary g we vary the underlying lattice and so otherwise we would have CM by β for each lattice associated with g which is not possible.
Let us put $f_a(x) = P_a(x, \beta)$. Then g is a root of $f_a \in \mathbb{Q}(\beta)[x]$ hence g is an algebraic number. Let F be a finite Galois extension of $\mathbb{Q}$ containing β and g. Let σ be an automorphism which fixes $\mathbb{Q}$. Note that $\sigma(\beta)$ is either β or $\overline{\beta}$ since β is imaginary quadratic. Applying σ to all the terms of $P_a(g, \beta)$ we get $P_a(\sigma g, \sigma\beta)$ we find that the curve $E^\sigma : y^2 = 4x^3 - \sigma(g)x - \sigma(g)$ admits CM by $\sigma(\beta)$ hence by β or $\overline{\beta}$ and thus by β. In fact if it admits CM by β it admits by the ring of algebraic integers of $\mathbb{Q}(\beta)$.
Notice that $j(E) = \frac{1728}{1-\frac{27}{g}}$ and thus $j(E^\sigma) = \frac{1728}{1-\frac{27}{\sigma(g)}}$. Therefore as we run through the automorphisms σ the number of different values assumed by $j(E^\sigma)$ corresponds to the number of different values of $\sigma(g)$. However since E^σ admits CM by the ring of algebraic integers of $\mathbb{Q}(\beta)$ if $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{-d})$ with $d \in \mathbb{N}$ then the number of different values assumed is at most $h(-d)$.
(Indeed, any two ideals in the ideal class are related by a prime ideal $\mathfrak{a} = \gamma\mathfrak{b}$ for $\mathfrak{a}, \mathfrak{b} \subseteq \mathbb{Q}(\sqrt{-d})$ and $\gamma \in \mathbb{Q}(\sqrt{-d})$ so if $j(E^{\sigma_1}) = j(E^{\sigma_2})$ then $\sigma_1(g) = \delta\sigma_2(g)$ so that $\sigma_2^{-1} \circ \sigma_1(g) = \sigma_2^{-1}(\delta)g$ and thus $\sigma_2^{-1} \circ \sigma_1$ is at most a scaling of g which does not change J so σ_1 and σ_2 are in the same ideal class and there are not necessarily representations for every ideal class.)
Therefore g and also $j(E)$ are algebraic numbers of degree at most $h(-d)$ since the Galois group has size bounded by $h(-d)$ from what we have just said. In particular if $h(-d) = 1$ then $j(E) = j(L) = j\left(\frac{\omega_2}{\omega_1}\right) \in \mathbb{Q}$.
Suppose that $\{1, \beta\}$ is an integral basis for the ring of algebraic integers of $\mathbb{Q}(\sqrt{-d})$ for some $d \in \mathbb{N}$. Consider the lattice $L = [1, \beta]$ then $j(L) = j(\beta)$ and $j(\beta)$ algebraic of degree at most $h(-d)$ over $\mathbb{Q}$.
Since $h(-163) = 1$ and $-163 \equiv 1 \pmod 4$ then we see that $j\left(\frac{1}{2}(1 + \sqrt{-163})\right) \in \mathbb{Q}$. In fact $j\left(\frac{1}{2}(1 + \sqrt{-163})\right)$

is an integers which is a perfect cube. Recall that if $q = \mathrm{e}^{2\pi iz}$

$$j(z) = \frac{1}{q} + 744 + 196884q + \dots$$

and when $z = \frac{1}{2}(1 + \sqrt{-163})$ then

$$q^{-1} = -\mathrm{e}^{\pi\sqrt{163}} = -262537412640768000 + 743.9999999999992\dots$$

In fact $j\left(\frac{1}{2}(1+\sqrt{-163})\right) = -262\cdots768000 = (-640320)^3$.
We will not prove this but the following facts hold: if $\tau \in \mathbb{Q}(\sqrt{-d})$ and $\mathrm{Im}(z) > 0$ then $j(\tau)$ is an algebraic number. Further, if $\{\omega_1, \omega_2\}$ is an integral basis for an ideal of the ring of algebraic integers of $\mathbb{Q}(\sqrt{-d})$ and $\tau = \frac{\omega_2}{\omega_1}$ then $j(\tau)$ has degree $h(-d)$ over both $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-d})$. Further, $\mathbb{Q}(\sqrt{-d})(j(\tau))$ is the maximal unramified Abelian extension of $\mathbb{Q}(\sqrt{-d})$. By an Abelian extension we mean a Galois extension of $\mathbb{Q}$ with Abelian Galois group. Given T a finite extension of K where $[K:\mathbb{Q}] < \infty$, T is said to be an unramified extension of K if every prime ideal decomposed into distinct prime ideals in the ring of algebraic integers of T.

One other interesting open problem is the following: can every finite group G be realized as a Galois group over the rationals? Shafarevitch showed that if G is solvable the answer is yes.
It is easy to realize S_n and A_n for $n \in \mathbb{N}$. The next class of non-solvable groups to be realized was $\mathrm{PGL}(2, \mathbb{Z}_n)$. Take $\mathrm{GL}(2, \mathbb{Z}_n)$ the set of 2×2 matrices over $\mathbb{Z}_n$ with determinent a unit in $\mathbb{Z}_n$. Then

$$\mathrm{PGL}(2, \mathbb{Z}_n) = \mathrm{GL}(2, \mathbb{Z}_n)/\{uI_2 : u \text{ a unit in } \mathbb{Z}_n\}$$

It can be shown that there exists, for each $n \in \mathbb{N}$ a polynomial $\Phi_n(x, y) \in \mathbb{Q}[x, y]$ such that $\Phi_n(j(z), j(nz)) = 0$. By Hilbert's irreducibility theorem there exists an $r \in \mathbb{Q}$ such that $\Phi_n(x, r)$ has a Galois group $\mathrm{PGL}(2, \mathbb{Z}_n)$ over $\mathbb{Q}$.

Lecture 13: Infinite Products and the Dedekind Eta Function

An infinite product $\prod_{i=1}^{\infty} a_i$ of complex numbers is defined to be A provided that

$$\lim_{n\to\infty} \prod_{i=1}^{n} a_i = \lim_{n\to\infty} A_n = A$$

and that $A \neq 0$. If there exists an integer N such that $a_n \neq 0$ for $n > N$ and such that $\lim_{n\to\infty} \prod_{k=N-1}^{n} a_k$ is equal to a non-zero complex number then we say that the infinite product converges.
Plainly, if $\prod_{n=1}^{\infty} a_n$ converges then $\lim_{n\to\infty} a_n = 1$. We can write $a_n = 1 + b_n$ and ask for the convergence of $\prod_{n=1}^{\infty}(1 + b_n)$ so that $b_n \to 0$. If no factor a_n is 0 then we compare the infinite product with the series $\sum_{n=1}^{\infty} \log(1 + b_n)$ where here we take the principal branch of the logarithm.
Let the partial sums of the log series above be denoted by S_n. Then $A_n = \mathrm{e}^{S_n}$ and if $S_n \to S$ then $A_n \to \mathrm{e}^S$. If no factor a_n is zero and the infinite product converges then $A_n \to \mathrm{e}^S \neq 0$ so it suffices to have the log series converge to conclude that the infinite product does.
In fact this condition is necessary. To see this, suppose $\log\left(\frac{A_n}{A}\right) \to 0$ and

$$\log\left(\frac{A_n}{A}\right) = \log A_n - \log A + 2\pi i h_n$$

for some integer h_n. Then

$$(h_{n+1}-h_n)2\pi i = \log\left(\frac{A_{n+1}}{A}\right) - \log\left(\frac{A_n}{A}\right) - \log(1+b_{n+1})$$

Therefore taking the imaginary part of each side of the equation gives

$$2\pi(h_{n+1}-h_n) = \operatorname{Im}\left(\log\left(\frac{A_{n+1}}{A}\right)\right) - \operatorname{Im}\left(\log\left(\frac{A_n}{A}\right)\right) - \operatorname{Im}(\log(1+b_{n+1}))$$

But $\operatorname{Im}\left(\log\left(\frac{A_{n+1}}{A}\right)\right), \operatorname{Im}\left(\log\left(\frac{A_n}{A}\right)\right) \to 0$ and $|\operatorname{Im}(\log(1+b_{n+1}))| \leq \pi$ for n large enough. Thus, $h_n = h$ for n large enough.
Therefore for n sufficiently large,

$$\log\left(\frac{A_n}{A}\right) = S_n - \log A + 2\pi i h$$

so $S_n \to \log A - 2\pi i h$. In conclusion, $\prod_{n=1}^{\infty}(1+b_n)$ converges if and only if $\sum_{n=1}^{\infty}\log(1+b_n)$ converges, where we take the principal branch of the logarithm. If $\operatorname{Re}(b_n) > -1$ for $n \in \mathbb{N}$ then we say that $\prod_{n=1}^{\infty}(1+b_n)$ converges absolutely if $\sum_{n=1}^{\infty}\log(1+b_n)$ converges absolutely.
Since $\frac{\log(1+z)}{z} \to 1$ as $z \to 0$ we obtain: if $\operatorname{Re}(b_n) > -1$ then $\prod_{n=1}^{\infty}(1+b_n)$ converges absolutely if and only if $\sum_{n=1}^{\infty}|b_n|$ converges.

Proposition 1. *Let U be an open subset of $\mathbb{C}$ and let f_n be analytic in U and not identically zero. If $\sum_{n=1}^{\infty}(f_n(z)-1)$ converges absolutely and uniformly on compact subsets of U then $\prod_{n=1}^{\infty}f_n(z)$ converges to an analytic function on U.*

We define the Dedekind Eta function in the upper half plane H by

$$\eta(z) = \mathrm{e}^{\frac{\pi i z}{12}}\prod_{n=1}^{\infty}\left(1-\mathrm{e}^{2\pi i n z}\right) = q^{\frac{1}{24}}\prod_{n=1}^{\infty}(1-q^n)$$

where $q = \mathrm{e}^{2\pi i z}$, where we choose the principal branch of the 24th root.
For $z \in H$, $|q| < 1$ and the infinite product converges absolutely (as a geometric series), we see from the proposition that $\eta(z)$ is analytic. We shall prove that $\eta(z)^{24} = (2\pi)^{-12}\Delta(z)$.
Notice that $\eta(z+1) = \mathrm{e}^{\frac{\pi i}{12}}\eta(z)$ and by induction $\eta(z+b) = \mathrm{e}^{\frac{\pi i b}{12}}\eta(z)$ for $b \in \mathbb{N}$ so $\eta(z+b)^{24} = \eta(z)^{24}$.

Theorem 13. *If $z \in H$ then $\eta\left(-\frac{1}{z}\right) = (-iz)^{\frac{1}{2}}\eta(z)$ where we take the principal branch of the square root function.*

Proof (Siegel): We prove the result for $z = iy$ with $y \in \mathbb{R}$, $y > 0$ and then the result holds for general $z \in H$ by analytic continuation. Thus, it suffices to prove that $\eta\left(\frac{i}{y}\right) = y^{\frac{1}{2}}\eta(iy)$. Equivalently,

$$\log\eta\left(\frac{i}{y}\right) - \log\eta(iy) = \frac{1}{2}\log y$$

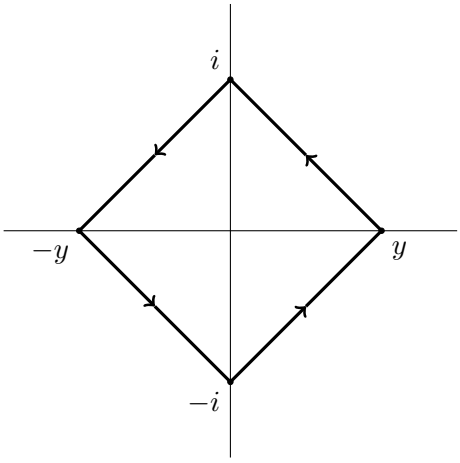

FIGURE 7. The Path of Integration Γ in Siegel's Proof

We have by the product definition

$$\begin{aligned}\log \eta(iy) &= -\frac{\pi y}{12} + \log \prod_{n=1}^{\infty} \left(1 - \mathrm{e}^{-2\pi n y}\right) = -\frac{\pi y}{12} + \sum_{n=1}^{\infty} \log\left(1 - \mathrm{e}^{-2\pi n y}\right) \\ &= -\frac{\pi y}{12} - \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \frac{\mathrm{e}^{-2\pi m n y}}{m} = -\frac{\pi y}{12} - \sum_{m=1}^{\infty} \frac{1}{m}\left(\frac{\mathrm{e}^{-2\pi m y}}{1 - \mathrm{e}^{-2\pi m y}}\right) \\ &= -\frac{\pi y}{12} + \sum_{m=1}^{\infty} \frac{1}{m(1 - \mathrm{e}^{2\pi m y})}\end{aligned}$$

Thus, it suffices to prove

$$\sum_{m=1}^{\infty} \frac{1}{m} \frac{1}{1 - \mathrm{e}^{2\pi m y}} - \sum_{m=1}^{\infty} \frac{1}{m} \frac{1}{1 - \mathrm{e}^{\frac{2\pi m}{y}}} - \frac{\pi}{12}\left(y - \frac{1}{y}\right) = -\frac{1}{2}\log y \tag{7}$$

To prove (7) we use a residue calculation. For fixed y and $n \in \mathbb{N}$ put

$$F_n(z) = -\frac{1}{8z}\cot(\pi i N z)\cot\left(\frac{\pi N z}{y}\right)$$

for $N = n + \frac{1}{2}$.

Let Γ be the contour in Figure 7. Inside Γ, $F_n(z)$ has simple poles at $z = \frac{ik}{N}$ and at $z = \frac{ky}{N}$ for $k = \pm 1, \pm 2, \ldots, \pm n$ and it has a triple pole at 0 by the expansion of cotangent derived above.
Recall that

$$z\cot z = 1 - \sum_{k=1}^{\infty} \frac{2^{2k} B_k}{(2k)!} z^{2k}$$

and from Euler's Theorem (Theorem 4) this converges for $|z| < \pi$. We have $B_1 = \frac{1}{6}$ and so $z\cot z = 1 - \frac{z^2}{3} + \ldots$.
The residue at $z = 0$ of $F_n(z)$ is the coefficient of z^2 in the power series expansion of $z^3 F_n(z)$ around 0.

Therefore

$$\begin{aligned} z^3 F_n(z) &= -\frac{1}{8}\left[\frac{1}{\pi i N}\left(\pi i N z \cot(\pi i N z)\right)\right]\cdot\left[\frac{y}{\pi N}\left(\frac{\pi N z}{y}\cot\left(\frac{\pi N z}{y}\right)\right)\right] \\ &= -\frac{y}{8\pi^2 i N^2}\left(1-\frac{(\pi i N)^2 z^2}{3}+\dots\right)\cdot\left(1-\left(\frac{\pi N}{y}\right)^2\frac{z^2}{3}+\dots\right) \end{aligned}$$

The coefficient of z^2 is thus

$$-\frac{y}{24\pi^2 i N^2}\left(\pi^2 N^2-\frac{\pi^2 N^2}{y^2}\right)=\frac{i}{24}\left(y-\frac{1}{y}\right)$$

Thus the residue of $F_n(z)$ at $z=0$ is $\frac{i}{24}\left(y-\frac{1}{y}\right)$.
What is the residue at $z=\frac{ik}{n}$? Notice that since $\tan \pi k = 0$,

$$\begin{aligned} &\lim_{z\to\frac{ik}{n}}\left(z-\frac{ik}{n}\right)\cot(\pi i N z)\left(-\frac{1}{8z}\cot\left(\frac{\pi N z}{y}\right)\right) \\ &= \lim_{z\to\frac{ik}{n}}\left(\frac{z-\frac{ik}{n}}{\tan(\pi i N z)-\tan \pi i N\frac{ik}{N}}\right)\left(-\frac{1}{8z}\cot\left(\frac{\pi N z}{y}\right)\right)=\left(\frac{d}{dz}(\tan \pi i N z)|_{z=\frac{ik}{N}}\right)^{-1}\left(-\frac{N}{8ik}\cot\left(\frac{\pi i k}{y}\right)\right) \\ &= \left[\frac{1}{\pi i N \sec^2 \pi i N z}|_{z=\frac{ik}{N}}\right]\left(-\frac{N}{8ik}\cot\left(\frac{\pi i k}{y}\right)\right)=\frac{1}{8\pi k}\cot\left(\frac{\pi i k}{y}\right) \end{aligned}$$

Notice that this is an even function of k. Therefore,

$$\sum_{\substack{k=-n\\k\neq 0}}^{n}\operatorname{Res}_{z=\frac{ik}{N}}F_n(z)=2\sum_{k=1}^{n}\frac{1}{8\pi k}\cot\frac{\pi i k}{y}$$

Finally, let us compute the residue of $F_n(z)$ at $z=\frac{ky}{N}$ for $k\neq 0$.

$$\begin{aligned} \lim_{z\to\frac{ky}{N}}\left(z-\frac{ky}{N}\right)\cot\left(\frac{\pi N z}{y}\right)\left(-\frac{1}{8z}\cot \pi i N z\right) &= \frac{N}{\pi y \sec^2\frac{\pi N z}{y}}|_{z=\frac{ky}{N}}\left(-\frac{N}{8ky}\cot \pi i k y\right) \\ &= -\frac{1}{8\pi k}\cot \pi i k y \end{aligned}$$

Thus,

$$\sum_{\substack{k=-n\\k\neq 0}}^{n}\operatorname{Res}_{z=\frac{ky}{N}}F_n(z)=2\sum_{k=1}^{n}\frac{1}{8\pi k}\cot \pi i k y$$

Now recall that

$$\begin{aligned} \cot i\theta = \frac{\cos i\theta}{\sin i\theta} &= i\frac{\mathrm{e}^{-\theta}+\mathrm{e}^{\theta}}{\mathrm{e}^{-\theta}-\mathrm{e}^{\theta}}=-i\frac{1+\mathrm{e}^{2\theta}}{\mathrm{e}^{2\theta}-1} \\ &= \frac{1}{i}\left(1+\frac{2}{\mathrm{e}^{2\theta}-1}\right)=\frac{1}{i}\left(1-\frac{2}{1-\mathrm{e}^{2\theta}}\right) \end{aligned}$$

Thus,

$$-2\sum_{k=1}^{n}\frac{1}{8\pi k}\cot \pi iky = -\frac{1}{4\pi i}\left[\sum_{k=1}^{n}\frac{1}{k} - 2\sum_{k=1}^{n}\frac{1}{k\left(1-\mathrm{e}^{2\pi ky}\right)}\right]$$
$$2\sum_{k=1}^{n}\frac{1}{8\pi k}\cot \frac{\pi ik}{y} = -\frac{1}{4\pi i}\left[\sum_{k=1}^{n}\frac{1}{k} - 2\sum_{k=1}^{n}\frac{1}{k\left(1-\mathrm{e}^{\frac{2\pi k}{y}}\right)}\right]$$

Therefore,

$$\int_{\Gamma} F_n(z)dz = -\frac{\pi}{12}\left(y-\frac{1}{y}\right) + \sum_{k=1}^{n}\frac{1}{k}\left[\frac{1}{1-\mathrm{e}^{2\pi ky}} - \frac{1}{1-\mathrm{e}^{\frac{2\pi k}{y}}}\right]$$

Consequently, it suffices to prove that

$$\lim_{n\to\infty}\int_{\Gamma} F_n(z)dz = -\frac{1}{2}\log y$$

Now

$$zF_n(z) = -\frac{1}{8}\cot(\pi iNz)\cot\frac{\pi Nz}{y} = -\frac{1}{8i}\left(1-\frac{2}{1-\mathrm{e}^{2\pi Nz}}\right)\frac{1}{i}\left(1-\frac{2}{1-\mathrm{e}^{-\frac{2\pi iNz}{y}}}\right)$$

and if $z = t+iu$, $t,u\in\mathbb{R}$ then

$$zF_n(z) = \frac{1}{8}\left(1-\frac{2}{1-\mathrm{e}^{2\pi N(t+iu)}}\right)\left(1-\frac{2}{1-\mathrm{e}^{\frac{2\pi N(-ti+u)}{y}}}\right)$$

Thus, since $N = n+\frac{1}{2}$,

$$\lim_{n\to\infty} zF_n(z) = \begin{cases}\frac{1}{8} & \text{if } z=t+iu, t,u>0 \text{ or } t,u<0\\ -\frac{1}{8} & \text{if } z=t+iu,\ t>0,\ u<0 \text{ or } t<0,\ u>0\end{cases}$$

Therefore, $\lim_{n\to\infty} zF_n(z)$ tends to $\frac{1}{8}$ on the line segments (excluding endpoints) joining y to i and $-y$ to $-i$ and it tends to $-\frac{1}{8}$ on the line segments (excluding endpoints) joining i to $-y$ and $-i$ to y.
Now since $y>0$ and $N = n+\frac{1}{2}$, $zF_n(z)$ is uniformly bounded on the contour Γ and so

$$\begin{aligned}\lim_{n\to\infty}\int_{\Gamma} F_n(z)dz &= \int_{\Gamma}\lim_{n\to\infty} zF_n(z)\frac{dz}{z} = \frac{1}{8}\left[\int_y^i\frac{dz}{z} - \int_i^{-y}\frac{dz}{z} + \int_{-y}^{-i}\frac{dz}{z} - \int_{-i}^{y}\frac{dz}{z}\right]\\ &= \frac{1}{8}(\log i - \log y - \log(-y) + \log i + \log(-i) - \log(-y) - \log y + \log(-i))\end{aligned}$$

Here, we are using the branch of the logarithm with $0\le\theta<2\pi$. We must pass through the cut line by passing along the contour Γ and therefore we must account for the winding number by including a term $2\pi i$. Thus,

$$\lim_{n\to\infty}\int_{\Gamma} F_n(z)dz = \frac{1}{8}\left(2i\frac{\pi}{2} - 2\log y - 2\log y - 2\pi i + 2\frac{3\pi i}{2} - 2\pi i\right) = -\frac{1}{2}\log y$$

as required. □

Theorem 14 (Jacobi). *Let $q = e^{2\pi iz}$ for $z \in H$. Then for all $z \in H$,*

$$\Delta(z) = (2\pi)^{12}\eta^{24}(z) = (2\pi)^{12} q \prod_{n=1}^{\infty}(1-q^n)^{24}$$

Proof. Put $f(z) = \frac{\Delta(z)}{\eta^{24}(z)}$. Observe that f is invariant under the action of the modular group (since $f(Sz) = \frac{z^{12}\Delta(z)}{\eta^{24}(Sz)} = \frac{z^{12}\Delta(z)}{(-iz)^{12}\eta^{24}(z)} = f(z)$ and $f(Tz) = f(z)$). Further, $\eta(z)$ is analytic and non-zero on H (since all the poles have norm < 1 or have imaginary part equal to 0).
We have

$$\eta^{24}(z) = \mathrm{e}^{2\pi iz}\prod_{n=1}^{\infty}\left(1-\mathrm{e}^{2\pi inz}\right)^{24} = q(1+P_1(q))$$

where P_1, P_2, P_3 denote power series in q with integer coefficients and zero constant term.
Further, since Δ is a cusp form,

$$\Delta(z) = (2\pi)^{12} q P_2(q)$$

Thus, $f(z) = (2\pi)^{12}(1+P_3(q))$ and so f is analytic at infinity. Therefore, f is a modular form of weight 0 and hence is a constant and that constant is $(2\pi)^{12}$. The result now follows. □

Lecture 14: The Partition Counting Function and Hecke Operators

For any positive integer n, let $p(n)$ denote the number of partitions of n into positive integers. Thus, $p(5) = 7$, since $5 = 4+1 = 3+1+1 = 2+1+1+1 = 3+2 = 2+2+1 = 1+1+1+1+1$.
Observe that for $z \in H$,

$$\prod_{n=1}^{\infty}(1-q^n)^{-1} = \prod_{n=1}^{\infty}\left(\sum_{j=0}^{\infty} q^{nj}\right) = \sum_{m=0}^{\infty} p(m)q^m$$

by grouping those terms in the sum with $nj = m$.

Theorem 15. *For all positive integers n, $p(n) < e^{\pi\sqrt{\frac{2n}{3}}}$.*

Proof. For $0 < x < 1$, define $f(x) = \prod_{n=1}^{\infty}(1-x^n)^{-1}$ Thus,

$$\begin{aligned}\log f(x) &= -\sum_{n=1}^{\infty}\log(1-x^n) = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\frac{x^{mn}}{m} \\ &= \sum_{m=1}^{\infty}\frac{1}{m}\sum_{n=1}^{\infty}x^{mn} = \sum_{m=1}^{\infty}\frac{x^m}{m(1-x^m)}\end{aligned}$$

where the change of order of summation is justified by the absolute convergence of the power series expansion of $\log(1-x^n)$ for every $n \in \mathbb{N}$ for $x \in (0,1)$.
Note that $x^k \geq x^{m-1}$ for $0 \leq k \leq m-1$ so that

$$mx^{m-1} \leq 1 + x + \ldots + x^{m-1} \leq \frac{1-x^m}{1-x}$$

from which it follows that

$$\frac{x^m}{1-x^m} \leq \frac{x}{m(1-x)}$$

Therefore

$$\log f(x) = \sum_{m=1}^{\infty} \frac{x^m}{m(1-x^m)} \leq \sum_{m=1}^{\infty} \frac{x}{m^2(1-x)} = \frac{x}{1-x}\frac{\pi^2}{6}$$

since $\zeta(2) = \frac{\pi^2}{6}$. Certainly for $0 < x < 1$ we have $p(n) \leq \frac{f(x)}{x^n}$ since

$$p(n)x^n \leq \sum_{m=1}^{\infty} p(m)x^m = \prod_{m=1}^{\infty} (1-x^m)^{-1} = f(x)$$

where $p(n) \in \mathbb{N} \cup \{0\}$ for all n. Thus, we can write

$$\log p(n) \leq \frac{\pi^2}{6}\left(\frac{x}{1-x}\right) - n\log x$$

Now for $\frac{1}{2} < x < 1$ we have

$$-\log x = \log\left(\frac{1}{x}\right) = \log\left(1 + \left(\frac{1}{x} - 1\right)\right) < \frac{1}{x} - 1 = \frac{1-x}{x}$$

since $0 \leq \frac{1}{x} - 1 < 1$. Therefore,

$$\log p(n) \leq \frac{\pi^2}{6}\left(\frac{x}{1-x}\right) + n\left(\frac{1-x}{x}\right)$$

On taking, for $n > 1$, $\frac{1}{2} < x = \frac{\sqrt{6n}}{\sqrt{6n}+\pi} < 1$, we find that $\log p(n) < \pi\sqrt{\frac{2n}{3}}$, and the result follows. □

In fact as $n \to \infty$,

$$p(n) \sim \frac{e^{\pi\sqrt{\frac{2n}{3}}}}{4\sqrt{3}n}$$

proved by Hardy and Ramanujan in 1918 and Uspensky proved this independently in 1920.
We will show later that the τ-function is multiplicative, i.e. $\tau(mn) = \tau(m)\tau(n)$ whenever $\gcd(m,n) = 1$. Further, if p is prime and $n \in \mathbb{N}$, $\tau(p)\tau(p^n) = \tau(p^{n+1}) + p^{11}\tau(p^{n-1})$.

General Question: When are the coefficients in the q-expansion of a modular form multiplicative in the sense above? Hecke answered this question by introducing Hecke Operators $T_1, T_2, \ldots$. These map $\mathcal{M}_k$ to $\mathcal{M}_k$ and even $\mathcal{M}_k^o$ to $\mathcal{M}_k^o$.

Definition 9. *Let k be an integer and n a positive integer. The operator $T_n : \mathcal{M}_k \to \mathcal{M}_k$ is defined by*

$$T_n f(z) = n^{2k-1} \sum_{d|n} d^{-2k} \sum_{b=0}^{d-1} f\left(\frac{nz+bd}{d^2}\right)$$

T_n is known as a Hecke operator.

Remarks. (1) *When n is a prime p,*

$$T_p f(z) = p^{2k-1} f(pz) + \frac{1}{p}\sum_{b=0}^{p-1} f\left(\frac{z+b}{p}\right)$$

(2) *We have work to do to show that T_n maps $\mathcal{M}_k$ to $\mathcal{M}_k$ and $\mathcal{M}_k^o$ to $\mathcal{M}_k^o$.*

Theorem 16. *Let $f \in \mathcal{M}_k$ and put $q = e^{2\pi iz}$. Suppose, for $z \in H$, $f(z) = \sum_{m=1}^{\infty} c(m)q^m$. Then for all $n \in \mathbb{N}$, $T_n f(z) = \sum_{m=0}^{\infty} r_n(m)q^m$ where*

$$r_n(m) = \sum_{d|\gcd(m,n)} d^{2k-1} c\left(\frac{mn}{d^2}\right)$$

Proof.

$$T_n f(z) = n^{2k-1} \sum_{d|n} d^{-2k} \sum_{b=0}^{d-1} \sum_{m=0}^{\infty} c(m) \mathrm{e}^{2\pi i m\left(\frac{nz+bd}{d^2}\right)}$$

$$= \sum_{m=0}^{\infty} \sum_{d|n} \left(\frac{n}{d}\right)^{2k-1} c(m) \mathrm{e}^{2\pi i \frac{nz}{d^2}} \frac{1}{d} \sum_{b=0}^{d-1} \mathrm{e}^{\frac{2\pi i m}{d} b}$$

since this converges absolutely on H.
But notice that

$$\frac{1}{d} \sum_{b=0}^{d-1} \mathrm{e}^{\frac{2\pi i m}{d} b} = \begin{cases} 0 & \text{if } d \nmid m \\ 1 & \text{if } d|m \end{cases}$$

Thus

$$T_n f(z) = \sum_{m=0}^{\infty} \sum_{\substack{d|m \\ d|n}} \left(\frac{n}{d}\right)^{2k-1} c(m) \mathrm{e}^{2\pi i\left(\frac{mnz}{d^2}\right)}$$

We now write $m = td$ so that

$$T_n f(z) = \sum_{t=0}^{\infty} \sum_{d|n} \left(\frac{n}{d}\right)^{2k-1} c(td) \mathrm{e}^{2\pi i\left(\frac{tnz}{d}\right)}$$

Now replace d in the inner sum by $\frac{n}{d}$ (by the symmetry of the sum over divisors of n) to get

$$T_n f(z) = \sum_{t=0}^{\infty} \sum_{d|n} d^{2k-1} c\left(\frac{tn}{d}\right) q^{td}$$

Now collect terms such that $td = m$ so that $d|m$. Thus

$$T_n f(z) = \sum_{m=0}^{\infty} \left(\sum_{\substack{d|n \\ d|m}} d^{2k-1} c\left(\frac{mn}{d^2}\right) \right) q^m = \sum_{m=0}^{\infty} r_n(m) q^m$$

and we are done. □

Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ for $a, b, c, d \in \mathbb{Z}$. We define the action $A \cdot z = \frac{az+b}{cz+d}$. We can define $T_n f$ in terms of matrices of the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ for $a, b, d \in \mathbb{N}_0$ and $ad = m$.
We have

$$T_n f(z) = n^{2k-1} \sum_{\substack{a \geq 1, ad = n \\ 0 \leq b \leq d-1}} d^{-2k} f\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} z\right)$$

and so

$$T_n f(z) = \frac{1}{n} \sum_{\substack{a \geq 1, ad=n \\ 0 \leq b \leq d-1}} a^{2k} f\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} z \right)$$

We wish to see how $T_n f$ behaves under the action of the modular group. In particular, we must show that $T_n f$ is in $\mathcal{M}_k$ for $f \in \mathcal{M}_k$. To see this, we introduce $\Gamma(n)$ where

$$\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - bc = n \right\} / \sim$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & -b \\ -c & -d \end{pmatrix}$ here, as in the modular group.
Note that $\Gamma(1)$ is the modular group. We put an equivalence relation $\sim$ on $\Gamma(n)$ by putting $A_1 \sim A_2$ whenever there exists $U \in \Gamma(1)$ such that $A_1 = UA_2$.

Proposition 2. *There is a representative of each equivalence class in* $\Gamma(n)$ *under* $\sim$ *of the form* $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$.

Proof. Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(n)$. If $c = 0$ we are done. If $c \neq 0$, let $\frac{s}{r} = -\frac{a}{c}$ with $\gcd(r, s) = 1$. Then there exist integers p and q such that $ps - qr = 1$. Put $U = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$ so that $U \in \Gamma(1)$. Then

$$UA = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} \star & \star \\ ra - cs & \star \end{pmatrix} = \begin{pmatrix} \star & \star \\ 0 & \star \end{pmatrix}$$

Further, $\det(UA) = \det(U)\det(A) = \det(A) = n$ so $UA \in \Gamma(n)$, and we are done. □

Proposition 3.

$$\Gamma(n) = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : d | n, a = \frac{n}{d}, b = 0, 1, \ldots, d-1 \right\}$$

The above list gives a complete set of representatives.

Proof. By proposition 2, we can find a representative of each equivalence class of the form $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Plainly, $ad = n$ and we may suppose a and d are positive. Thus, $d | n$ and $a = \frac{n}{d}$.
It remains to show that we can restrict b to the range $0, 1, \ldots, d-1$. Let $b = qd + r$ where $0 \leq r < d$. Then $U = \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \in \Gamma(1)$. Further,

$$U \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & b - qd \\ 0 & d \end{pmatrix} = \begin{pmatrix} a & r \\ 0 & d \end{pmatrix}$$

Thus, the first assertion follows since $ad = n$ and $0 \leq r \leq d-1$. It remains to show that the list is complete. Suppose that $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ and $\begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$ are representatives for the same equivalence class with $ad = n$ and $a_1 d_1 = n$, $a_1 > 0$ and $0 \leq b < d$ and $0 \leq b_1 < d_1$. Thus, if $U \in \Gamma(1)$ and $U \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$ we have

$$U = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} \frac{1}{a} & -\frac{b}{ad} \\ 0 & \frac{1}{d} \end{pmatrix} = \begin{pmatrix} \frac{a_1}{a} & \frac{b_1}{d} - \frac{a_1 b}{ad} \\ 0 & \frac{d_1}{d} \end{pmatrix}$$

Since $U \in \Gamma(1)$, $\frac{a_1 d_1}{ad} = 1$ and $\frac{a_1}{a}, \frac{d_1}{d} \in \mathbb{Z}$ so $\frac{a_1}{a} = \frac{d_1}{d} = 1$ and thus $a_1 = a$ and $d_1 = d$. But then $\frac{b_1 - b}{d} \in \mathbb{Z}$ is the resulting top right entry, and $b_1, b < d$ so that $b_1 = b$. □

Proposition 4. *Let $A_1 \in \Gamma(n)$ and $U_1 \in \Gamma(1)$. There exists $A_2 \in \Gamma(n)$ and $U_2 \in \Gamma(1)$ such that $A_1 U_1 = U_2 A_2$. Further, if $A_i = \begin{pmatrix} a_i & b_i \\ 0 & d_i \end{pmatrix}$ and $U_i = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ for $i = 1, 2$ then $a_1(\gamma_2 A_2 z + \delta_2) = a_2(\gamma_1 z + \delta_1)$.*

Proof. Since $\det(A_1 U_1) = \det(A_1) = n$, from proposition 2 we see that $A_1 U_1$ is equivalent under $\sim$ to A_2 where $A_2 = \begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$. Then there exists $U_2 \in \Gamma(1)$ such that $A_1 U_1 = U_2 A_2$.
Next, observe that

$$A_1 U_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix} \begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix} = \begin{pmatrix} \star & \star \\ d_1\gamma_1 & d_1\delta_1 \end{pmatrix}$$

Thus,

$$\begin{pmatrix} \alpha_2 & \beta_2 \\ \gamma_2 & \delta_2 \end{pmatrix} = A_1 U_1 A_2^{-1} = \frac{1}{n} \begin{pmatrix} \star & \star \\ d_1\gamma_1 & d_1\delta_1 \end{pmatrix} \begin{pmatrix} d_2 & -b_2 \\ 0 & a_2 \end{pmatrix} = \frac{1}{n} \begin{pmatrix} \star & \star \\ d_1 d_2 \gamma_1 & d_1 a_2 \delta_1 - d_1 b_2 \gamma_1 \end{pmatrix}$$

Therefore,

$$\gamma_2 = \frac{d_1 d_2 \gamma_1}{n} = \frac{d_2 \gamma_1}{a_1}, \qquad \delta_2 = \frac{d_1 a_2 \delta_1 - d_1 b_2 \gamma_1}{n} = \frac{a_2 \delta_1 - b_2 \gamma_1}{a_1}$$

Thus, $a_1 \gamma_2 = d_2 \gamma_1$ and $a_1 \delta_2 = a_2 \delta_1 - \gamma_1 b_2$.
Hence,

$$\begin{aligned} a_1(\gamma_2 A_2 z + \delta_2) &= a_1 \gamma_2 A_2 z + a_1 \delta_2 = d_2 \gamma_1 \left(\frac{a_2 z + b_2}{d_2} \right) + a_2 \delta_1 - \gamma_1 b_2 \\ &= a_2 \gamma_1 z + b_2 \gamma_1 + a_2 \delta_1 - b_2 \gamma_1 = a_2(\gamma_1 z + \delta_1) \end{aligned}$$

and we are done. □

Theorem 17. *Let $k \in \mathbb{Z}$, $m \in \mathbb{N}$, $f \in \mathcal{M}_k$ and $U_1 = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma(1)$. Then $T_n f(U_1 z) = (\gamma z + \delta)^{2k} T_n f(z)$.*

Proof. Recall that

$$T_n f(z) = \frac{1}{n} \sum_{A_1} a_1^{2k} f(A_1 z)$$

where the sum runs over a complete set of inequivalent matrices of the form $A_1 = \begin{pmatrix} a_1 & b_1 \\ 0 & d_1 \end{pmatrix}$ in $\Gamma(n)$ under $\sim$.
Now by proposition 4, for each A_1 we can find an $A_2 \in \Gamma(n)$, $U_2 \in \Gamma(1)$ such that $A_1 U_1 = U_2 A_2$. Thus, by proposition 2, we may suppose that A_2 is of the form $\begin{pmatrix} a_2 & b_2 \\ 0 & d_2 \end{pmatrix}$ and let $U_2 = \begin{pmatrix} \alpha_2 & \beta_2 \\ \gamma_2 & \delta_2 \end{pmatrix}$. Again by proposition 3, $a_1(\gamma_2 A_2 z + \delta_2) = a_2(\gamma z + \delta)$. Thus, since f is modular of weight $2k$,

$$a_1^{2k} f(A_1 U_1 z) = a_1^{2k} f(U_2 A_2 z) = (a_1(\gamma_2 A_2 z + \delta_2))^{2k} f(A_2 z) = (a_2(\gamma z + \delta))^{2k} f(A_2 z)$$

Hence, since A_1 runs over all equivalence classes, so does A_2 thus

$$T_n f(Uz) = \frac{1}{n} \sum_{A_1} a_1^{2k} f(A_1 U z) = \frac{1}{n} \sum_{A_2} (\gamma z + \delta)^{2k} a_2^{2k} f(A_2 z) = (\gamma z + \delta)^{2k} T_n f(z)$$

The result is shown. □

Theorem 18. *Let $k \in \mathbb{Z}$, $n \in \mathbb{N}$. If $f \in \mathcal{M}_k$ then $T_n f \in \mathcal{M}_k$ and if $f \in \mathcal{M}_k^o$ then $T_n f \in \mathcal{M}_k^o$.*

Proof. If $f \in \mathcal{M}_k$ then from the definition of $T_n f$ we see that $T_n f$ is analytic in H. By theorem 16, $T_n f$ is analytic at ∞. Further, by theorem 17, $T_n f$ is modular of weight $2k$.
If $f \in \mathcal{M}_k^o$ then $c(0) = 0$ and by theorem 16,

$$r_n(0) = \sum_{d|n} d^{2k-1} c(0) = 0$$

and so $T_n f \in \mathcal{M}_k^o$. □

Theorem 19. *If $m, n \in \mathbb{Z}$ are coprime then $T_m \circ T_n = T_{mn}$.*

Proof. Let $f \in \mathcal{M}_k$. Then

$$T_n f(z) = \frac{1}{n} \sum_{\substack{a \le 1, ad = n \\ 0 \le b \le d-1}} a^{2k} f(Az)$$

for $A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$. Further, for $B = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$ for α, β, δ in the range of the sum below,

$$T_m(T_n f)(z) = \frac{1}{m} \sum_{\substack{\alpha \le 1, \alpha\delta = m \\ 0 \le \beta \le \delta - 1}} \alpha^{2k} T_n f(Bz) = \frac{1}{mn} \sum_{\substack{\alpha \le 1, \alpha\delta = m \\ 0 \le \beta \le \delta - 1}} \sum_{\substack{a \le 1, ad = n \\ 0 \le b \le d-1}} (\alpha a)^{2k} f(ABz)$$

$$= \frac{1}{mn} \sum_{\substack{\alpha \le 1, \alpha\delta = m \\ 0 \le \beta \le \delta - 1}} \sum_{\substack{a \le 1, ad = n \\ 0 \le b \le d-1}} (\alpha a)^{2k} f(Cz)$$

where $C = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} a\alpha & a\beta + b\delta \\ 0 & d\delta \end{pmatrix}$.
Now as d and δ run through divisors of n and m respectively, $d\delta$ runs through the divisors of mn by coprimality. It follows that d and δ are also coprime so $a\beta + b\delta$ runs through distinct integers modulo $d\delta$ as we range over pairs (b, β) with $0 \le b \le d-1$ and $0 \le \beta \le \delta - 1$.
Thus,

$$T_m(T_n f)(z) = \frac{1}{mn} \sum_{\substack{A \le 1, AD = mn \\ 0 \le B \le D-1}} A^{2k} f\left(\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} z \right) = T_{mn}(z)$$

for arbitrary $z \in H$, and the result follows. □

Theorem 20. *Let $m, n \in \mathbb{N}$. Then T_m and T_n commute on $\mathcal{M}_k$ and*

$$T_m \circ T_n = \sum_{d | \gcd(m,n)} d^{2k-1} T_{\frac{mn}{d^2}} \tag{8}$$

Proof. If $\gcd(m, n) = 1$ then it follows from theorem 19 if we know it for prime pairs.
Suppose that $p|m$ and $p|n$ and $p^{m_1} || m$ and $p^{n_1} || n$ (that is, m_1 and n_1 are the maximal exponents of p dividing m and n, respectively). Then by theorem 19,

$$T_m \circ T_n = T_{\frac{m}{p^{m_1}}} \circ T_{p^{m_1}} \circ T_{\frac{n}{p^{n_1}}} \circ T_{p^{n_1}} = T_{\frac{m}{p^{m_1}}} \circ T_{\frac{n}{p^{n_1}}} \circ T_{p^{m_1}} \circ T_{p^{n_1}}$$

since $\frac{n}{p^{n_1}}$ and p^{m_1} are coprime and commute by theorem 19.
We will first show this for $m = p$ and $n = p^r$ which we will get by showing

$$T_p T_{p^r} = T_{p^{r+1}} + p^{2k-1} T_{p^{r-1}}$$

Note that for $f \in \mathcal{M}_k$ we have by definition

$$T_{p^r} = p^{-r} \sum_{\substack{0 \le t \le r \\ 0 \le b \le p^t - 1}} p^{2(r-t)k} f\left(\frac{p^{r-t}z + b}{p^t}\right)$$

and if $g \in \mathcal{M}_k$ then

$$T_p g(z) = p^{2k-1} g(pz) + p^{-1} \sum_{b=0}^{p-1} g\left(\frac{z+b}{p}\right)$$

Therefore,

$$T_p(T_{p^r} f)(z) = p^{2k-1-r} \sum_{\substack{0 \le t \le r \\ 0 \le b \le p^t - 1}} p^{2(r-t)k} f\left(\frac{p^{r-t+1}z + b}{p^t}\right) + p^{-1} \sum_{b=0}^{p-1} p^{-r} \sum_{\substack{0 \le t \le r \\ 0 \le b \le p^t - 1}} p^{2(r-t)k} f\left(\frac{1}{p^t}\left(p^{r-t}\left(\frac{z+b}{p}\right) + b\right)\right) \tag{9}$$

Taking the $t = r$ term of the rightmost term in (9) and adding it to the leftmost term gives the first term of (9) as

$$p^{-1-r} \sum_{\substack{0 \le t \le r+1 \\ 0 \le c \le p^t - 1}} p^{2(r+t-1)k} f\left(\frac{p^{r+1-t}z + c}{p^t}\right) = T_{p^{r+1}} f(z)$$

The remaining terms of the second term of (9) are

$$p^{-1-r} \sum_{\substack{0 \le t \le r-1 \\ 0 \le b \le p^t - 1}} p^{2(r-t)k} \sum_{b'=0}^{p-1} f\left(\frac{p^{r-t-1}z + b + p^{r-t-1}b'}{p^t}\right)$$

If $t \le \frac{r-1}{2}$ then $\frac{p^{r-t-1}b'}{p^t} \in \mathbb{Z}$ so by the periodicity of f there is no dependence on b' and the contributions for such a fixed t is

$$p^{-r+2(r-t)k} \sum_{0 \le b \le p^t - 1} f\left(\frac{p^{r-t-1}z + b}{p^t}\right) \tag{10}$$

since the sum over b above gives p copies of the same contribution. Further, for any t, $b + p^{r-t-1}b'$ modulo p^t runs over the set of residues modulo p^t exactly p times so the contribution for any t is given by (10), summing over t powers and yields the claimed formula we made above. We will use this formula, that is,

$$T_p T_{p^r} = T_{p^{r+1}} + p^{2k-1} T_{p^{r-1}}$$

as our base case.
Now suppose that

$$T_{p^s} T_{p^r} = \sum_{d \mid \gcd(p^s, p^r)} d^{2k-1} T_{\frac{p^{s+r}}{d^2}} \tag{11}$$

is true up to some fixed s. Then, using our base case, we have that

$$T_p(T_{p^s} T_{p^r}) = \sum_{0 \le t \le \mu} p^{t(2k-1)} T_p T_{p^{s+r-2t}}$$

where $\mu = \min(s, r)$. Note that the associativity of Hecke operators follows by the linearity of these operators, and linear maps act associatively in multiplication.
Using the base case again, we have

$$T_{p^{s+1}}T_{p^r} = \sum_{0\le t\le \mu} p^{t(2k-1)}T_pT_{p^{s+r-2t}} - p^{2k-1}T_{p^{s+1}}T_{p^r} = \sum_{0\le t\le \mu}\left(p^{t(2k-1)}T_{p^{s+r-2t}} + p^{(t+1)(2k-1)}T_{p^{s+r-1-2t}}\right) - p^{2k-1}T_{p^{s-1}}T_{p^r}$$

Expanding out the $s-1$case of (11) gives (where here, $\mu' = \min(s-1, r)$)

$$T_{p^{s-1}}T_{p^r} = \sum_{0\le t\le \mu'} p^{t(2k-1)}T_{p^{s+r-2t}}$$

If $s > r$, then $\mu = \mu'$ since $s - 1 \ge r$ so $\mu' = r = \mu$. The case $s \le r$ is the only possible problem.
Suppose $s < r$. Then $\mu = s$ and $\mu' = s - 1$. Then

$$\begin{aligned} T_{p^{s+1}}T_{p^r} &= \sum_{0\le t\le s} p^{t(2k-1)}T_{p^{s+r+1-2t}} + \sum_{0\le t\le s} p^{(t+1)(2k-1)}T_{p^{s+r-1-2t}} - \sum_{0\le t\le s-1} p^{(t+1)(2k-1)}T_{p^{s+r-1-2t}} \\ &= \sum_{0\le t\le s} p^{t(2k-1)}T_{p^{s+r+1-2t}} + p^{(s+1)(2k-1)}T_{p^{s+r-1-2s}} \\ &= \sum_{0\le t\le s} p^{t(2k-1)}T_{p^{s+r+1-2t}} + p^{(s+1)(2k-1)}T_{p^{s+r+1-2(s+1)}} = \sum_{0\le t\le s+1} p^{t(2k-1)}p^{s+r+1-2t} \end{aligned}$$

which proves the induction for $s < r$. □

Recall from Theorem 16 that if $f(z) = \sum_{m=0}^{\infty} c(m)q^m$, $T_nf(z) = \sum_{m=0}^{\infty} r_(m)q^m$ with $r(m) = \sum_{d|(m,n)} d^{2k-1}c\left(\frac{mn}{d^2}\right)$. For each $k \in \mathbb{Z}$ and $n \in \mathbb{N}$, T_n is a linear operator mapping $\mathcal{M}_k$ tp $\mathcal{M}_k$. Let $n \in \mathbb{N}$. If $f \in \mathcal{M}_k$ is not identically zero and there exists a non-zero complex number $\lambda(n)$ such that $T_nf(z) = \lambda(n)f(z)$ then f is said to be an eigenfunction or eigenform of T_n and $\lambda(n)$ is said to be an eigenvalue of T_n.
Observe that if f is an eigenform of T_n then so is cf for all $c \in \mathbb{C}\backslash\{0\}$.
Next, notice that if $\mathcal{M}_k$ is of dimension 1 vector space then every non-zero element of $\mathcal{M}_k$ is an eigenform for T_n for $n \in \mathbb{N}$.
(Observe that if f is non-zero then theorem 16, for example, tells us that T_nf is non-zero). Similarly, if $\mathcal{M}_k^o$ is of dimension 1, the same conclusion follows.
Recall that $\dim \mathcal{M}_k = 1$ for $k = 0, 2, 3, 4, 5, 7$ and $\dim \mathcal{M}_k^o = 1$ for $k = 6, 8, 9, 10, 11, 13$. Further, since $\Delta(z) \in \mathcal{M}_6^o$ we see that Δ is an eigenform for T_n for all $n \in \mathbb{N}$.

Definition 10. *An eigenform for T_n for all $n \in \mathbb{N}$ is said to be a simultaneous eigenform.*

Definition 11. *An eigenform $f(z) = \sum_{m=0}^{\infty} c(m)q^m$ is said to be normalized if $c(1) = 1$.*

Theorem 21. *Let $k \in \mathbb{N}$, $k \ge 2$. If $\mathcal{M}_k$ contains a simultaneous eigenform $f(z)$ with $f(z) = \sum_{m=0}^{\infty} c(m)q^m$ then $c(1) \ne 0$.*

Proof. By Theorem 16, if $T_nf(z) = \sum_{m=0}^{\infty} r_n(m)q^m$ with $r_n(m) = \sum_{d|(m,n)} d^{2k-1}c\left(\frac{mn}{d^2}\right)$ then $r_n(1) = c(n)$. Since f is a simultaneous eigenform, $c(n) = \lambda(n)c(1)$ for some $\lambda(n) \in \mathbb{C}$, $\lambda(n) \ne 0$. Thus, if f is non-zero, there exists some $k \in \mathbb{N}$ such that $c(k) = \lambda(k)c(1) \ne 0$ so $c(1) \ne 0$. □

Theorem 22. *Assume that $f(z) = \sum_{m=0}^{\infty} c(m)q^m$ is a cusp form of weight $2k$. Then f is a simultaneous normalized eigenform if and only if*

$$c(m)c(n) = \sum_{d|(m,n)} d^{2k-1} c\left(\frac{mn}{d^2}\right)$$

for all positive integers m and n and $c(n)$ is an eigenvalue for T_n for every $n \in \mathbb{N}$.

Proof. ($\Rightarrow$) Suppose f is a simultaneous normalized eigenform. Then $T_n f = \lambda(n) f$, $\lambda(n) \in \mathbb{C}\backslash\{0\}$ for all $n \in \mathbb{N}$.
By Theorem 16, $r_n(1) = c(n)$ and $c(n) = \lambda(n)c(1) = \lambda(n)$ by normalization. Thus, for all $m \in \mathbb{N}$, $r_n(m) = \lambda(n)c(m) = c(n)c(m)$ as required.
($\Leftarrow$) Suppose $c(m)c(n) = \sum_{d|(m,n)} d^{2k-1} c\left(\frac{mn}{d^2}\right)$ for all $m, n \in \mathbb{N}$. Then for every $n \in \mathbb{N}$,

$$T_n f(z) = \sum_{m=0}^{\infty} r_n(m) q^m = c(n) \sum_{m=0}^{\infty} c(m) q^m = c(n) f(z)$$

so f is a simultaneous eigenform. Further, $c(n) = r_n(1) = c(n)c(1)$ so $c(1) = 1$. □

Recall that for $z \in H$,

$$\Delta(z) = (2\pi)^{12} \sum_{n=1}^{\infty} \tau(n) q^n = (2\pi)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

and $\Delta(z) = g_2^3(z) - 27 g_3^2(z)$.

Theorem 23. *For positive integers m and n, $\tau(m)\tau(n) = \sum_{d|(m,n)} d^{11} \tau\left(\frac{nm}{d^2}\right)$.*

Proof. Since $\Delta \in \mathcal{M}_6^o$, it is a simultaneous eigenform that is also a cusp form. Furthermore,

$$(2\pi)^{-12} \Delta(z) = \sum_{m=1}^{\infty} \tau(m) q^m$$

has $\tau(1) = 1$. Thus, $(2\pi)^{-12}\Delta(z)$ is a simultaneous normalized eigenform. Our result now follows from Theorem 22 with $k = 6$. □

Theorem 24. *For each integer $k \geq 2$, there is precisely one simultaneous normalized eigenform in $\mathcal{M}_k$ that is not a cusp form. Furthermore, it is*

$$f(z) = \frac{(2k-1)!}{2(2\pi i)^{2k}} G_k(z)$$

Recall that

$$G_k(z) = \sum_{(m,n) \neq (0,0)} \frac{1}{(mz+n)^{2k}}$$

Recall also as in the proof of Lemma 1 that

$$\sum_{n=-\infty}^{\infty} \frac{1}{(z+n)^k} = \frac{1}{(k-1)!} (-2\pi i)^k \sum_{r=1}^{\infty} r^{k-1} q^r$$

Replacing z by mz, we find that

$$G_k(z) = \sum_{(m,n)\neq(0,0)} \frac{1}{(mz+n)^{2k}} = 2\zeta(2k) + 2\sum_{n=1}^{\infty}\sum_{m=-\infty}^{\infty} \frac{1}{(mz+n)^{2k}}$$
$$= 2\zeta(2k) + \frac{2(-2\pi i)^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sum_{r=1}^{\infty} r^{2k-1}q^{nr} = 2\zeta(2k) + \frac{2(2\pi i)^{2k}}{(2k-1)!}\sum_{l=1}^{\infty}\sigma_{2k-1}(l)q^l$$

where the last equality follows by summing over the common products $nr = l$ for $l \in \mathbb{N}$. Thus, dividing through by the coefficient of the series above gives

$$\frac{(2k-1)!}{2(2\pi i)^{2k}}G_k(z) = \frac{(2k-1)!}{(2\pi i)^{2k}}\zeta(2k) + \sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n$$

and by Euler's theorem, $\zeta(2k) = 2^{2k-1}(2k!)^{-1}B_k\pi^{2k}$ so that

$$\frac{(2k-1)!}{2(2\pi i)^{2k}}G_k(z) = \frac{(-1)^k B_k}{4k} + \sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n$$

Observing that $\sigma_{2k-1}(1) = 1$, it follows that $\frac{(2k-1)!}{2(2\pi i)^{2k}}G_k(z)$ is normalized.

Proof of Theorem 24. Suppose that f is a simultaneous normalized eigenform of weight $2k$ which is not a cusp form. Let $f(z) = \sum_{m=0}^{\infty} c(m)q^m$, $c(0) \neq 0$ and $c(1) = 1$. The relation $T_n f = \lambda(n)f$ implies that $r_n(m) = \lambda(n)c(m)$ for $m \in \mathbb{N}$. An argument we have used a few times shows that $c(n) = \lambda(n)$ for all $n \in \mathbb{N}$. Now by Theorem 16,

$$r_n(0) = \sum_{d|(n,0)} d^{2k-1}c(0) = c(0)\sigma_{2k-1}(n)$$

We also have $r_n(0) = \lambda(n)c(0) = c(n)c(0)$. Since $c(0) \neq 0$ we see that $c(n) = \sigma_{2k-1}(n)$ for $n \in \mathbb{N}$.
Thus,

$$f(z) = c(0) + \sum_{m=1}^{\infty}\sigma_{2k-1}(m)q^m$$

f is modular of weight $2k \geq 4$ so $c(0)$ is uniquely determined since if $f_1(z) = c_1(0) + \sum_{m=1}^{\infty}\sigma_{2k-1}(m)q^m$ is also a simultaneous eigenform then the difference is $c_0 - c_1$ and this is a contradiction.
Since

$$f(z) = \frac{(2k-1)!}{2(2\pi i)^{2k}}G_k(z) = \frac{(-1)^k B_k}{4k} + \sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n$$

is a modular form of weight $2k$ it is the only possible normalized simultaneous eigenform of weight $2k$. But for all $m, n \in \mathbb{N}$,

$$\sigma_{2k-1}(m)\sigma_{2k-1}(n) = \left(\sum_{d|m} d^{2k-1}\right)\left(\sum_{e|n} e^{2k-1}\right) = \sum_{\substack{d|m\\ e|n}}(de)^{2k-1}$$
$$= \sum_{d|(m,n)}\left(\sum_{l|\frac{mn}{d^2}} l^{2k-1}\right) = \sum_{d|(m,n)}\sigma_{2k-1}\left(\frac{mn}{d^2}\right)$$

Thus, by Theorem 22, f is a simltaneous normalized eigenform. □

What about simultaneous cuspforms? We can determine then for k small easily. When $\dim \mathcal{M}_k^o = 1$, we have exactly one such form. This happens when $k = 6, 7, 8, 9, 10, 11, 13$.
We know that $(2\pi)^{-12}\Delta(z)$ is a cusp form which is a simultaneous normalized eigenform of weight 12. Further, $\Delta(z)G_{k-6}(z)$ is a cusp form of weight $2k$ for $k = 8, 9, \ldots$.
If we define, for $k \geq 2$,

$$E_k(z) = \frac{1}{2\zeta(2k)}G_k(z) = 1 + \frac{(-1)^k 4k}{B_k}\sum_{k=1}^{\infty}\sigma_{2k-1}(n)q^n$$

then we see that $(2\pi)^{-12}\Delta(z)E_{k-6}(z)$ is a simultaneously normalized eigenform of weight $2k$ which is a cusp form for $k = 8, 9, 10, 11, 13$ (as $\Delta(z)$ has lowest order term z, as it is a cusp form). We have

$$E_2(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n$$
$$E_3(z) = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n$$

and so forth. We can use these functions to prove seemingly surprising relations between the $\sigma_{2k-1}(n)$ values.
Since $\dim \mathcal{M}_k = 1$ for $k = 2, 3, 4, 5, 7$, we see that $E_2^2 = E_4$, $E_2E_3 = E_5$, $E_7 = E_2E_5 = E_3E_4$. For the first case, notice

$$(E_2(z))^2 = \left(1 + 20\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^2 = 1 + 480\sum_{n=1}^{\infty}\sigma_7(n)q^n$$

and therefore for every $n \geq 1$,

$$\sigma_7(n) = \sigma_3(n) + 120\sum_{k=1}^{n-1}\sigma_3(k)\sigma_3(n-k)$$

Similarly, for $E_2E_3 = E_5$,

$$11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 5040\sum_{k=1}^{n-1}\sigma_3(k)\sigma_5(n-k)$$

Finally, $E_6 - E_3^2$ is a modular form of weight 12. Further, it has constant coefficient $\frac{762048}{691}$. Thus,

$$\frac{691}{762048}\left(E_6 - E_3^2\right) = (2\pi)^{-12}\Delta(z) = \sum_{n=1}^{\infty}\tau(n)q^n$$

By examining the coefficients $r(n)$ of q^n, we find

$$r(n) = \frac{691}{762048}\left(\frac{65520}{691}\sigma_{11}(n) + 1008\sigma_5(n) - (504)^2\sum_{k=1}^{n-1}\sigma_5(k)\sigma_5(n-k)\right)$$

which is $\tau(n)$.
Thus, $762048\tau(n) \equiv 65520\sigma_{11}(n) \pmod{691}$ and so $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$, called *Ramanujan's congruence*.

Other Directions in Modular Forms

Let $f(z) = \sum_{n=1}^{\infty} c(n)q^n$ be a cusp form of weight $2k$. Hecke associated to f the Dirichlet series $L_f(s) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s}$. This is not arbitrary. Indeed, let us define the Mellin transform of f, $\mathcal{M}(f)(s)$ as

$$\mathcal{M}(f)(s) = \int_0^{\infty} f(it)t^{s-1}dt$$

Notice that if $f(z) = \mathrm{e}^{iz}$ then $\mathcal{M}(f)(s) = \Gamma(s)$, for $\mathrm{Re}(s) > 0$.
If f is a cusp form then

$$\begin{aligned}\mathcal{M}(f)(s) &= \sum_{n=1}^{\infty} c(n) \int_0^{\infty} e^{-2\pi nt} t^{s-1} dt = \frac{1}{2\pi} \sum_{n=1}^{\infty} \frac{c(n)}{n} \int_0^{\infty} e^{-u} \left(\frac{u}{2\pi n}\right)^{s-1} du \\ &= (2\pi)^{-s} \left(\int_0^{\infty} \mathrm{e}^{-u} u^{s-1} du \right) \sum_{n=1}^{\infty} \frac{c(n)}{n^s} = (2\pi)^{-s} \Gamma(s) L_f(s)\end{aligned}$$

Suppose that f is a simultaneous normalized eigenform, say $f(z) = \sum_{n=1}^{\infty} c(n)q^n$. Then $L_f(s) = \sum_{n=1}^{\infty} \frac{c(n)}{n^s}$. It is not difficult to show that $c(n) = O(n^k)$. Thus, $L_f(s)$ is defined by the series as an analytic function for $\mathrm{Re}(s) > k+1$.
Since f is a simultaneous normalized eigenform, $L_f(s)$ has an Euler product representation

$$L_f(s) = \prod_p \left(1 - c(p)p^{-s} + p^{2k-1-2s}\right)^{-1}$$

for $\mathrm{Re}(s) \geq k+1$. Hecke used this to extend $L_f(s)$ analytically to all of $\mathbb{C}$. He put $\Lambda_f(s) = (2\pi)^{-s}\Gamma(s)L_f(s)$ and he showed that $\Lambda_f(s) = (-1)^k \Lambda_f(2k-s)$.
Petersson conjectured that if f is a simultaneous normalized eigenform in $\mathcal{M}_k^o$ then $|c(p)| \leq 2p^{k-\frac{1}{2}}$ for p prime. This generalized Ramanujan's conjecture that $|\tau(p)| \leq 2p^{\frac{11}{2}}$ for p prime. More generally, Ramanujan conjectured that $|\tau(n)| \leq d(n)n^{\frac{11}{2}}$. These two conjectures were proved by Deligne in 1973 as a consequence of his proofs of the Weil conjectures.
Let $a, b \in \mathbb{Z}$ with $4a^3 + 27b^2 \neq 0$ and put $E : y^2 = x^3 + ax + b$. For any prime p we can consider the reduction of E mod p. Usually we get an elliptic curve mod p in particular when $4a^3 + 27b^2 \equiv 0 \pmod{p}$ and in this case we say that we have good reduction. We count the number of points $\#E(\mathbb{F}_p)$ on the reduced curve.
Hasse proved that if we put $a_p = p + 1 - \#E(\mathbb{F}_p)$ then $|a_p| \leq 2\sqrt{p}$. Define $L_p(E, s)$ by

$$L_p(E,s) = \begin{cases} (1 - a_p p^{-s} + p^{1-2s})^{-1} & \text{if } E \text{ has good reduction mod } p \\ (1-p^{-s})^{-1} & \text{if } E \text{ has split multiple reduction mod } p \\ (1+p^{-s})^{-1} & \text{if } E \text{ is non-split} \\ 1 & \text{otherwise} \end{cases}$$

Birch and Swinnerton-Dyer conjectured that the rank of rational points of E is equivalent to the order of the pole of $L(E, s)$ at $s = 1$.

In this curse, we have concentrated on modular forms, i.e. forms connected with the full modular group. There is an associated theory for subgroups of the modular group. There is an associated theory for subgroups of the modular group. In particular, let N be a positive integer. Then $\Gamma_0(N)$ consists of those

elements $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ for which $c \equiv 0 \pmod{N}$. An elliptic curve E is said to be modular if the cusp form f of weight 2 for $\Gamma_0(N)$ for some N, such that $L_f(s) = L(E, s)$.

Taniyama and Shimura conjectured that every elliptic curve over $\mathbb{Q}$ is modular. This has now been proved by Wiles, Taylor, Diamond, Breuil and Conrad. This was a key ingredient in the proof by Wiles of Fermat's last theorem.

Frey showed that if p is a prime with $p \geq s$ and u, v, w are positive integers with $u^p + v^p = w^p$ then we can consider the elliptic curve E given by $E : y^2 = x(x - u^p)(x - v^p)$. Further, if E is modular then $L(E, s) = L_f(s)$ for a cusp form of weight 2 on $\Gamma_0(N)$ where $N = \prod_{\substack{q|uvw \\ q \text{ prime}}} q$.

By a result of RIbet there is an associated f_1 with level 2 and inspection shows no such f_1 exists, a contradiction that proves FLT.