Modular Forms and Representation Theory.

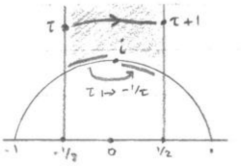
Definition: Upper half-plane, H = complex numbers τ with $\operatorname{im}\tau > 0$.
Modular group, $\Gamma = SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z},\ ad - bc = 1 \right\}$

$SL_2(\mathbb{Z})$ (or $SL_2(\mathbb{R})$) acts on H by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}(\tau) = \frac{a\tau + b}{c\tau + d}$.

Exercise: Check $(AB)(\tau) = A(\theta(\tau))$

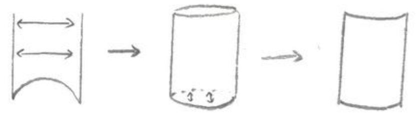
A modular function (= "meromorphic modular form of weight 0") is a function on H (meromorphic in H and at "$i\infty$") invariant under $\Gamma = SL_2(\mathbb{Z})$, = function on quotient Γ/H.
Example: constant functions.

What is Γ/H? Fundamental domain for Γ acting on H = nice subset containing a unique point in each orbit.
Standard fundamental domain:



$SL_2(\mathbb{Z})$ contains: $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} : \tau \mapsto \tau + 1$
$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} : \tau \mapsto -1/\tau$.

So Γ/H = funny-shaped region / identification of boundary points.



$\cong \mathbb{R}^2$ Add a point at "$i\infty$" $\Rightarrow$ get S^2.

Deep Theorem: Any Riemann surface homeomorphic to S^2 is isomorphic to S^2 (as Riemann surfaces).

This implies there is an isomorphism j of Riemann surfaces from $\Gamma/H \cup i\infty \to \mathbb{C} \cup \infty$.
So modular functions are all of form $f(j(\tau))$, where f = meromorphic function on $\mathbb{C} \cup \infty$, = rational function.

Explicit construction of $j(\tau)$.

$j(\tau) = j(\tau+1)$, so $j(\tau) = \sum c(n) e^{2\pi i n \tau} = \sum c(n) q^n$, where $q = e^{2\pi i \tau}$.
Simplest case: $j(\tau) = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots$

$$= \frac{\left(1 + 240 \cdot \sum_{m>0} \sigma_3(m) q^m\right)^3}{q \cdot \prod_{n \geq 1} (1-q^n)^{24}}, \quad \text{where } \sigma_3(n) = \sum_{d|n} d^3.$$

Note: "$j(\tau)$ is meromorphic at $i\infty$" means meromorphic at $q=0$ (as a function of q).

Suppose we find two 1-forms $f(\tau)d\tau$, $g(\tau)d\tau$ on H invariant under Γ. Then $\frac{f(\tau)d\tau}{g(\tau)d\tau} = \frac{f(\tau)}{g(\tau)}$ is a modular function. What is the condition for $f(\tau)d\tau$ to be invariant?

Need $f\left(\frac{a\tau+b}{c\tau+d}\right) \underbrace{d\left(\frac{a\tau+b}{c\tau+d}\right)}_{= \frac{ad-bc}{(c\tau+d)^2} d\tau \,=\, \frac{d\tau}{(c\tau+d)^2}} = f(\tau)d\tau$

So $f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2 f(\tau)$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

Functions with this property are called modular forms of weight 2 (if holomorphic on H and at $i\infty$).

A modular form of weight k: $f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau)$, if holomorphic on H and at $i\infty$

If f, g have weight k, then f/g is a modular function.

If f, g have weights k_1, k_2, then fg has weight $k_1 + k_2$.

Examples of modular forms:

(i) Eisenstein Series. $E_k(\tau) = 1 - \frac{2k}{B_k} \cdot \sum_{n\geq 1} \sigma_{k-1}(n) q^n$ for k even, $k \geq 4$; where $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$,

and B_k are the Bernoulli numbers, given by: $\frac{x}{e^x - 1} = \sum_{n\geq 0} \frac{B_n x^n}{n!}$

n:	0	1	2	3	4	5	6	7	8	...
B_n:	1	$-\frac{1}{2}$	$\frac{1}{6}$	0	$\frac{-1}{30}$	0	$\frac{1}{42}$	0	$\frac{-1}{30}$	...

Eg: $E_4(\tau) = 1 - \frac{8}{-1/30} \cdot \sum_n \sigma_3(n) q^n = 1 + 240 \sum_n \sigma_3(n) q^n = 1 + 240q + 2160q^2 + \cdots$

= modular form of weight 4.

(ii) $\Delta(\tau) = q \cdot \prod_{n\geq 1} (1-q^n)^{24} = q - 24q^2 + 252q^3 + \cdots = \sum_n \tau(n) q^n$, where τ is Ramanujan's τ-function: it satisfies $\tau(m)\tau(n) = \tau(mn)$ if $(m,n) = 1$

$\tau(p) \leq 2p^{1/2}$ (p prime) [Deligne 1974]

$\Delta(\tau)$ = modular form of weight 12.

So $j(\tau) = \frac{E_4(\tau)^3}{\Delta(\tau)}$, of weight $3.4 - 12 = 0$.

(iii) Suppose E is an elliptic curve defined over $\mathbb{Q}$. (Riemann surface homeomorphic to torus = $S^1 \times S^1$). Eg: $y^2 + y = x^3 - x^2 - 10x - 20$.

E has an L-series: $\sum_{n\geq 1} \frac{c(n)}{n^s}$, $c(p)$ related to the number of points on E defined over $\mathbb{F}_p$.

(Wiles): If E is "semistable" then $\sum c(n) q^n$ is a modular form [at "level $N > 1$", ie replace $SL_2(\mathbb{Z})$ by $\Gamma_0(N) = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : N | c \}$).

$\Rightarrow$ Fermat's Last Theorem.

(iv) Theta Functions: How many ways can an integer be written as the sum of four squares? = solutions of $n = x_1^2 + \cdots + x_4^2$, $x_i \in \mathbb{Z}$.

= coefficient of q^n in $(\underbrace{\sum_m q^{m^2}})^4$

– This is a modular form (at level $N > 1$).

More generally, let L be a lattice in $\mathbb{R}^n$, with inner product $(,)$.

So L = discrete free abelian subgroup of $\mathbb{R}^n$ of rank n, such that $(\alpha, \beta) \in \mathbb{Z}$ if $\alpha, \beta \in L$.

Eg: $L = \mathbb{Z}^n \subset \mathbb{R}^n$. Put $\Theta_L(\tau) = \sum_{\lambda \in L} q^{\lambda^2/2}$ = modular form.

(v) $e^{\pi\sqrt{163}} = 262537412640768743 \cdot 99999999999925$ $\quad 262\cdots 68000 = 2^{18}.3^3.5^3.23^3.29^3$

$e^{\pi\sqrt{67}} = 147197952743 \cdot 999998$ $\quad 147\ldots 52000 = 2^{15}.3^3.5^3.11^3$

$e^{\pi\sqrt{43}} = 884736743 \cdot 99977$ $\quad 86\ldots 6000 = 2^{18}.3^3.5^3$ – cubes of smooth numbers.

Explanation: $j(\tau)$ is an algebraic integer if $\tau = \frac{a + i\sqrt{b}}{c}$ for $a, b, c \in \mathbb{Z}$.

τ = "imaginary quadratic irrational"

So $j(\tau)$ = number x with $x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$, some $a_i \in \mathbb{Z}$

(Degree = class number of some order of imaginary quadratic field).

Relation with Moonshine.

Finite simple groups: ~ 40 infinite groups, 26 exceptions.

Largest sporadic group = "Monster". Order = $2^{46}.3^{20}.5^{12}.7^{6}.11^{2}.13^{3}.17.19.23.29.31.41.47.59.71 \sim 10^{54}$

Dimensions of representations ("action of group on complex vector space").

Smallest has dimension $\overset{\curvearrowright}{196883}$ (cf: $j(\tau) = q^{-1} + 744 + 196884q + \underset{\text{\small Σ first three irreducible representations of Monster.}}{\overset{\shortparallel}{21493760}} q^2 + \dots$)

(Proved by Frenkel, Lep, Memman, McKay, Thompson, Conway, Norton, ...)

M acts on ∞-graded vector space $V = \bigoplus_{n} V_n$, $\dim V_n = c(n)$.

Upcoming Main Theorems.

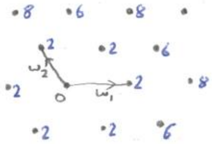
1. The following are examples of modular forms:
   - Eisenstein Series, $E_k = 1 - \frac{2k}{B_k} \sum \sigma_{k-1}(n) q^n$, where $q = e^{2\pi i c}$, k even ≥ 4, of weight k
   - Delta Function, $\Delta(\tau) = q.\prod(1-q^n)^{24}$, of weight 12.
   - Theta function $\theta_L(\tau)$ of even unimodal Lattices in $2k$ dimensions - of weight k.

     ↑ volume of fundamental domain of $\mathbb{R}^{2k}/$Lattice $=1$

     norm (v,v) of any vector is even.

$$\theta_L(\tau) = \sum_{\lambda \in L} q^{\lambda^2/2}, \quad \lambda^2 = (\lambda, \lambda)$$
$$= \sum_{n \in \mathbb{Z}} c(n) \cdot q^n, \quad c(n) = \text{number of vectors of } L \text{ of norm } 2n.$$

Example: - of an even lattice.



$(\omega_1, \omega_1) = (\omega_2, \omega_2) = 2$

$(\omega_1, \omega_2) = -1.$

Matrix of inner products $(\omega_i, \omega_j) = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$

$(m\omega_1 + n\omega_2)^2 = (m\omega_1 + n\omega_2, m\omega_1 + n\omega_2) = m^2\omega_1^2 + n^2\omega_2^2 + 2mn(\omega_1 + \omega_2) = $ even.

Theta function: Eg, $(2\omega_2 + \omega_1)^2 = 4\omega_2^2 + \omega_1^2 + 4(\omega_2, \omega_1) = 8 + 2 - 4 = 6.$

$$\theta_L(\tau) = \underset{\substack{\uparrow \\ \text{1 vector} \\ \text{of norm 0}}}{1 \cdot q^0} + \underset{\substack{\uparrow \text{6 vectors} \\ \text{of norm } 2\times 1}}{6 \cdot q^1} + 6 \cdot q^2 + 6 \cdot q^3 + \cdots$$

But the lattice is not unimodular. Volume of fundamental domain $= \sqrt{\det\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}} = \sqrt{3} \neq 1$

2. Classification of all modular forms, functions.

   Modular functions are exactly rational functions of $j(\tau) = E_4(\tau)^3/\Delta(\tau)$

   Ring of modular forms is graded by weight. (ie, $= \bigoplus M_k$, $M_k =$ forms of weight k)

   In fact, ring of modular forms $= \mathbb{C}[E_4, E_6] =$ ring of polynomials in E_4, E_6.

$k =$	0	2	4	6	8	10	12	14	16	18	...
	1	–	E_4	E_6	E_4^2	E_4E_6	E_6^2				
							E_4^3	$E_4^2E_6$	$E_4E_6^2$	E_6^3	
									E_4^4	...	

Eg: "modular forms of weight 12" is a 2-dimensional vector space spanned by E_4^3, E_6^2.

Application: We will calculate the number of norm 4 vectors of the Leech Lattice (without knowing what it is exactly). Leech Lattice is a 24-dimensional even unimodular Lattice with no norm 2 vectors. (Construction hard - see Conway & Stone)

Conway: Aut (Leech Lattice) = double cover of Conway's largest sporadic simple group.

Look at $\theta_\Lambda(\tau) = 1 + c(1)q^1 + c(2)q^2 + c(3)q^3 + \cdots$, $c(n)$ = number of vectors of norm $2n$.

We know (i) $c(1) = 0$, (ii) $\theta_\Lambda(\tau)$ is a modular form of weight 12.

So $\theta_\Lambda(\tau) = a E_4(\tau)^3 + b E_6(\tau)^2$, some a, b. Fix a, b by looking at coefficients of $q^0, q^1, \ldots$

q^0: $a + b = 1$

Recall: $E_4(\tau) = 1 + 240q + 2160q^2 + \cdots \Rightarrow E_4^3 = 1 + 720q + 179280q^2 + \cdots$

$E_6(\tau) = 1 - 504q - 4536q - \cdots \Rightarrow E_6^2 = 1 - 1008q + 220752q^2 + \cdots$

So q^1: $0 = 720a - 1008b \Rightarrow a = \frac{1008}{1728}$, $b = \frac{720}{1728}$.

So $\theta_\Lambda(\tau) = \frac{1008}{1728} E_4^3 + \frac{720}{1728} E_6^2 = 1 + \underbrace{196560}_{} q^2 + 16773120 q^3 + \cdots$

$\hookrightarrow$ = number of norm 4 vectors of Leech lattice.

Remark: How many non-overlapping spheres can touch a fixed sphere in n-dimensional space?

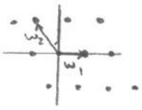
$n = 1$:	2
$n = 2$:	6
$n = 3$:	12 (eg, iron atom in crystal)
$n = 4$:	24, 25
$n = 5, 6, 7$:	?
$n = 8$:	240
$n = 9, \ldots, 23$:	?
$n = 24$	196560 (placing them on points of Leech lattice!)
$n = 25+$	?

Look at action of $SL_2(\mathbb{Z})$ on H and on 2-dimensional lattices with bases.

Problem: functional equation $f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau)$ is a bit complicated.

We want to show that modular forms just correspond to functions of lattices $L \subseteq \mathbb{C}$ with a much simpler functional equation.

(Non-integral) lattice in $\mathbb{C}$ is just a subgroup of $\mathbb{C} = \mathbb{R}^2$ generated by two vectors w_1, w_2 linearly independent over $\mathbb{R}$. Typical example:



So, lattice = $\{ m w_1 + n w_2 : m, n \in \mathbb{Z} \}$

= "2-dimensional crystal".

We say two lattices L_1, L_2 are the same shape if $L_1 = \lambda L_2$ for some $\lambda \in \mathbb{C}$.

$\lambda = x e^{i\theta}$, $x \in \mathbb{R}$. $e^{i\theta} L$ = rotation of L through angle θ.

xL = magnification of L by factor x.

If L is a lattice in $\mathbb{C}$, then $\mathbb{C}/L$ is an elliptic curve. If $L_1 = \lambda L_2$ for $\lambda \in \mathbb{C}$, then $\mathbb{C}/L_1 \cong \mathbb{C}/L_2$ as Riemann surfaces.

It is also known that: (i) All elliptic curves come from lattices L.

(ii) If $\mathbb{C}/L_1 \cong \mathbb{C}/L_2$ then L_1, L_2 are of the same shape.

So, set of isomorphism classes of elliptic curves = $\dfrac{\text{set of lattices in } \mathbb{C}}{\text{being same shape}}$

$\|$

"moduli space of elliptic curves"

Any lattice can be specified by giving a basis $\omega_1, \omega_2 \in L = \{m\omega_1 + n\omega_2 : m, n \in \mathbb{Z}\}$.
Basis not unique: if $\{\omega_1, \omega_2\}$ is a basis, so is $\{a\omega_1 + b\omega_2, c\omega_1 + d\omega_2\}$ for any $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Z}) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{Z}) : \det = \pm 1\}$.

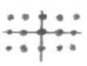
Oriented base $\{\omega_1, \omega_2\}$ is a base with $\operatorname{Im}\left(\frac{\omega_1}{\omega_2}\right) > 0$. If $\{\omega_1, \omega_2\}$ is an oriented basis, then $\{a\omega_1 + b\omega_2, c\omega_1 + d\omega_2\}$ is oriented if $\det\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = +1$, and not oriented if $\det = -1$.
So,
$$\frac{\text{set of lattices in } \mathbb{C}}{\text{multiplication by } \lambda \in \mathbb{C}^\times} = \frac{\text{set of lattices } L \text{ with oriented base}}{\begin{array}{c}\text{action of } SL_2(\mathbb{Z}) \text{ on possible oriented bases} \\ \text{and action of } \mathbb{C}^\times \text{ on lattices } L\end{array}}$$

(Choose λ so that ω_2 becomes 1)
$$= \frac{\text{lattices } L \text{ with base } \tau, 1,\ \operatorname{im}\tau > 0}{\text{action of } SL_2(\mathbb{Z}).}$$

(Action of $SL_2(\mathbb{Z})$ on lattices L with base $\tau, 1$: $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ takes L with basis $\tau, 1$ to L with basis $a\tau + b, c\tau + d$, $= (c\tau + d) \times \left(L/(c\tau+d), \text{ basis: } \frac{a\tau+b}{c\tau+d}, 1\right)$. So $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ takes L to $L/(c\tau+d)$ with basis $\frac{a\tau+b}{c\tau+d}, 1$.)
$$\cong \frac{\text{upper half plane}, H}{\left(\begin{array}{c}\text{action of } SL_2(\mathbb{Z}) \text{ given} \\ \text{by } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(\tau) = \frac{a\tau+b}{c\tau+d}\end{array}\right)} \qquad (= \text{similarity classes of lattices}).$$

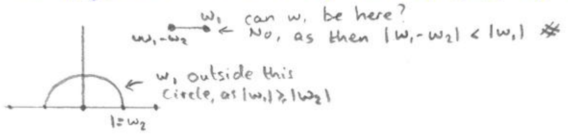
Modular function f:= function on H invariant under $SL_2(\mathbb{Z})$, = function g of lattices, homogeneous of degree 0 (ie, $g(\lambda L) = g(L)$), = functions of elliptic curves.
"Non-holomorphic" modular forms of weight k are "same as" functions g of lattices L, homogeneous of degree $-k$ (ie, $g(\lambda L) = \lambda^{-k} g(L)$).
$$f(\tau) \longrightarrow g(\langle \omega_1, \omega_2 \rangle) = \omega_2^{-k} f\left(\tfrac{\omega_1}{\omega_2}\right), \quad (\omega_1, \omega_2 = \text{oriented basis of } L)$$
$$f(\tau) = g(\langle \tau, 1 \rangle) \longleftarrow g$$
Need to check that this correspondance is well-defined and gives an isomorphism between the two spaces of functions. Eg, check g is a well-defined function of lattice L (ie, does not depend on choice of basis ω_1, ω_2). So have to check: $\omega_2^{-k} f\left(\frac{\omega_1}{\omega_2}\right) = (c\omega_1 + d\omega_2) . f\left(\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2}\right)$
This is equivalent to: $f(\tau) = (c\tau + d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right)$ where $\tau = \omega_1/\omega_2$. This is the functional equation for modular forms.

We will construct modular forms as follows:
(i) Find some function of lattices (eg, Weierstrass $\wp(z, L)$).
(ii) Try to make it homogeneous of some degree.

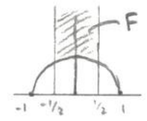
We want to find a "nice" fundamental domain F for $SL_2(\mathbb{Z})$ on H. (So every point of H should be conjugate to a unique point of F, so F can be identified with $SL_2(\mathbb{Z}) \backslash H$).
We use correspondance between points τ of H and lattices $L = \langle \tau, 1 \rangle = \{m\tau + n : m, n \in \mathbb{Z}\}$.
If we have a lattice L, can we find a canonical basis ω_1, ω_2 for it?
"Canonical": if $L, \lambda L$ are lattices, $\lambda \in \mathbb{C}^\times$, the canonical base for λL should be $\lambda \times$ the canonical base for L. But this is not possible. For example, take the canonical base ω_1, ω_2. Take $\lambda = -1$, so $\lambda L = L$, but $(\lambda\omega_1, \lambda\omega_2) \neq (\omega_1, \omega_2)$. Can we find a base canonical up to sign?
No: eg, square lattice:  $iL = L$. So if ω_1, ω_2 is a base, so is $i\omega_1, i\omega_2$, and this is not $\pm\ \omega_1, \omega_2$.

eg, triangular lattice: Let $\omega^3 = -1$, so $\omega = \frac{1}{2} + i\frac{\sqrt{3}}{2}$. Then $\omega L = L$.

Problem is caused by automorphisms σ of lattices L, given by multiplication. If σ is such an automorphism and w_1, w_2 is a basis, then so is $\sigma(w_1), \sigma(w_2)$.
$\mathrm{Aut}(L)$ acts on sets of bases of L. Can we find a canonical orbit of bases under $\mathrm{Aut}(L)$?
Yes, as follows: First choose basis element w_2 as shortest non-zero element of L (length of $\lambda = |\lambda|$)
Then choose second basis element w_1 as next shortest element of L, not a multiple of w_2, with $\mathrm{im}\left(\frac{w_1}{w_2}\right) > 0$. Scale L by multiplying by a constant so that $w_2 = 1$. What can w_1 be?


w_1 can w_1 be here?
$w_1 - w_2$
No, as then $|w_1 - w_2| < |w_1|$ ※
w_1 outside this circle, as $|w_1| \geq |w_2|$
$1 = w_2$

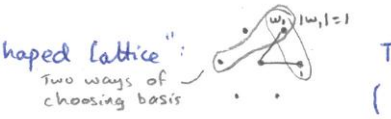
We have $|w_1 - w_2| \geq |w_1|$. $|w_1 - 1| = |w_1| \Rightarrow \mathrm{Re}(w_1) = 1/2$
Similarly, $|w_1 + w_2| \geq |w_1|$. $|w_1 + 1| = |w_1| \Rightarrow \mathrm{Re}(w_1) = -1/2$ } Take:



So, put $F = \{\tau : |\tau| \geq 1, |\mathrm{Re}(\tau)| \leq 1/2\}$. We have shown that if we choose w_1, w_2 as above, then $\frac{w_1}{w_2} \in F$. Conversely, if $\tau \in F$ and $L = \langle 1, \tau \rangle$, then 1 is element of smallest length, and τ is element of smallest length not in $\mathbb{Z} \subseteq L$. (Exercise.)

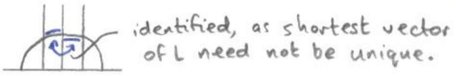
When can two elements of F correspond to the same lattice? When are rules for choosing a base ambiguous? (Trivial change: $w_2 \to -w_2$).
(i) might be more than one shortest vector L other than $w_2, -w_2$.
(ii) might be more than one shortest vector not a multiple of w_2.

Case (i): "Diamond-shaped lattice":

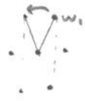


Two values of $\frac{w_1}{w_2}$ are related by $\tau_1 \tau_2 = -1$.
$(w_1, 1 \Rightarrow \tau_1 = w_1$, and $-1, w_1 \Rightarrow \tau_2 = -1/w_1)$.

So,

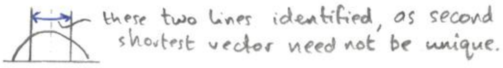


Case (ii): Eg:



$|w_1| = |w_1 - 1|$, so $\mathrm{Re}(w_1) = 1/2$. So vectors τ in F with $\mathrm{Re}(\tau) = 1/2$ give same lattice as vectors $\tau - 1$ with $\mathrm{Re} = -1/2$.

So,


these two lines identified, as second shortest vector need not be unique.

Summary: For each lattice we can find a basis $(\tau, 1)$ with $\tau \in F$, and if τ is on the boundary of F, τ is not quite unique (unless $\tau = i$). Conversely, easy to check that τ is unique except for cases listed above.

Recall that H acted on by $SL_2(\mathbb{Z})$ is "same as" $\frac{\text{lattices}}{\mathbb{C}^\times}$ with bases w_1, w_2 acted on by $SL_2(\mathbb{Z})$.
Each lattice has basis $\tau, 1$ with τ in F is same as saying that each τ in H is conjugate under $SL_2(\mathbb{Z})$ to a point of F unique up to exceptions above.
So F is almost a fundamental domain for $SL_2(\mathbb{Z})$, except for problems on boundary.

Lemma: $SL_2(\mathbb{Z})$ is generated by elements $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Corollary: $f(\tau)$ is a modular form of weight k iff f is holomorphic, and $f(\tau) = f(\tau+1)$, $f(\frac{-1}{\tau}) = \tau^k f(\tau)$.
Proof: By exercise 3, if f transform properly under $A, B \in SL_2(\mathbb{Z})$ then it transforms under AB, so sufficient to check functional equation for f under a set of generators of $SL_2(\mathbb{Z})$.

Proof of lemma: Take any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Try to make it $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ by multiplying by S,T on right, trying to make $|c|$ as small as possible. So we can assume that bottom Left corner of $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ cannot be decreased by multiplying by S,T.

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} S = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} * & * \\ d & -c \end{pmatrix}$ - so if $|c|$ is as small as possible, then $|d| \geq |c|$.

If c is non-zero, Look at $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} T^n = \begin{pmatrix} * & * \\ c & nc+d \end{pmatrix}$.

If $c \neq 0$, $nc+d$ can be made to be $< c$ in absolute value. But $|nc+d| \geq |c| \Rightarrow c = 0$.

So we can assume $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \underset{=1 \text{ or } S^2}{\underset{\uparrow}{\pm 1}} \times \underset{\uparrow \text{power of } T.}{\begin{pmatrix} 1 & \pm b \\ 0 & 1 \end{pmatrix}}$

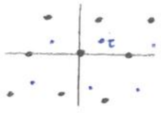
Remark: This is really the Euclidean algorithm for finding the hcf of c,d. (Keep subtracting a multiple of the smaller from the other.

Reminder: Modular forms $f(\tau)$ are "same as" functions g of lattices $L \subseteq \mathbb{C}$, homogeneous of degree $-k$.

Trigonometric function: $f(\tau) = f(\tau+\lambda)$ for $\lambda \in \mathbb{Z}$ (or $\in 2\pi i\,\mathbb{Z}$)

Elliptic Function: $f(\tau) = f(\tau+\lambda)$ for $\lambda \in$ lattice L (f a meromorphic function on $\mathbb{C}$).

Construct a function: Take any function $g(\tau)$. Let $f(\tau) = \sum_{\lambda \in L} g(\tau+\lambda)$. This obviously satisfies $f(\tau+\lambda) = f(\tau)$, provided it converges nicely (and uniformly on compact subsets). What can we use for g? In order for the sum to converge, we should have



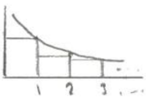
$g(\tau) \to 0$ as $\tau \to \infty$. Simplest possibilities: $g(\tau) = \frac{1}{\tau^n}$, $n \in \mathbb{Z}$, $n > 0$.

When does $\sum_{\lambda \in L} \frac{1}{(\tau-\lambda)^n}$ converge nicely? For large λ, $\frac{1}{(\tau-\lambda)^n} \approx \frac{1}{\lambda^n}$.

So look at convergence of $\sum'_{\lambda \in L} \frac{1}{|\lambda|^n}$, $\left(\sum'_{\lambda \in L} = \sum_{\lambda \in L, \lambda \neq 0}\right)$

Compare with some integral. Say, Look at convergence of $\sum_{n \geq 1} \frac{1}{n^x}$ - close to $\int_1^\infty \frac{dn}{n^x}$

Find $\sum_{n \geq 1} \frac{1}{n^x}$ converges iff $\int_1^\infty \frac{dn}{n^x}$ converges, $= \left[\frac{n^{1-x}}{1-x}\right]_1^\infty$ - converges if $\mathrm{Re}(x) > 1$.



Similarly we find that $\sum'_{\lambda \in L} \frac{1}{|\lambda|^n}$ converges nicely iff $\iint_{\substack{x,y \in \mathbb{R} \\ x^2+y^2 \geq 1}} \frac{1}{(x^2+y^2)^n}\,dx\,dy$ converges. Convert to polar coordinates: $2\pi \int_1^\infty r.r^{-n}\,dr$. Converges iff $\mathrm{Re}(n) > 2$.

So assume $\mathrm{Re}(n) > 2$, and define $\wp'(z, L) = -\frac{1}{2} \sum_{\lambda \in L} \frac{1}{(z-\lambda)^3}$

It is elliptic: $\wp'(z+\lambda, L) = \wp'(z, L)$. It is meromorphic - poles of order 3 at all points of L.

We want to integrate $\wp'(z, L)$. $\wp(z,L) = \int_?^z \wp'(z,L)\,dz$. (Note - residues of all poles of $\wp'$ are 0).

Try $\int_0^z \wp'(z,L)\,dz$. Problem: $\wp' = \infty$ at $z=0$.

So define: $\wp(z,L) = -\frac{1}{2}\int^z \underset{\substack{\uparrow \\ \text{from } \lambda=0}}{\frac{1}{z^3}}\,dz - \frac{1}{2}\sum_{\lambda \neq 0} \int_0^z \frac{1}{(z-\lambda)^3}\,dz = \frac{1}{z^2} + \sum_{\substack{\lambda \in L \\ \lambda \neq 0}} \left(\frac{1}{(z-\lambda)^2} - \underset{\substack{\uparrow \\ \text{this factor makes everything converge well.}}}{\frac{1}{\lambda^2}}\right) \left[\neq \sum_{\lambda \in L} \frac{1}{(z-\lambda)^2}\right]$

Does $\wp(z+\lambda, L) = \wp(z, L)$?

(i) We know $\wp(z+\lambda, L) = \wp(z, L) + c_\lambda$, since $\wp'(z+\lambda, L) = \wp'(z, L)$.

(ii) $\wp(-z, L) = \wp(z, L)$, as $\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2} = \frac{1}{(z-(-\lambda))^2} - \frac{1}{(-\lambda)^2}$

These imply that $\wp(z+\lambda, L) = \wp(z, L)$.

Remark: If we integrate $\wp$ again, we get a function which is not elliptic, as corresponding terms c_λ are no longer 0.

Note also that $\wp(az, aL) = a^{-2}\wp(z, L)$ for $a \in \mathbb{C}^{\times}$. $\wp$ has poles of order 2 at all $\lambda \in L$.

We now construct modular forms. Eg, putting $z=0$. $\wp(0, aL) = a^{-2}\wp(0, L)$. So $\wp(0, aL)$ should correspond to a modular form of weight 2. Problem: $\wp(0, L) = \infty$.
So look at Laurent Series of $\wp(z, L)$, $= \sum_{k \in \mathbb{Z}} z^{k-2}.(k-1)\, G_k(L)$.
$\wp(az, aL) = a^{-2}\wp(z, L)$ implies that this equals $a^2 \sum_{k \in \mathbb{Z}} a^{k-2}.\, z^{k-2}.\, (k-1).\, G_k(aL)$
Compare coefficients of z^{k-2} on both sides: $G_k(L) = a^k\, G_k(aL)$.
$G_k(\tau) = G_k(\langle 1, \tau \rangle)$, so that $G_k\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k.\, G_k(\tau)$.

Work out G_k by finding Laurent series of $\wp(z, L)$ explicitly. $\frac{1}{(z-\lambda)^2} = \frac{1}{\lambda^2} + \frac{2z}{\lambda^3} + \frac{3z^2}{\lambda^4} + \dots$
So $\wp(z, L) = \frac{1}{z^2} + \sum_{\substack{\lambda \in L \\ \lambda \neq 0}} \left(\frac{1}{\lambda^2} + \frac{2z}{\lambda^3} + \frac{3z^2}{\lambda^4} + \dots - \frac{1}{\lambda^2} \right) = \sum_k z^{k-2}.\, (k-1).\, G_k(L)$.

Compare coefficients of z^{k-2}: $G_0(L) = 1$, $G_k(L) = 0$ if k not even, ≥ 0.
$G_2(L) = 0$
$G_4(L) = \sum_{\substack{\lambda \in L \\ \lambda \neq 0}} \frac{1}{\lambda^4}$, $G_k(L) = \sum_{\substack{\lambda \in L \\ \lambda \neq 0}} \frac{1}{\lambda^k}$, k even, $k \geq 4$.

We can show directly that the functions G_k defined by $G_k(\tau) = \sum_{\substack{\lambda \in L \\ \lambda \neq 0}} \frac{1}{\lambda^k}$, $L = \langle 1, \tau \rangle$, are modular forms.
$G_k(\tau) = \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq 0}} \frac{1}{(m\tau+n)^k}$, $(\lambda = m\tau + n)$. $G_k(\tau+1) = \sum_{m,n}' \frac{1}{(m(\tau+1)+n)^k} = \sum' \frac{1}{(m\tau + (m+n))^k} = \sum \frac{1}{(m\tau+n)^k} = G_k(\tau)$.

Similarly, $G_k\left(\frac{-1}{\tau}\right) = \sum_{m,n}' \frac{1}{(m(\frac{-1}{\tau})+n)^k} = \tau^k \sum_{m,n}' \frac{1}{(-m+n\tau)^k}$ (k even), $= \tau^k. \sum_{m,n}' \frac{1}{(m\tau+n)^k} = \tau^k.\, G_k(\tau)$.

Important note: we are using the fact that all series are absolutely convergent, which requires $k > 2$. We later need to use the function $G_2(\tau) = \sum_{(m,n)}' \frac{1}{(m\tau+n)^2}$. Then $G_2\left(\frac{-1}{\tau}\right) \neq \tau^k.\, G_2(\tau)$.

Question: What is the Fourier Series of G_k?
$G_k(\tau+1) = G_k(\tau)$, so put $G_k(\tau) = \sum_n c(n)\, e^{2\pi i n \tau} = \sum c(n)\, q^n$, $q = e^{2\pi i \tau}$. $|q| < 1$ as $\operatorname{Im}\tau > 0$.
What are the $c(n)$'s? $G_k(\tau) = \frac{-(2\pi i)^k B_k}{k!}\left(1 - \frac{2k}{B_k} . \sum_{n \geq 1} \sigma_{k-1}(n)\, q^n\right)$, $\sigma_{k-1}(n) = \sum_{d \mid n} d^{k-1}$.
Usually, write $E_k(\tau) = 1 - \frac{2k}{B_k} . \sum_{n \geq 1} \sigma_{k-1}(n)\, q^n$ - Eisenstein Series.
Write $G_k(\tau) = 2 \sum_{\substack{n \geq 1 \\ (m=0)}} \frac{1}{n^k} + 2 \sum_{m \geq 1} \Big(\underbrace{\sum_{n \in \mathbb{Z}} \frac{1}{(m\tau+n)^k}}_{\text{also periodic in } \tau} \Big)$

Question: What is the Fourier Series of $\sum_{n \in \mathbb{Z}} \frac{1}{(\tau+n)^k}$? - converges for $\operatorname{Re}(k) > 1$.
We want to start with $k = 1$. But $\sum_{n \in \mathbb{Z}} \frac{1}{\tau+n}$ does not converge.
Rewrite it as: $\frac{1}{\tau} + \sum_{n \geq 1} \left(\frac{1}{\tau+n} + \frac{1}{\tau-n} \right) = \frac{1}{\tau} + \sum_{n \geq 1} \left(\frac{2\tau}{\tau^2 - n^2} \right)$. This converges absolutely, so we use it as the definition of $\sum_{n \in \mathbb{Z}} \frac{1}{\tau+n}$. (Alternatively, add terms in order of $|n|$).
Look at the function $f(\tau) = \frac{1}{\tau} + \sum_{n \geq 1} \left(\frac{1}{\tau+n} + \frac{1}{\tau-n} \right)$. What properties does it have?
(i) f has a pole of residue 1 at $\tau =$ integer, and is holomorphic elsewhere.
(ii) $f(\tau+1) = f(\tau)$: Look at $f'(\tau) = -\frac{1}{\tau^2} - \sum_{n \geq 1} \left(\frac{1}{(\tau+n)^2} + \frac{1}{(\tau-n)^2} \right) = -\sum_{n \in \mathbb{Z}} \frac{1}{(\tau-n)^2}$. So $f'(\tau+1) = f'(\tau)$.
(iii) $f(\tau)$ is bounded for $\operatorname{Im}\tau \geq 1$ (see example sheet).
So, (ii) continued: We know that $f(\tau+1) = f(\tau) + \text{constant}$. $f(\tau)$ bounded for $\tau = i + n \Rightarrow \text{constant} = 0$.
(iv) $f(-\tau) = -f(\tau)$ - Trivial.
These four properties characterise $f(\tau)$.
Suppose $f(\tau), g(\tau)$ have same properties. Look at $h(\tau) = f(\tau) - g(\tau)$.

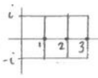
Properties of $h(\tau)$:

(i) $h(\tau)$ is holomorphic for all τ.

(ii) $h(\tau+1) = h(\tau)$

(iii) $|h(\tau)|$ is bounded for $\operatorname{Im}\tau \geqslant 1$

(iv) $h(-\tau) = -h(\tau)$.

Now, (i), (ii) $\Rightarrow$ $h(\tau)$ bounded for $\operatorname{Im}\tau \leq 1$: 

(Bounded for $\operatorname{Im}(\tau) \leq 1$, $\operatorname{Re}(\tau) \leq 1$, as compact, so bounded for all τ with $\operatorname{Im}\tau \leq 1$ by periodicity).

So $h(\tau)$ is a bounded holomorphic function $\Rightarrow$ $h(\tau) = \text{constant}$ (Liouville's Theorem).

(iv) $\Rightarrow$ constant $= 0$. So $h(\tau) = 0$, so $f(\tau) = g(\tau)$.

We evaluate $f(\tau)$ by writing a function with same properties (i) - (iv).

Take $\frac{\pi}{\tan(\pi\tau)}$. $\tan(\tau+\pi) = \tan\tau$, $\tan(-\tau) = -\tan\tau$, $\tan(n\pi) = 0$.

$$\text{So, } \frac{1}{\tau} + \sum_{n\geqslant 1}\left(\frac{1}{\tau+n} + \frac{1}{\tau-n}\right) = \frac{\pi}{\tan(\pi\tau)} = \frac{\pi\cos\pi\tau}{\sin\pi\tau} = \pi i \cdot \frac{e^{\pi i\tau}+e^{-\pi i\tau}}{e^{\pi i\tau}-e^{-\pi i\tau}} = -\pi i\left(\frac{1+e^{2\pi i\tau}}{1-e^{2\pi i\tau}}\right) = -\pi i \cdot \frac{1+q}{1-q} = -2\pi i\left(\frac{1}{2} + \sum_{n\geqslant 1} q^n\right)$$

($|q|<1$ as $\operatorname{Im}\tau > 0$).

Differentiate $\frac{1}{\tau} + \sum_{n\geqslant 1}\left(\frac{1}{\tau+n} + \frac{1}{\tau-n}\right) = -2\pi i\left(\frac{1}{2} + \sum_{n\geqslant 1} q^n\right)$ $(k-1)$ times wrt τ.

Get:
$$\underbrace{\frac{(-1)^{k-1}\cdot(k-1)!}{\tau^k} + (-1)^{k-1}(k-1)!\sum_{n\geqslant 1}\left(\frac{1}{(\tau+n)^k} + \frac{1}{(\tau-n)^k}\right)}_{= \sum_{n\in\mathbb{Z}} \frac{(-1)^{k-1}(k-1)!}{(\tau-n)^k}} = -(2\pi i)^k \sum_{n\geqslant 1} n^{k-1}\cdot q^n$$
$\left(\frac{d}{d\tau} q^n = \frac{d}{d\tau} e^{2\pi i n\tau} = (2\pi i n) q^n\right)$.

$$\text{So, for } k \geqslant 2, \sum_{n\in\mathbb{Z}} \frac{1}{(\tau-n)^k} = \frac{-(2\pi i)^k}{(-1)^{k-1}(k-1)!}\cdot\sum_{n\geqslant 1} n^{k-1}\cdot q^n.$$

Evaluation of $\zeta(k)$: $k \geqslant 2$, even. $\zeta(s) = \sum_{n\geqslant 1}\frac{1}{n^s}$, $\operatorname{Re}(s) > 1$.

Expand identity $\frac{1}{\tau} + \sum_n \frac{2\tau}{\tau^2-n^2} = -2\pi i\left(\frac{1}{2} + \sum_n q^n\right)$ as a Laurent Series in τ (around $\tau = 0$).

$\frac{1}{\tau^2-n^2} = -\frac{1}{n^2} - \frac{\tau^2}{n^4} - \frac{\tau^4}{n^6} - \cdots$, $\frac{1}{2} + \sum_{n\geqslant 1} q^n = -\frac{1}{2} + \frac{1}{1-q} = -\frac{1}{2} + \frac{1}{1-e^{2\pi i\tau}} = -\frac{1}{2} - \frac{1}{2\pi i\tau}\cdot\sum_{n\geqslant 1}\frac{B_n(2\pi i\tau)^n}{n!}$

(Recall: $\frac{t}{e^t-1} = \sum_n \frac{B_n t^n}{n!}$)

$$\text{So } \frac{1}{\tau} + \underbrace{2\tau\sum_{n\geqslant 1}\left(-\frac{1}{n^2} - \frac{\tau^2}{n^4} - \frac{\tau^4}{n^6} - \cdots\right)}_{= 2\tau\left(-\zeta(2) - \tau^2\cdot\zeta(4) - \tau^4\zeta(6) - \cdots\right)} = 2\pi i\left(\frac{1}{2} + \frac{1}{2\pi i\tau}\sum_{n\geqslant 0}\frac{B_n(2\pi i\tau)^n}{n!}\right)$$

Compare coefficients of τ^*: $\zeta(k) = \frac{-(2\pi i)^k B_k}{2(k!)}$, $k \geqslant 2$, even. (k odd not known explicitly).

$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \zeta(2) = \frac{-(2\pi i)^2}{2.2!}\cdot B_2 = \frac{(2\pi)^2}{2.2!}\cdot\frac{1}{6} = \pi^2/6$.

$\frac{1}{1^4} + \frac{1}{2^4} + \frac{1}{3^4} + \cdots = \zeta(4) = \frac{-(2\pi i)^4}{2.4!} B_4 = \pi^4/90$. $(B_4 = 1/30)$.

In particular, $\zeta(k) = \pi^k \times$ rational number (k even, $\geqslant 2$).

Size of B_k: note that $\zeta(k) \approx 1$ for k large. So $|B_k| \approx \frac{2.k!}{(2\pi)^k}$. So B_k decreases for small k, but tends to ∞ rapidly for large k.

$$\text{So } G_k = \sum_m \sum_n{}' \frac{1}{(m\tau+n)^k} = 2\sum_{n\geqslant 1}\frac{1}{n^k} + 2\sum_{m>0}\sum_{n\in\mathbb{Z}}\frac{1}{(m\tau+n)^k}.$$
$$= \frac{-(2\pi i)^k}{k!}B_k + 2\sum_{m>0}\frac{-(2\pi i)^k}{(-1)^{k-1}.(k-1)!}\cdot\sum_{n\geqslant 1} n^{k-1}\cdot q^{mn}$$
$$= \frac{-(2\pi i)^k B_k}{k!}\left(1 - \frac{2k}{B_k}\sum_{m,n\geqslant 1} n^{k-1}\cdot q^{mn}\right)$$
$$= -\frac{(2\pi i)^k B_k}{k!}\left(1 - \frac{2k}{B_k}\sum_{n\geqslant 1}\sigma_{k-1}(n)\cdot q^n\right)$$

$E_k(\tau) =$ constant $\times\, G_k(\tau)$ so that constant term of Taylor Series is 1

$= 1 - \frac{2k}{B_k}\sum_{n\geq 1}\sigma_{k-1}(n)\,q^n.$

$$E_4(\tau) = 1 - \frac{8}{(-1/30)}\sum_{n\geq 1}\sigma_3(n) = 1 + 240q + (240.\underset{\substack{\uparrow\\ 1^3+2^3}}{9})\,q^2 + (240.\underset{\substack{\uparrow\\ 1^3+3^3}}{28})\,q^3 + (240.\underset{\substack{\uparrow\\ 1^3+2^3+4^3}}{73})\,q^4 + \cdots$$

$$E_6(\tau) = 1 - \frac{12}{(1/42)}\sum_{n\geq 1}\sigma_5(n) = 1 - 504q - (504\times \underset{\substack{\uparrow\\ 1^5+2^5}}{33})\,q^2 - \cdots$$

$k=2$: why is $E_2(\tau)$ not a modular form? G_2 is not a coefficient of $\wp(z,L)$.
Proof that $\sum_m\sum_n{}' \frac{1}{(m\tau+n)^2} = \frac{-(2\pi i)^2 B_2}{2!}\left(1 - \frac{2.2}{B_2}\sum\sigma_1(n)q^n\right)$ works fine. What goes wrong with the "elementary" proof that $G_2(\tau) = \sum_m\sum_n{}'\frac{1}{(m\tau+n)^2}$ is a modular form? $G_2(\tau+1) = G_2(\tau)$ is trivial.

But $\frac{1}{\tau^2}G_2\left(\frac{-1}{\tau}\right) \neq G_2(\tau)$.

$'' \quad \frac{1}{\tau^2}\sum_m\sum_n{}'\frac{1}{\left(-\frac{m}{\tau}+n\right)^2} = \sum_n\sum_m \frac{1}{(m\tau+n)^2}.$

But series $\sum_{m,n}{}'\frac{1}{(m\tau+n)^2}$ is not absolutely convergent, and we get different answers depending on whether we sum over m or n first. What is the difference: $\left(\sum_m\sum_n{}' - \sum_n\sum_m{}'\right)\frac{1}{(m\tau+n)^2}$.

Two problems: (i) double sums not absolutely convergent.

(ii) we cannot evaluate them explicitly.

Write $\frac{1}{(m\tau+n)^2} = f(m,n) + g(m,n)$, with (i) $f(m,n)$ so small that $\sum'\sum'|f(m,n)| < \infty$

(ii) $\sum_m\sum_n{}' g(m,n)$, $\sum_n\sum_m{}' g(m,n)$ can be evaluated.

Then, $\left(\sum_m\sum_n{}' - \sum_n\sum_m{}'\right)\frac{1}{(m\tau+n)^2} = \cancel{\sum_m\sum_n{}'} f + \sum_m\sum_n{}' g - \cancel{\sum_n\sum_m{}'} f - \sum_n\sum_m{}' g =$ known.

Try approximating sums by integrals. (Eg: $\sum_{n=1}^m \frac{1}{n}$. $\frac{1}{n} \approx \int_{n-\frac12}^{n+\frac12}\frac{1}{x}dx$, so $\Sigma \sim \sum_{n=1}^m \int_{m-\frac12}^{m+\frac12}\frac{1}{x}dx = \int_{\frac12}^{m+\frac12}\frac{1}{x}dx = \log(m+\frac12) - \log\frac12$)

Let $g(m,n) = \int_{x=m-\frac12}^{m+\frac12}\int_{y=n-\frac12}^{n+\frac12}\frac{1}{(x\tau+y)^2}\,dx\,dy \approx \frac{1}{(m\tau+n)^2}$.

Can check that the difference $f(m,n)$ is small enough so that $\sum\sum'|f(m,n)| < \infty$.

$\left(|f(m,n)| \leq (m^2+n^2)^{-3/2} + \text{const.}\right)$

$\sum_m\sum_n\int_{x=m-\frac12}^{m+\frac12}\int_{y=n-\frac12}^{n+\frac12}\frac{1}{(x\tau+y)^2}\,dx\,dy = \int_x\left(\int_{\substack{y\\ \&(x,y)\in\ |x|,|y|\leq\frac12}}\frac{1}{(x\tau+y)^2}\,dy\right)dx.$ Similarly, $\sum_n\sum_m \to \int_y\left(\int_x \cdots dx\right)dy.$

Integrals are now elementary to do. Get $\sum_m\sum_n{}' * - \sum_n\sum_m{}' * = -\frac{2\pi i}{\tau}$.

So $G_2\left(\frac{-1}{\tau}\right) = \tau^2 G_2(\tau) - 2\pi i\tau$, and $E_2\left(\frac{-1}{\tau}\right) = \tau^2 E_2(\tau) + \frac{12\tau}{2\pi i}$.

Put $\Delta(\tau) = q\prod_{n\geq 1}(1-q^n)^{24} = q - 24q^2 + \cdots$ (Dedekind Δ function)

Theorem: $\Delta(\tau)$ is a modular form of weight 12 with no zeroes in H,

Proof: $\Delta(\tau+1) = \Delta(\tau)$ is trivial. ∞ product for Δ converges for $|q|<1$ ($\operatorname{Im}\tau > 0$).

(Look at $\log\prod_{n\geq 1}(1-q^n)^{24} = \sum_{n\geq 1}24\log(1-q^n)$. $\log(1-q^n) = -q^n - \frac{q^{2n}}{2} - \cdots \approx -q^n$. $\sum_{n\geq 1}24q^n$ converges for $|q|<1$)

Series for $\log\Delta$ converges on H, so $\Delta = \exp(\log\Delta)$ has no zeroes in H.

$\Delta\left(-\frac{1}{\tau}\right) = \tau^{12}.\Delta(\tau)$: $\frac{d}{d\tau}(\log\Delta(\tau)) = \frac{d}{d\tau}\left(\log q + 24\sum_{n\geq 1}\log(1-q^n)\right)$, $\quad q = e^{2\pi i\tau}$, $\frac{d}{d\tau}q^n = 2\pi i n q^n$

$= \frac{d}{d\tau}\left(\log q - 24\sum_{n\geq 1}\sum_{m\geq 1}\frac{q^{nm}}{m}\right) \qquad \frac{d}{d\tau}\log q = 2\pi i.$

$= 2\pi i - 2\pi i.24\sum_{m,n\geq 1} n q^{nm} = 2\pi i\left(1 - 24\sum_{n\geq 1}\sigma_1(n)q^n\right) = 2\pi i E_2(\tau).$

So $\frac{d}{d\tau}\left(\log\Delta\left(\frac{-1}{\tau}\right)\right) = 12\tau + \tau^2.\frac{d}{d\tau}\log\Delta(\tau)$

This implies that $\Delta\left(\frac{-1}{\tau}\right) =$ constant $\times\,\tau^{12}\times\Delta(\tau)$.

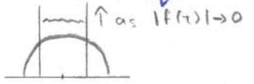
Put $\tau = i$. $\Delta(i) =$ const. $\times\, i^{12}\times\Delta(i)$, $\Delta(i) \neq 0$, so constant $= 1$. So $\Delta\left(\frac{-1}{\tau}\right) = \tau^{12}\Delta(\tau)$.

Theorem: Every modular form is a polynomial in $E_4(\tau)$, $E_6(\tau)$. (E_4, E_6 algebraically independent).

We need the following properties: (i) E_4 is a modular form of weight 4. $E_4(\tau) = 1 + 240q + \cdots$
(ii) E_6 is a modular form of weight 6. $E_6(\tau) = 1 - 504q + \cdots$
(iii) Δ is a modular form of weight 12. $\Delta(\tau) = q + \cdots$, $\Delta(\tau) \neq 0 \ \forall \tau \in H$.

Step 0: There are no modular forms of odd weight. Look at $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in SL_2\mathbb{Z}$. $f\left(\frac{-\tau}{-1}\right) = (-1)^k f(\tau)$.
So for k odd, $f(\tau) = -f(\tau) \Rightarrow f \equiv 0$.

Step1: Any modular form of weight 0 is constant. Such an f is a modular function, holomorphic on H and at $i\infty$. $f(\tau) = c(0) + c(1)q + \cdots$ Replace $f(\tau)$ by $f(\tau) - c(0)$. Note that $f(\tau)$ is bounded for $\operatorname{Im}\tau \geq \frac{1}{2}$, say, and $|f(\tau)| \to 0$ as $\operatorname{Im}\tau \to \infty$ ($|q| \to 0$)
Look at fundamental domain of $SL_2(\mathbb{Z})$.



So $f(\tau)$ is bounded.

This implies that $f(\tau)$ achieves a maximum value somewhere in the fundamental domain F. $f(\tau)$, for any $\tau \in H$, is given by some $f(\tau)$ for $\tau \in F$. So $f(\tau)$ achieves its maximum at some point of open set H. By maximum modulus principle, $f(\tau)$ is constant.
So any modular form of weight 0 is constant.

Step2: $E_4(\omega) = 0$, $E_6(i) = 0$, where $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ ($\omega^3 = 1$).
For E_6, look at $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z})$. $\tau \mapsto -\frac{1}{\tau}$, fixes i. $E_6\left(\frac{-1}{\tau}\right) = \tau^6 E(\tau)$, so $E_6(i) = -E_6(i)$.
For E_4, use $\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} : \tau \to \frac{-\tau-1}{\tau}$, fixing ω. Proof similar.
(Any modular form of weight not divisible by $\left\{\begin{matrix} 6 \\ 4 \end{matrix}\right\}$ vanishes at $\left\{\begin{matrix} \omega \\ i \end{matrix}\right\}$).

Step3: For any even $k \geq 4$, we can find a modular form of weight k of form $1 + \cdots$, given by $(E_4)^{k/4}$ or $E_6 E_4^{(k-6)/4}$.

Step4: No forms of weight k, even ≤ -4.
Eg: weight -4. If f has weight -4, then $E_4 . f$ has weight 0, so is constant, and vanishes at ω, so is 0. For weights $-6, -8, \ldots$, use E_4^* or $E_6 E_4^*$.

Step5: If f has weight -2, then f^2 has weight -4. So none have weight -2.

Summary: any form of weight ≤ 0 has weight 0 and is constant.

Step6: If f is a form of weight k, even, ≥ 4, then $f = \text{constant}. E_4^* + \Delta g$, or $\text{constant}\, E_6 E_4^* + \Delta g$, where g is a form of weight $k-12$.

Proof: Subtract a constant $\times E_4^* \{E_6\}$ to make constant term 0. So can assume $f(\tau) = c(1)q + c(2)q^2 + \cdots$
Now look at $\frac{f(\tau)}{\Delta(\tau)} = c(1) + *q + *q^2 + \cdots$ So $\frac{f(\tau)}{\Delta(\tau)}$ is holomorphic at $i\infty$, and holomorphic on H, as $\Delta \neq 0$. So $\frac{f(\tau)}{\Delta(\tau)}$ is a modular form of weight $\operatorname{wt} f - \operatorname{wt} \Delta = k - 12$.

Step7: Modular forms of weight 4: any such $f = \text{constant} \times E_4 + \Delta g$, g of weight $4 - 12 = -8$, so $g = 0$.
So $f = \text{constant} \times E_4$. For weights 6, 8, 10 same argument shows such a form is E_6, E_4^2, $E_6 E_4$.

Step 8: Fill in gap about weight 2. Suppose f has weight 2. Then f^2 has weight 4, so is const. $\times E_4$ = const. $(1+240q+\cdots) \Rightarrow f=$ const. $(1+120q+\cdots)$. Similarly, $f^3=$ const. $\times E_6$ = const. $(1-504q+\cdots) \Rightarrow f=$ const. $(1-168q+\cdots)$ - Inconsistent, so no forms of weight 2.

Step 9: Δ is a polynomial in E_4, E_6. By step 6, $E_6^2=$ const. $\times E_4^3 + \Delta g$, g of weight $12-12=0$, so g constant. So $E_6^2 = aE_4^3 + b\Delta$. Now, $E_6^2 = (1-504q+\cdots)^2 = 1-1008q+\cdots$,
$E_4^3 = (1+240q+\cdots)^3 = 1+720q+\cdots$, $\Delta = q-24q^2+\cdots$
Look at constant term: $a=1$. Coefficients of q: $720 = -1008+b \Rightarrow b=1728$.
So $E_4^3 - E_6^2 = 1728\Delta$.

Step 10: Proof that any modular form = polynomial in E_4, E_6 - by induction on weight.
We have proved this for weights $\leqslant 10$. Now look at weight k, even $\geqslant 10$.
Let f be a modular form of weight k. $f=$ const. $E_4^* + \Delta g$, or $f=$ const. $E_6E_4^* + \Delta g$.
g has weight $k-12$, so is a polynomial in E_4, E_6 by induction.
Δ is a polynomial by step 9. So f is a polynomial in E_4, E_6.

Step 11: There are no polynomial relations between E_4, E_6 (see example sheet 3).

So, ring of modular forms = ring of polynomials in two variables E_4, E_6.

Applications: In particular, all the Eisenstein Series $E_8, E_{10}, E_{12}, \ldots$, are polynomials in E_4, E_6.
Eg: E_8 has weight 8. Only monomial in E_4, E_6 of weight 8 is E_4^2. So $E_8=$ const. $\times E_4^2$, so $E_8 = E_4^2$ (compare constant terms). Similarly, $E_{10} = E_4E_6$, $E_{14} = E_4^2E_6$, as E_4E_6, $E_4^2E_6$ are the only monomials of weights 10, 14.

$E_{12} \neq E_4^3$ or E_6^2. (There are two monomials in E_4, E_6 of weight 12). We can write E_{12} as a linear combination of E_4^3, E_6^2, or of E_4^3 and Δ.

$E_{12}(\tau) = 1 - \frac{2\times 12}{B_{12}} \cdot \sum_{n\geqslant 1} \sigma_{11}(n)q^n$, $B_{12} = \frac{-691}{2730}$. Recall: $E_4^3 = 1+720q+\cdots$

$= 1+\frac{65520}{691}\sum\sigma_{11}(n)q^n$ $\qquad\qquad$ $\Delta = q+\cdots = \sum\tau(n)q^n$.

Put $E_{12} = aE_4^3 + b\Delta$. Look at constant terms: $a=1$.
Look at coefficients of q: $b = \frac{65520}{691} - 720$.
So $1+\frac{65520}{691}\sum\sigma_{11}(n)q^n =$ (something with integral coefficients) $+ \frac{65520}{691}\cdot\Delta$.

$E_4^3 \,'' - 720$

So $65520\sum\sigma_{11}(n)q^n = 691(\text{integral}) + 65520\Delta$. 65520 is coprime to 691.
So $65520\left(\sum\sigma_{11}(n)q^n - \sum\tau(n)q^n\right) \equiv 0 \mod 691$. So $\sigma_{11}(n) \equiv \tau(n) \mod 691$ (Ramanujan).

Now we will classify all modular functions $f(\tau)$ (f such that $f\left(\frac{a\tau+b}{c\tau+d}\right) = f(\tau)$ - weight 0, f meromorphic on H and at $i\infty$ - ie $f = \sum c(n)q^n$, $c(n)=0$ for $n \ll 0$).
Recall that if f, g are modular forms of the same weight, then $\frac{f}{g}$ is a modular function. ($g \not\equiv 0$)
We need a space of modular forms of weight k of dimension $\geqslant 2$. Dimensions of spaces of modular forms:

$k=$	0	2	4	6	8	10	12	
	1	-	E_4	E_6	E_4^2	E_4E_6	E_4^3, E_6^2	- so take $k=12$ as simplest case.

So we choose two modular forms f, g of weight 12. Take $g = \Delta$ (no zeroes on H), so f/g is holomorphic on H. Take $f = E_4^3$ (for historical reasons). Define $j(\tau) = \frac{E_4^3(\tau)}{\Delta(\tau)}$ - modular function, no zeroes on H, pole of order 1 at $i\infty$ (ie, at $q=0$).

(If we change f to $aE_4^3 + b\Delta$, then $\frac{f}{\Delta}$ becomes $aj+b$, which differs only trivially from j).

$$j(\tau) = \frac{(1+240q+2160q^2+\dots)^3}{q-24q^2+252q^3+\dots} = q^{-1} + \underbrace{744}_{} + 196884q + \cdots$$

└ arbitrary, as we can add constants.

Any rational function of $j(\tau)$ is (obviously) a modular function. Conversely, any modular function is a rational function of $j(\tau)$. We will prove this by showing that any modular function is a quotient of two modular forms. Suppose f is a modular function. We try to find a product g of modular forms so that fg has no poles on H or at $i\infty$, so that fg is a modular form.

Lemma: For any $\tau_0 \in H$ (or $\tau_0 = i\infty$), there is some non-zero linear combination of E_4^3, E_6^2 vanishing at τ_0.

Proof: $E_4(\tau), E_6(\tau)$ cannot both vanish for $\tau_0 \in H$, since $E_4^3(\tau_0) - E_6^2(\tau_0) = 1728\Delta(\tau_0)$ is non-zero. But then $E_4^3(\tau_0)E_6^2(\tau) - E_4^3(\tau)E_6^2(\tau_0)$ is a non-zero modular form vanishing at $\tau = \tau_0$. (For $\tau = i\infty$, $E_4^3 - E_6^2$ vanishes).

Suppose f is a modular function with pole of order n at τ_0. Multiply it by $(h(\tau))^n$, where $h(\tau)$ is a modular form vanishing at τ_0. This kills off the pole of f at τ_0. By repeating this, can kill all poles. So $f \times$ (some product of modular forms) has no poles, so is a modular form. So any modular function is a quotient of two modular forms.

So if f is a modular function, then $f(\tau) = \frac{\text{modular form of weight } k}{\text{modular form of weight } k}$ (some k, $12 | k$).

$= \frac{\text{poly. in } E_4, E_6, \text{ weight } k}{\text{poly. in } E_4, E_6, \text{ weight } k}$ (Polynomial in E_4, E_6 of weight $k = * E_4^{k/4} + * E_4^{\frac{k-12}{4}} \cdot E_6^2 + \dots + * E_6^{k/6}$

$= \text{polynomial in } (E_4^3/E_6^2) \times E_6^{k/6}$

$= \frac{\text{poly in } (E_4^3/E_6^2) \times \cancel{E_6^{k/6}}}{\text{poly. in } (E_4^3/E_6^2) \times \cancel{E_6^{k/6}}}$ = rational function of E_4^3/E_6^2.

Now, $\frac{1728}{j(\tau)} = \frac{E_4^3 - E_6^2}{E_4^3} = 1 - E_6^2/E_4^3$. So f = rational function of $j(\tau)$.

So any modular function is a rational function in $j(\tau)$. (easy to check that no polynomial in j is 0)

So, ring of modular functions $\cong$ ring of rational functions in one variable.

Summary.

1. Eisenstein Series: $E_k = 1 - \frac{2k}{B_k} \cdot \sum_{n \geq 1} \sigma_{k-1}(n) q^n$ are modular forms of weight k. (k even, ≥ 4).
2. $\Delta(\tau) = q \cdot \prod (1-q^n)^{24}$ is a modular form of weight 12, with no zeroes on H. ($1728\Delta = E_4^3 - E_6^2$)
3. Any modular form is a polynomial in E_4, E_6.
4. Modular functions are rational functions of $j(\tau) = \frac{E_4^3(\tau)}{\Delta(\tau)}$

Application - Theta Functions of Lattices.

Example: E_8 Lattice. Construction: Lattice I^n = set of all points $(x_1, \dots, x_n)$ in $\mathbb{R}^n$ with all $x_i \in \mathbb{Z}$. Trivial that $(\lambda, \mu) \in \mathbb{Z}$ for $\lambda, \mu \in I^n$, so I^n is an integral lattice. Put L = vectors of I^n with $\sum x_i$ even. So L has index 2 in I^n. Now look at lattice generated by L and $v = (\frac{1}{2}, \dots, \frac{1}{2})$. v has integral inner product with all vectors in L. When is (v,v) integral? $(v,v) = n/4$, so $(v,v) \in \mathbb{Z}$ if $4 | n$. If $(v,v) \in \mathbb{Z}$, $(v, \lambda) \in \mathbb{Z}$ for $\lambda \in L$, then v and L generate an integral lattice. If $2 | n$ then (λ, λ) is even. If $8 | n$ then $(v,v) = \frac{n}{4}$ is also even.

If $8|n$ then every vector in the lattice generated by v and L is even:

$(mv+\lambda, mv+\lambda) = m^2(v,v) + 2m(v,\lambda) + (\lambda,\lambda) = $ even.

A lattice is called even if (v,v) is even for all vectors v.

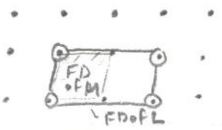
A lattice is unimodular if the volume of a fundamental domain is 1.

Example: Set of all points $D = x_1v_1 + \dots + x_nv_n$ where $v_1,\dots,v_n$ is some fixed basis of L, $0 \le x_i < 1$

Every point of $\mathbb{R}^n$ can be written as (something in L) + (something in D)

I^n is unimodular: Let $v_i = (0,\dots,1,\dots 0)$. So D = unit hypercube, volume $=1$.

Note that if $L \subseteq M$ are two lattices with L index n in M, then volume of fundamental domain of $L = 2\times$ (that of M) :



Let E_8 = lattice generated by L and $(\frac12,\dots,\frac12)$ in $\mathbb{R}^8$. We have:

$$\begin{tikzcd} \overset{V(FD)=1}{I^8} & & E_8 \quad \therefore V(FD)=\tfrac12\cdot 2=1. \\ & L \therefore V(FD)=2\cdot 1=2 \arrow[ul, dash, "\text{index }2"] \arrow[ur, dash, "\text{index }2"'] & \end{tikzcd}$$

So E_8 is unimodular and even. (And we can also find even unimodular lattices in any dimension divisible by 8. We will see later that such lattices exist only in $\mathbb{R}^n$ for $8|n$).

Aim: we want to show the theta function $\theta_{E_8}(\tau) = \sum_{\lambda\in E_8} e^{2\pi i(\lambda^2/2)\tau} = \sum_{n\in\mathbb{Z}} c(n)q^n$, where $c(n)$ is the number of vectors of norm $2n$, is a modular form of weight 4.

So we want to show:

(i) $\theta_{E_8}(\tau+1) = \theta_{E_8}(\tau)$. - follows from $\frac{\lambda^2}{2}$ being an integer. (as E_8 is even).

(ii) $\theta_{E_8}(-1/\tau) = \tau^4\theta_{E_8}(\tau)$. We will deduce this from the fact that E_8 is a unimodular lattice.

We work out the first few coefficients $c(n)$ of $\theta_{E_8}(\tau)$. $c(0)=1$, as E_8 has only one vector of norm 0. $c(1)$ = number of vectors of norm 2.

Vectors of E_8 are either $(n_1,\dots,n_8)$ or $(n_1+\frac12,\dots,n_8+\frac12)$ with $n_i \in \mathbb{Z}$, $\sum n_i$ even.

Try $n_1^2+\dots+n_8^2 = 2$. Only solutions are: $n_i = \pm1$, $n_j = \pm1$, all other $n_k = 0$. $\# = \frac{8\times7}{2}\times 2^2 = 28\times 4 = 112$

For $(n_1+\frac12,\dots,n_8+\frac12)$, minimum value is 2, when all coefficients are $\pm\frac12$. $\# = 2^8\times\frac12 = 128$.

So, number of norm 2 vectors $= 112 + 128 = 240$.

$c(2)$: count vectors of norm 4:

$$\left.\begin{array}{ll} \text{(i) } (0,\dots,\pm2,\dots,0) & \# = 8\times 2 = 16. \\ \text{(ii) } (0,\dots\pm1,\dots\pm1,\dots\pm1,\dots\pm1,\dots). & \# = \binom{8}{4}\times 2^4 = 1120 \\ \text{(iii) } (\pm\frac12,\dots,\pm\frac32,\dots,\pm\frac12). & \# = 2^8\times 8\times\frac12 = 1024 \end{array}\right\} \text{ So } c(2) = 2160.$$

So $\theta_{E_8}(\tau) = 1 + 240q + 2160q^2 + \dots$ (cf: $E_4(\tau)$).

We should check that $\theta_{E_8}(\tau)$ is holomorphic. It is holomorphic at $i\infty$ as θ_{E_8} has no terms in q^n for $n<0$. Holomorphic on H: want to show $\sum c(n)q^n$ converges for $|q|<1$.

$c(n) \le$ const. n^8. (If a vector v has norm $\le C$ then all coordinates must be at most C, so the number of possibilities is at most $(4C+1)^8 \le$ polynomial in C).

So $c(n) \le$ polynomial in n, so $\sum c(n)q^n$ converges for $|q|<1$

Review of Fourier Series and Fourier Transforms.

Suppose f is a function on $\mathbb{R}$ with $f(x) = f(x+1)$. (Assume integrable on $[0,1]$). Fourier Series of f is $\sum_n c(n)\, e^{2\pi i n x}$, where $c(n) = \int_0^1 e^{-2\pi i n x} f(x)\,dx$. When does the Fourier Series of f converge to f? It does whenever f is continuous and has a continuous derivative.

Suppose f is a function on $\mathbb{R}^n$ with $f(x+\lambda) = f(x)$ whenever $\lambda \in \mathbb{Z}^n$. Then $f(x) = \sum_{n \in \mathbb{Z}^n} c(n)\, e^{2\pi i (n,x)}$, where $c(n) = \int_0^1 \cdots \int_0^1 e^{-2\pi i (n,x)} f(x)\, d^n x$. This converges to f if f is continuous and has continuous partial derivatives.

Suppose f is a function on $\mathbb{R}$. (Assume all derivatives of f are rapidly decreasing, ie, product with any polynomial is bounded). The Fourier Transform is defined by $\hat{f}(y) = \int_{-\infty}^{\infty} e^{2\pi i x y} f(x)\,dx$.
Then $f(x) = \int_{-\infty}^{\infty} e^{-2\pi i x y} \hat{f}(y)\,dy$ - Inversion formula for Fourier Transforms.
(We will prove it explicitly for cases we need).
For n variables $\hat{f}(y) = \int_{-\infty}^{\infty} \cdots \int_{-\infty}^{\infty} e^{2\pi i (x,y)} f(x)\, d^n x$. $\hat{\hat{f}}(x) = f(-x)$.

Suppose V is any finite dimensional vector space over $\mathbb{R}$. Suppose f is a "nice" function on V. We want to define $\hat{f}(y)$ by $\int_{x \in V} e^{2\pi i (x,y)} f(x)\, d^n x$. To make this well-defined, we need:
(i) a volume element on V.
(ii) $y \in \mathrm{Hom}(V, \mathbb{R})$ so that (x,y) is well-defined.

So Fourier Transform takes functions on vector space V to functions on dual vector space V^*. Similarly, suppose we take L to be any lattice (= discrete free abelian subgroup of V, rank = dim V). Look at functions f on V with $f(x+\lambda) = f(x)$ for $\lambda \in L$.
Then $f(x) = \sum_{\mu \in L^*} e^{2\pi i (\mu, x)} c(\mu)$, $c(\mu) = \int_{V/L} f(x)\, e^{-2\pi i (\mu,x)}\, d^n(x)$. (Abstract form of Fourier Series in n variables. L^* = vectors in V^* which have integral inner product with all $\lambda \in L$)

Choose volume on V so that $\mathrm{vol}(V/L) = 1$. (For any isomorphism from $\mathbb{R}^n$ to V we get a volume on V. Volumes on V for different isomorphisms differ only by constant factors, so volume on V is well-defined up to a constant. Setting $\mathrm{vol}(V/L) = 1$ fixes constant.)
Fourier Transform of a function f on V is $\hat{f}(y) = \int_V e^{2\pi i (x,y)} f(x)\, d^n x$.
Fourier Series of f (if $f(x+\lambda) = f(x)$ for $\lambda \in L$) is $f(x) = \sum c(\mu)\, e^{2\pi i (x,\mu)}$, $c(\mu) = \int_{V/L} f(x)\, e^{-2\pi i (x,\mu)}\, dx$.

Poisson Summation Formula: Suppose f is "nice". Then $\sum_{\lambda \in L} f(\lambda) = \sum_{\mu \in L^*} \hat{f}(\mu)$.
Proof: Look at $g(x) = \sum_{\lambda \in L} f(x+\lambda)$. Then $g(x) = g(x+\lambda)$. Look at Fourier Series of $g(x) = \sum c(\mu)\, e^{2\pi i (x,\mu)}$,

$$c(\mu) = \int_{V/L} e^{-2\pi i (x,\mu)} g(x)\,dx = \int_{V/L} e^{-2\pi i (x,\mu)} \sum_{\lambda \in L} f(x+\lambda)\,dx = \int_V e^{-2\pi i (x,\mu)} f(x)\,dx = \hat{f}(-\mu)$$

$$\text{So } \sum_{\lambda \in L} f(\lambda) = g(0) = \sum c(\mu)\, e^{2\pi i (0,\mu)} = \sum c(\mu) = \sum_{\mu \in L^*} \hat{f}(\mu).$$

Remark: Everything about Fourier transforms, Poisson formula, etc. can be generalised to the following case:

V = any locally compact abelian group, V^* = dual group = continuous homomorphisms $V \to U(1) = \{z \in \mathbb{C} : |z| = 1\}$.
L = any closed subgroup of V, L^* = elements of V^* whose value on L is always 1.
If $V = \mathbb{R}^n$, then $V^* \cong$ dual of V, as if f is a linear map $\mathbb{R}^n \to \mathbb{R}$, then $v \mapsto e^{2\pi i f(x)}$ is in the dual group of $\mathbb{R}^n$.

$V = \mathbb{R}^n$, $V^* = \mathbb{R}^n \Rightarrow$ Fourier Transforms.

$V = S^1 = \mathbb{R}/\mathbb{Z}$, $V^* = \mathbb{Z} \Rightarrow$ Fourier Series.

$V =$ ring of adeles, used in algebraic number theory.

Example: Take V to be some Euclidean space with $(\,,\,)$. Take $f(x) = e^{2\pi i (x^2/2)\tau}$.

Then $\sum_{\lambda \in L} f(\lambda) = \sum_{\lambda \in L} e^{2\pi i (\lambda^2/2)\tau} = \theta_L(\tau)$. This is $\sum_{\lambda \in L^*} \hat{f}(\lambda)$, by Poisson summation.

So we need to know Fourier Transform of $e^{2\pi i (\lambda^2/2)\tau}$.

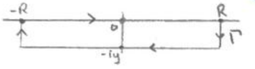
Step1: $I = \int_{\mathbb{R}} e^{-\pi x^2} dx = 1$.

$I^2 = \int_{\mathbb{R}}\int_{\mathbb{R}} e^{-\pi x^2} e^{-\pi y^2} dx\,dy = \int_{\mathbb{R}^2} e^{-\pi(x^2+y^2)} dx\,dy$. Change to polar coordinates:

$x = r\cos\theta$, $y = r\sin\theta$, so $dx\,dy = r\,dr\,d\theta$. So $I^2 = \int_{r=0}^{\infty}\int_{\theta=0}^{2\pi} e^{-\pi r^2} r\,dr\,d\theta = 2\pi \int_0^{\infty} re^{-\pi r^2} dr = 2\pi \cdot \frac{1}{2\pi} = 1$.

Step2: Fourier transform of $e^{-\pi x^2}$ is $e^{-\pi y^2}$.

We must evaluate $\int_{\mathbb{R}} e^{-\pi x^2} \cdot e^{2\pi i x y} dx = \int_{\mathbb{R}} e^{-\pi(x-iy)^2} \cdot e^{-\pi y^2} dx = e^{-\pi y^2} \int_{\mathbb{R}-iy} e^{-\pi x^2} dx \quad -(*)$.



By Cauchy, $\int_{\Gamma} e^{-\pi x^2} dx = 0$. As $R \to \infty$, short edge integrals $\to 0$.

So $\int_{-\infty}^{\infty} e^{-\pi x^2} dx = \int_{-\infty - iy}^{\infty - iy} e^{-\pi x^2} dx$.

So $(*) = e^{-\pi y^2}$

Step3: Fourier transform of $e^{-\pi a x^2}$ is $\frac{1}{\sqrt{a}} e^{-\pi y^2/a}$ (a real, or $\mathrm{Re}(a) > 0$).

$\int e^{-\pi a x^2} e^{2\pi i x y} dx = \int e^{-\pi x^2} \cdot e^{2\pi i x (y/\sqrt{a})} \cdot \frac{dx}{\sqrt{a}} = \frac{e^{-\pi(y/\sqrt{a})^2}}{\sqrt{a}}$

(If a not real, need to change contour using Cauchy's Theorem, as before)

Step4: F.T. on $\mathbb{R}^n$ of $e^{-\pi a x^2} = e^{-\pi a x_1^2} \cdot e^{-\pi a x_2^2} \cdots$ is: $\int_{\mathbb{R}^n} e^{-\pi a x_1^2} e^{2\pi i x_1 y_1} \cdot e^{-\pi a x_2^2} e^{2\pi i x_2 y_2} \cdots dx_1\,dx_2 \cdots$

$= \int_{\mathbb{R}} e^{-\pi a x_1^2} e^{2\pi i x_1 y_1} dx_1 \times \int_{\mathbb{R}} e^{-\pi a x_2^2} e^{2\pi i x_2 y_2} dx_2 \times \cdots = \frac{1}{\sqrt{a}} e^{-\pi y_1^2/a} \times \frac{1}{\sqrt{a}} e^{-\pi y_2^2/a} \times \cdots = a^{-\frac{n}{2}} \cdot e^{-\pi y^2/a}$

Step5: Put $a = \tau/i$. $(\mathrm{Im}\,\tau > 0)$. F.T. of $e^{2\pi i \tau (x^2/2)}$ on $\mathbb{R}^n$ is $\left(\frac{\tau}{i}\right)^{-n/2} \cdot e^{2\pi i (-\frac{1}{\tau})(x^2/2)}$

Insert into Poisson summation formula. $L =$ any lattice in $\mathbb{R}^n$ with $\mathrm{vol}(\mathbb{R}^n/L) = 1$.

$\sum_{\lambda \in L} e^{2\pi i (\lambda^2/2)} = \left(\frac{\tau}{i}\right)^{-n/2} \cdot \sum_{\lambda \in L^*} e^{2\pi i (-1/\tau) \lambda^2/2}$. So $\theta_L(\tau) = \left(\frac{\tau}{i}\right)^{-n/2} \theta_{L^*}(-1/\tau)$.

Suppose $L = L^*$. Then $\theta_L\left(\frac{-1}{\tau}\right) = \left(\frac{\tau}{i}\right)^{n/2} \theta_L(\tau)$

Example: E_8. $\mathrm{Vol}(\mathbb{R}^n/L) = 1$. $E_8^* = E_8$: Have

$$\begin{tikzcd}
 & \mathbb{Z}^8 + \left(\left(\tfrac{1}{2}\right)^8 + \mathbb{Z}^8\right) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Z}^{8*} = \mathbb{Z}^8 \arrow[dr, dash] & & E_8 = E_8^* \arrow[dl, dash] \\
 & L &
\end{tikzcd}$$

So $\theta_{E_8}\left(\frac{-1}{\tau}\right) = \left(\frac{\tau}{i}\right)^{8/2} \theta_{E_8}(\tau) = \tau^4 \theta_{E_8}(\tau)$

As $\theta_{E_8}(\tau+1) = \theta_{E_8}(\tau)$, we see that $\theta_{E_8}(\tau)$ is a modular form of weight 4.

More generally, if L is any self-dual lattice (with $\mathrm{vol}(\mathbb{R}^n/L) = 1$), even, then $\theta_L(\tau)$ is a modular form of weight $n/2$. ($\mathrm{vol} = 1$ follows from L being self-dual).

Theorem: If L is even, self-dual lattice (with $\mathrm{vol}(\mathbb{R}^n/L) = 1$) then $8 | n$.

Proof: We know $\theta_L(\tau+1) = \theta_L(\tau)$ via $T: \tau \mapsto \tau+1$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, and $\theta_L\left(\frac{-1}{\tau}\right) = \left(\frac{\tau}{i}\right)^{n/2} \theta_L(\tau)$, via $S: \tau \mapsto -\frac{1}{\tau}$, $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Relations between S, T and $Z = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$: $S^2 = Z$, $Z^2 = 1$, $(ST)^3 = Z$. $Z \in$ centre.

(This is in fact a presentation for $SL_2(\mathbb{Z})$). So $\vartheta_L((ST)^3(\tau)) = \vartheta_L(\tau)$.

Calculate $\vartheta_L((ST)^3(\tau))$.

$$\begin{aligned}
T:&\ \vartheta_L(\tau+1) = \vartheta_L(\tau).\\
S:&\ \vartheta_L\left(\tfrac{-1}{\tau+1}\right) = \left(\tfrac{\tau+1}{i}\right)^{n/2}\vartheta_L(\tau)\\
T:&\ \vartheta_L\left(\tfrac{\tau}{\tau+1}\right) = \left(\tfrac{\tau+1}{i}\right)^{n/2}\vartheta_L(\tau)\\
S:&\ \vartheta_L\left(\tfrac{-\tau-1}{\tau}\right) = \left(\tfrac{\tau}{(\tau+1)i}\right)^{n/2}\cdot\left(\tfrac{\tau+1}{i}\right)^{n/2}\vartheta_L(\tau)\\
T:&\ \vartheta_L\left(\tfrac{-1}{\tau}\right) = \text{same, and also equals } \left(\tfrac{\tau}{i}\right)^{n/2}\vartheta_L(\tau).
\end{aligned}$$

So need $\left(\frac{\tau}{(\tau+1)i}\right)^{n/2}\cdot\left(\frac{\tau+1}{i}\right)^{n/2} = \left(\frac{\tau}{i}\right)^{n/2}$, so $i^{n/2} = 1$, so $8 \mid n$. (assuming $\vartheta_L(\tau) \not\equiv 0$).

Suppose L is self-dual but not even, eg $L = \mathbb{Z}^n$. Then $\vartheta_L(\tau+2) = \vartheta_L(\tau)$, as $e^{2\pi i\tau(\lambda^2/2)} = e^{2\pi i(\tau+2)(\lambda^2/2)}$ if $\lambda^2 \in \mathbb{Z}$, and $\vartheta_L(\frac{-1}{\tau}) = (\frac{\tau}{i})^{n/2}\vartheta_L(\tau)$ as before

The matrices $\{\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}1&2\\0&1\end{smallmatrix}\right)\}$ generate group $\Gamma(2) \cup \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)\Gamma(2)$, $\Gamma(2) = \{\text{matrices } \left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right) \equiv \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \bmod 2\}$. $\Gamma(2)$ has index 6 in $SL_2(\mathbb{Z})$. "ϑ_L is a modular form at level >1".

Let $\vartheta(\tau) = 1 + 2q + 2q^4 + \cdots = \sum_n q^{n^2}$. Very rapidly convergent. For example, calculate $\vartheta(\frac{i}{100})$ to 100 significant figures. $q = e^{-2\pi/100} \simeq 0.94$. Use functional equation: $\vartheta(\frac{i}{100}) = (100)^{1/2}\vartheta(100i)$ $= 10(1 + 2e^{-2\pi\times 100} + \cdots) = 10.0\cdots0$. For τ imaginary, $\tau \to 0$, see that $\vartheta(\tau) \sim (\frac{\tau}{i})^{1/2}$

Suppose L is any self-dual even lattice in 8 dimensions. $\vartheta_L(\tau)$ is a modular form of weight 4, so is a multiple of E_4. Constant term of $\vartheta_L(\tau)$ is 1 [$\exists$ 1 vector of norm 0].

So $\vartheta_L(\tau) = E_4(\tau) = 1 + 240q + 2160q^2 + \cdots$

Eg: how many norm 100 vectors does E_8 have? = coefficient of q^{50} in $E_4(\tau) = 1 + 240\sum\sigma_3(n)q^n$,
$= 240 \times \sigma_3(50) = 240(1+2^3)(1+5^3+5^{25})$.

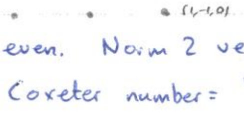
We now show that E_8 is the only lattice in dimension 8 which is even and self-dual. E_8 has dimension 8, is even, and has 240 vectors of norm 2. We classify all lattices generated by vectors of norm 2. Answer: such is an orthogonal direct sum of following lattices:

(i) A_n = vectors $(m_1, \ldots, m_{n+1}) \in \mathbb{Z}^{n+1}$ with $\sum m_i = 0$. Norm 2 vectors: $(0, \ldots, \pm1, \ldots 0, \ldots, \mp1, \ldots, 0)$.

$\#$ norm 2 vectors $= \binom{n+1}{2} \times 2 = n(n+1)$. Coxeter number $= \frac{\#\text{ roots}}{\text{dimension}} = n+1$.

A_1 = vectors $(m, -m) \in \mathbb{Z}^2$ = one-dimensional lattice $\mathbb{Z}$ generated by element v with $(v,v) = 2$.

A_2 = vectors (a, b, c) with $a+b+c = 0$.



(ii) D_n = all vectors $(m_1, \ldots, m_n) \in \mathbb{Z}^n$ with $\sum m_i$ even. Norm 2 vectors: $(0, \ldots \pm1, \ldots, 0, \ldots, \pm1, \ldots, 0)$.

$\#$ norm 2 vectors $= \binom{n}{2} \times 2^2 = n(2n-2)$. Coxeter number $= \frac{n(2n-2)}{n} = 2n-2$.

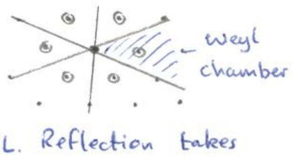
(iii) E_8 = vectors $(m_1, \ldots, m_8)$, $\sum m_i$ even, all $m_i \in \mathbb{Z}$ or all $m_i \in \mathbb{Z} + \frac{1}{2}$. $\#$ norm 2 vectors $= 240$,

Coxeter number $= \frac{240}{8} = 30$.

(iv) E_7 = vectors $(m_1, \ldots, m_8)$ of E_8 with $m_1 = m_2$. $\#$ norm 2 vectors $= 126$. Coxeter number $= \frac{126}{7} = 18$.

(v) E_6 = vectors $(m_1, \ldots, m_8)$ of E_8 with $m_1 = m_2 = m_3$. $\#$ norm 2 vectors $= 72$. Coxeter number $= \frac{72}{6} = 12$.

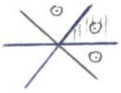
Suppose L is any lattice generated by norm 2 vectors (positive definite). Eg, L:



Draw hyperplanes perpendicular to norm 2 vectors. (Automorphism group acts transitively on Weyl chambers. If $v^2 = 2$, then reflection in $v^\perp$ is an automorphism of L. Reflection takes $w \mapsto w - \frac{2(w,v)}{(v,v)}v$. So if $(v,v) = 2$, then reflection takes $w \mapsto w - (w,v)v \in L$, as $(w,v) \in \mathbb{Z}$)

So any Weyl chamber has the same shape as any adjacent chamber. ⇒ any two Weyl chambers have same shape (ie, there is an automorphism of L taking one to the other).

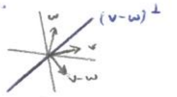
Pick one chamber W. Look at its walls. For each wall, pick the norm 2 vector orthogonal to the wall which has positive definite inner product with elements of W.



Suppose v, w are two such vectors. What is (v,w)?

If v, w are any norm 2 vectors, then $|(v,w)| \le |v|.|w| \le 2$. So $(v,w) = \begin{cases} 2 \Rightarrow v=w \\ 1, 0, -1 \\ -2 \Rightarrow v=-w. \end{cases}$

If $(v,w)=1$, then $(v-w)^2$ has norm 2. Wall of $(v-w)$ separates walls of v,w:

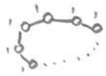


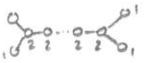
So then $v^\perp, w^\perp$ cannot be walls of same Weyl chamber.

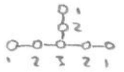
So either $v=w$, $(v,w)=0$, or $(v,w)=-1$.

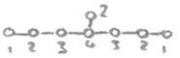
Draw Dynkin diagram: one node for each wall; two vectors joined if corresponding vectors v,w have $(v,w)=-1$, and not if $(v,w)=0$.

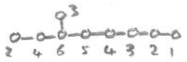
Consider following set of graphs:

$\hat{A}_n$:  n+1 vertices

$\hat{\tilde{D}}_n$:  n+1 vertices ($n \geqslant 4$)

$\tilde{E}_6$: 

$\tilde{E}_7$: 

$\tilde{E}_8$: 

Each number on a node $= \frac{1}{2}$ (sum of numbers on nodes joined to it).

Corollary: No Dynkin diagram can contain one of these graphs.

Proof: Suppose v_i is vector of each node of Dynkin diagram in one graph above.

Put $m_i :=$ number associated to node. Consider vector $v = \sum v_i m_i$.

(i) $v \neq 0$ as all $m_i > 0$, and v_i has inner product >0 with elements of W, so v does too.

(ii) $(v_i, v) = 0 \ \forall i$, as it equals $2 \times m_i - \sum_{j \text{ joined to } i} m_j = 0$

(iii) $(v,v)=0$, as v is a linear combination of v_i's.

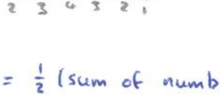
We cannot have a vector v with $v \neq 0$, $v^2 = 0$, as L is positive definite.

We now classify all connected graphs G not containing $\tilde{A}_n, \tilde{D}_n, \tilde{E}_6, \tilde{E}_7, \tilde{E}_8$.

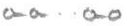
Step 1: G does not contain any A_n (= cycle), so G is a tree.

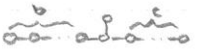
Step 2: G does not contain $\tilde{D}_4$, so all vertices have degree ≤ 3.

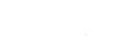
Step 3: G does not contain $\tilde{D}_n$, so G contains ≤ 1 vertex of valence 3.

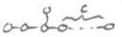
So G looks like: 

Step 4: One of a,b,c must be 0 or 1. (If all $\geqslant 2$, then G contains $\tilde{E}_6$).

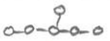
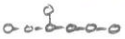
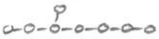
Case (i): One of $a,b,c = 0$. $G =$  $=: A_n$.

Otherwise, we can assume (say), $a=1$, $b,c \geqslant 1$. So G: 

Case (ii): $a=b=1$:  $=: D_n$.

We can thus assume $a=1$, $b,c \geqslant 2$. Note we cannot have $b,c \geqslant 3$ as G does not contain $\tilde{E}_7$. So we can assume $b=2$: 

$c \le 4$, since G does not contain $\tilde{E}_8$

$c=1 \Rightarrow D_5$. So can assume $c = 2, 3, 4$:   

$\overset{!!}{E_6}$ $\quad$ $\overset{!!}{E_7}$ $\quad$ $\overset{!!}{E_8}$

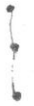
Summary: Any Dynkin diagram of a lattice must be a union of the graphs A_n, D_n, E_6, E_7, E_8 above, since it cannot contain $\tilde{A}_n, \tilde{D}_n, \tilde{E}_6, \tilde{E}_7, \tilde{E}_8$.

If L is a lattice generated by norm 2 vectors, Dynkin diagram of L is a union of A_n, D_n, E_6, E_7, E_8.
Check that Dynkin diagram determines L:
L is generated by norm 2 vectors corresponding to walls of Weyl chamber W.
We know L is generated by norm 2 vectors, so enough to check any norm 2 vector of L is generated by norm 2 vectors of W. Let W' be adjacent to W.

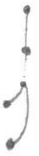
So W' = reflection of W in some norm 2 vector r. So vector $\perp$ wall of W' = vector $v \perp$ to wall of W reflected in r, $= v - 2\frac{(v,r)}{(r,r)} r = v-(v,r)r \in$ lattice generated by v and r.
Carry on like this: $\Rightarrow$ all norm 2 vectors $\perp$ walls of any Weyl chamber are in lattice generated by vectors of Dynkin diagram.

So L is determined by Dynkin diagram, = lattice generated by a vector v_i for each node of Dynkin diagram, with $(v_i, v_j) = \begin{cases} 2 & \text{if } i=j \\ 0 & \text{if } i \text{ not joined to } j \ (i \neq j) \\ -1 & \text{if } i \text{ joined to } j \ (i \neq j) \end{cases}$
Check that A_n, D_n, E_6, E_7, E_8, diagrams correspond to A_n, D_n, E_n lattices.
We have to find a Weyl chamber of each lattice:

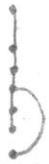
A_n: Lattice := $(m_1,.., m_{n+1})$, $\Sigma m_i = 0$.
norm 2 vectors corresponding to Weyl chamber $(1,-1,0,..,0)$
$(0,1,-1,0,..,0)$
$\vdots$
$(0,...,0,1,-1)$



D_n: Lattice := $(m_1,..,m_n)$, Σm_i even.
norm 2 vectors corresponding to Weyl chamber $(1,-1,0,..,0)$
$(0,1,-1,..0)$
$\vdots$
$(0,..,0,1,-1)$
$(0,..,0,1,1)$



E_8: $(m_1,..,m_8)$, Σm_i even, all $m_i \in \mathbb{Z}$, or all $m_i \in \mathbb{Z}+\frac{1}{2}$.
norm 2 vectors corresponding to Weyl chamber $(1,-1,0,..,0)$
$(0,1,-1,0..0)$
$\vdots$
$(0,...,0,1,-1)$
$(\frac{1}{2},..,\frac{1}{2},-\frac{1}{2},-\frac{1}{2},\frac{1}{2})$



L = even, self-dual lattice in dimension 8. Modular form $\Rightarrow$ L has 240 norm 2 vectors.
vectors / dimension = 30.
Look at sublattice of L generated by these norm 2 vectors. Lattices must be a sum of $A_n (n \leq 8)$, $D_n (n \leq 8)$ and E_6, E_7, E_8.

A_1 : 2	D_4 : 6	E_6 : 12
3	D_5 : 8	
$\vdots$	$\vdots$	E_7 : 18
A_8 : 9	D_8 : 14	E_8 = 30.

$\uparrow$ Coxeter number = vertices/dimension

All these lattices A_n, D_n, E_n $(n \leq 8)$ have average of 30 norm 2 vectors per dimension.
So to get average of 30, all the A_n, D_n, E_n's occurring must have average of exactly 30

vectors per dimension. So lattice generated by norm 2 vectors is the E_8 lattice. So $L \supseteq E_8$. But E_8 is self-dual ($E_8^* = E_8$), so it is maximal, so $L = E_8$.

Classify 16-dimensional even self-dual lattices.

Step 1: Work out θ function of L: it is a modular form of weight $\frac{\dim L}{2} = 8$. Space of such modular forms is 1-dimensional, spanned by $E_8 = E_4^2$. $E_8(\tau) = 1 + 480q + \cdots$
So L has 480 vectors of norm 2. # vectors/dimension $= 480/16 = 30$.

As before, all Coxeter numbers of A_n, D_n, E_n $(n \leq 16)$ are ≤ 30, with equality only for D_{16}, E_8.
So Dynkin diagram = union of E_8's, D_{16}'s. So sublattice generated by norm 2 vectors is E_8^2 or D_{16}. E_8^2 is maximal $\Rightarrow$ 1 possibility.
D_{16} not maximal (not self-dual). So what self-dual lattices contain D_{16}?
Any lattice containing D_{16} must be in D_{16}^*
D_{16}^* = vectors with integral inner product with $(m_1, \ldots, m_{16})$, Σm_i even.
= vectors $(m_1, \ldots, m_{16})$ with either all $m_i \in \mathbb{Z}$ or all $m_i \in \mathbb{Z} + 1/2$.

$$D_{16}^* / D_{16} = \underbrace{(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})}_{\text{represented by } (0^{16}),\ (1, 0^{15}),\ (\frac{1}{2}^{16}),\ (-\frac{1}{2}, \frac{1}{2}^{15}).}$$

Subgroups of D_{16}^* containing D_{16} $\Leftrightarrow$ subgroups of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$

Subgroups of $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$	Lattice
0	D_{16}
$(1, 0^{15})$	$D_{16} + (1, 0, \ldots, 0) = \mathbb{Z}^{16}$ (not even).
$(\frac{1}{2})^{16}$	$D_{16} + (\frac{1}{2})^{16}$ - even, self-dual.
$(-\frac{1}{2}, \frac{1}{2}^{15})$	$D_{16} + (-\frac{1}{2}, \frac{1}{2}^{15})$ - even, self-dual.
$(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$	not integral.

Reflection in vector $(1, 0^{15})^\perp$ exchanges these cases. So, up to isomorphism there is exactly 1 even self-dual lattice containing D_{16}. So we get two even self-dual lattices in dimension 16, namely E_8^2 and $D_{16} + (\frac{1}{2})^{16}$.

Even self-dual lattices in dimension 24 - 24 lattices.

1. Leech lattice (no norm 2 vectors).
2. Possible Dynkin diagrams are:

$$\left.\begin{array}{l} A_1^{24},\ A_2^{12},\ A_3^{8},\ A_4^{6},\ A_6^{4},\ A_8^{3},\ A_{12}^{2},\ A_{24} \\ D_4^{6},\ D_6^{4},\ D_8^{3},\ D_{12}^{2},\ D_{24} \\ A_5^4 D_4,\ A_7^2 D_5^2,\ A_9^2 D_6,\ A_{15} D_9 \\ E_6^4,\ \underset{\underset{12}{\downarrow}}{A_{11}}\ \underset{\underset{12}{\downarrow}}{D_7}\ \underset{\underset{12}{\downarrow}}{E_6},\ E_7^2 D_{10},\ E_7 A_{17},\ E_8^3,\ E_8 D_{16} \end{array}\right\} \text{Niemeier lattices.}$$

- Coxeter number $11 + 7 + 6 = 24$.

Venkor: Modular forms imply that Dynkin diagram is either empty or the union of a set of A, D, E's of total rank 24, such that all components have the same Coxeter number.
Dynkin diagrams satisfying these conditions exactly list above.

32 dimension: $\geqslant 8 \times 10^7$ self-dual even lattices.

Remark: (i) Lattices generated by vectors of norms 1 and 2 are lattices above, $\oplus \mathbb{Z}^n$.

(ii) Lattices generated by vectors of norm 3 seem impossible to classify.

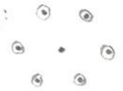
(iii) We can classify lattices generated by roots. A root is a vector v such that reflection in $v^\perp$ is an automorphism of the lattice.

Lattices generated by roots are same as above, except:

(i) can multiply A_n, D_n, E_n by constants.

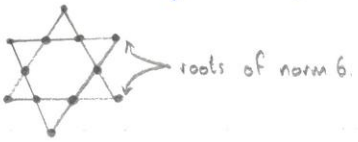
(ii) some lattices have >1 set of roots generating them.

(iii) A_2:



lattice generated by 6 roots.

G_2:



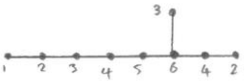
Lattice also generated by roots of norm 2 and 6.

(iv) Root systems $A_n, D_n, E_n, B_n, C_n, F_4, G_2$ correspond to finite dimensional simple Lie algebras, ~ Lie groups. $\tilde{A}_n, \tilde{D}_n, \tilde{E}_n \Rightarrow$ "Affine Lie algebras"

= Loop algebras = Kac-Moody algebras = Euclidean Lie algebras.

(v) Classify rotation groups in $\mathbb{R}^3$: A_n cyclic, D_n dihedral, E_6 E_7 E_8 - rotations of tetrahedron, octahedron, icosahedron.

Eg: Take icosahedral group A_5. Has double cover $\hat{A}_5$ of order 120.
Look at representations of A_5: irreducible representations 1, 2, 2, 3, 3, 4, 4, 5, 6.



Representations $\hat{A}_5 \Leftrightarrow$ nodes of $\hat{E}_8$.
Representation × 2 dim. representation = Σ representations joined to it.

$$6 \otimes 2 = 3 \oplus 5 \oplus 4.$$

A_n, D_n, E_n also turn up in singularity theory, conformal field theory, von Neumann algebras, ...
Completely unexplained fact about E_8: McKay - Look at the monster group ($\sim 10^{54}$). Look at conjugacy class 2A of elements of order 2. Look at products of pairs g, h of elements of order 2.
9 orbits of pairs g, h. Look at orders of gh: 1, 2, 2, 3, 3, 4, 4, 5, 6. (Remark: if the monster is replaced by Baby Monster or F_{24}' get similar relations with $\tilde{E}_7, \tilde{E}_8$ diagrams.

Hecke Operators.

Main properties:

1. For each $n \geq 1$, we will construct a Hecke operator T_n, from modular forms of weight k to modular forms of weight k (or mod. fns. → mod. fns.)
2. Hecke operators commute: $T_m T_n = T_n T_m$.
3. All self-adjoint.

2, 3 ⇒ can find a basis of modular forms consisting of "eigenforms."

Look at simplest Hecke operator T_2 on modular function $j(\tau)$.

Recall: $SL_2(\mathbb{Z})$ generated by $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$: $j(\tau+1) = j(\tau)$, $j(\frac{-1}{\tau}) = j(\tau)$

Modular functions with no poles on H = polynomials in $j(\tau)$.

Approach 1: Try making $j(2\tau)$ into a modular function by adding things to it.

$j(\tau)$ invariant under $\tau \mapsto \tau+1$, but not under $\tau \mapsto {}^{-1}/_{\tau}$. So add $j(2(\frac{-1}{\tau})) = j(\frac{-2}{\tau}) = j(\tau/2)$.

Try $\underset{\tau\mapsto\tau+1}{j(2\tau)} + \underset{\tau\mapsto -\frac{1}{\tau}}{j(\tau/2)}$ – not invariant under $\tau \mapsto \tau+1$

$\tau \mapsto \tau+1$ takes $j(\tau/2) \mapsto j(\frac{\tau+1}{2})$.

Try $\underset{\tau\mapsto\tau+1}{j(2\tau)} + \underset{\tau\mapsto -\frac{1}{\tau}}{j(\tau/2)} + \underset{\tau\mapsto\tau+1}{j(\frac{\tau+1}{2})}$. $j(\frac{\tau+1}{2})$ invariant under $\tau \mapsto \frac{-1}{\tau}$: $j(\frac{-\frac{1}{\tau}+1}{2}) = j(\frac{\tau-1}{2\tau}) \overset{S}{=} j(\frac{-2\tau}{\tau-1})$
$\overset{T^2}{=} j(\frac{-2}{\tau-1}) \overset{S}{=} j(\frac{\tau-1}{2}) \overset{T}{=} j(\frac{\tau+1}{2})$

Application: We know $j(2\tau) + j(\tau/2) + j(\frac{\tau+1}{2})$ is a modular function, as it is invariant under S, T. It obviously has no poles on H, so it must be a polynomial in $j(\tau)$. Two polynomials in j are equal $\Leftrightarrow$ coefficients of q^n for $n<0$ are the same.

So look at
$$j(\tau) = q^{-1} + 744 + 196884q + \cdots$$
$$j(\tau)^2 = q^{-2} + 2\times 744 q^{-1} + \text{constant} + \cdots$$
$$j(2\tau) = q^{-2} + 744 + \cdots$$
$$j(\tfrac{1}{2}\tau) = q^{-1/2} + 744 + \cdots$$
$$j(\tfrac{\tau+1}{2}) = -q^{-1/2} + 744 + \cdots$$

$$j(2\tau) + j(\tau/2) + j(\tfrac{\tau+1}{2}) = a j(\tau)^2 + b j(\tau) + c.$$
$$q^{-2} + 3\times 744 = a(q^{-2} + 1488 q^{-1} + \cdots) + b(q^{-1} + \cdots) + c.$$
$a = 1$ (coefficient of q^{-2}), $b = -1488$ (coefficient of q^{-1}), $c = 162000$.

So $j(2\tau) + j(\tau/2) + j(\frac{\tau+1}{2}) = j(\tau)^2 - 1488 j(\tau) + 162000$.

$j(\tau) = \sum c(n) q^n = q^{-1} + 744 + 196884q + 21493760 q^2 + 864299970 q^3 + 20245856256 q^4 + \cdots$

$$\overset{j(2\tau)}{\sum c(\tfrac{n}{2}) q^n} + \underbrace{\overset{j(\tau/2)}{\sum c(n) q^{n/2}} + \overset{j(\frac{\tau+1}{2})}{\sum (-1)^n c(n) q^{n/2}}}_{= 2\sum c(2n) q^n.} = \sum_n \Big(\sum_i c(n-i) c(i)\Big) q^n - 2c(0)\sum c(n) q^n + 162000$$
$(c(\frac{n}{2}) = 0,\ n \text{ odd})$

Compare coefficients of q^n: $c(\frac{n}{2}) + 2c(2n) = \sum c(n-i) c(i) - 2c(0)c(n)$, $n>0$.

Eg: $n=2$: $c(1) + 2c(4) = (2c(-1)c(3) + 2c(0)c(2) + c(1)^2) - 2c(0)c(2)$

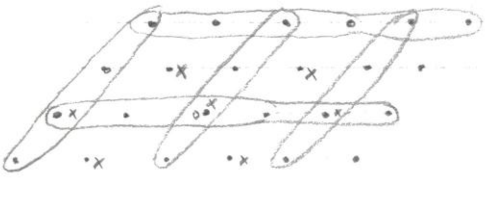
$c(4) = c(3) + \frac{c(1)^2 - c(1)}{2}$. Similarly get recursive relations for $c(2n)$, $n \geq 2$.

Approach 2: Recall modular functions $\equiv$ homogeneous functions of lattices.

$$f(\tau) \equiv f(L) : L = \langle 1, \tau \rangle$$
$$f(\lambda L) = f(L),\ \lambda \in \mathbb{C}.$$

Suppose f is a function of lattices L. Then so is $\sum_{\substack{L' \subset L \\ |L/L'| = 2}} f(L')$ – sum over all sublattices of index 2.

If f is homogeneous then so is $f(L')$. What is sublattice of index 2 of lattice $= \langle 1, \tau \rangle$?
($\equiv$ homomorphisms from L onto $\mathbb{Z}/2\mathbb{Z}$, so 3 such sublattices).



Sublattices of index 2:

1. $\langle 1, 2\tau \rangle$
2. $\langle 2, \tau \rangle$
3. $\langle 2, \tau+1 \rangle$

$\sum_{L:L'=2} f(L')$ = when $L = \langle 1,\tau\rangle$

$= f(\langle 1, 2\tau\rangle) + f(\langle 2,\tau\rangle) + f(\langle 2,\tau+1\rangle)$, as $f(\lambda L') = f(L')$.

$\rightsquigarrow f(2\tau) + f(\frac{\tau}{2}) + f(\frac{\tau+1}{2})$

1. This explains why sum in approach 1 was finite. A lattice has only finitely many sublattices of index 2.
2. We can look at sublattices of index n instead of index 2.
3. Works for modular forms of weight k, as if f is a function of lattices of degree $-k$, so is $\sum_{L'} f(L')$.

Approach 3: via double cosets.

Look at $M_2(\mathbb{Z})$ = 2x2 matrices of determinant 2. ($M_2(\mathbb{Z})$ is a double coset of $SL_2(\mathbb{Z})$ is $SL_2(\mathbb{Q})$).

Look at $f(\tau) = \sum_{A \in SL_2(\mathbb{Z})\backslash M_2(\mathbb{Z})} j(A\tau)$ (†)

Look at $f(B\tau)$, $B \in SL_2(\mathbb{Z})$, $= \sum_{A \in SL_2(\mathbb{Z})\backslash M_2(\mathbb{Z})} j(AB\tau) = \sum_{A \in SL_2(\mathbb{Z})\backslash M_2(\mathbb{Z})} j(A\tau)$, as $M_2(\mathbb{Z})B = M_2(\mathbb{Z})$.

$= f(\tau)$, so (†) takes modular functions to modular functions.

What is a set of representotives of $SL_2(\mathbb{Z})\backslash M_2(\mathbb{Z})$?

↖ row operations on matrices.

If $\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in M_2(\mathbb{Z})$ we can use row operations to make $c=0$, so assume it is $\begin{pmatrix} a & b \\ 0 & d\end{pmatrix}$, $\det = ad = 2$.

So it is $\begin{pmatrix} 2 & b \\ 0 & 1\end{pmatrix}$ or $\begin{pmatrix} 1 & b \\ 0 & 2\end{pmatrix}$. More operations ⇒ $\begin{pmatrix} 2 & 0 \\ 0 & 1\end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 0 & 2\end{pmatrix}$ or $\begin{pmatrix} 1 & 1 \\ 0 & 2\end{pmatrix}$.

So sum above is: $f(\begin{pmatrix} 2 & 0 \\ 0 & 1\end{pmatrix}\tau) + f(\begin{pmatrix} 1 & 0 \\ 0 & 2\end{pmatrix}\tau) + f(\begin{pmatrix} 1 & 1 \\ 0 & 2\end{pmatrix}\tau) = f(2\tau) + f(\frac{\tau}{2}) + f(\frac{\tau+1}{2})$.

Approach 4: Suppose element $g \in SL_2(\mathbb{R})$ normalises $SL_2(\mathbb{Z})$. Then look at $f(g\tau)$.

This is invariant under $SL_2(\mathbb{Z})$, as $f(gA\tau) = f((gAg^{-1})g\tau) = f(g(\tau))$, as $gAg^{-1} \in SL_2(\mathbb{Z})$.

For each element of $N_{SL_2(\mathbb{R})}(SL_2(\mathbb{Z}))$ we get a function from modular forms to modular forms.

$SL_2(\mathbb{Z})$ is its own normalisers.

Remark: for subgroups other than $SL_2(\mathbb{Z})$, this does give new operations:

eg, if $\Gamma_0(2) = \{\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in SL_2\mathbb{Z} : 2|c\}$, then the element $\begin{pmatrix} 0 & 1/\sqrt{2} \\ -1/\sqrt{2} & 0\end{pmatrix} \in SL_2(\mathbb{R})$ normalises $\Gamma_0(2)$

– this is the Fricke involution.

Suppose g almost normalises $SL_2(\mathbb{Z})$ in the sense that $G = g^{-1}SL_2(\mathbb{Z})g \cap SL_2(\mathbb{Z})$ has finite index in $SL_2(\mathbb{Z})$. Then $f(g\tau)$ is invariant under group G of finite index in $SL_2(\mathbb{Z})$. So by summing $f(g\tau)$ over a finite number of cosets of G in $SL_2(\mathbb{Z})$ we can leave it invariant:

eg: Take $g = \begin{pmatrix} 2 & 0 \\ 0 & 1\end{pmatrix}$. $G = \Gamma_0(2) = \{\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in SL_2(\mathbb{Z}) : 2|c\}$ – has index 3 in $SL_2(\mathbb{Z})$.

So $f(\tau)$ a modular function ⇒ $f(2\tau) + f(\tau/2) + f(\frac{\tau+1}{2})$ is a modular function.

We want to generalise this, replacing 2 by n and modular functions by modular forms.

We use method 2, using lattices. This works as follows.

Modular form $f(\tau)$ of weight k ⇒ function $f(L)$ of lattices, $f(\lambda L) = \lambda^{-k} f(L)$.

⟶ $\sum_{L', L:L'=n} f(L')$, function of lattices, homogeneous of degree $-k$

⟶ function of τ, value of L at $\langle \tau, 1\rangle$.

We want to calculate this explicitly. We first need to find lattices L' of index n in L.

Assume L has basis $\{\omega_1, \omega_2\}$, oriented. Choose a basis of L': it must be of the form $\{a\omega_1 + b\omega_2, c\omega_1 + d\omega_2\}$, $a,b,c,d \in \mathbb{Z}$. Index of L' in L = $|\det\begin{pmatrix} a & b \\ c & d\end{pmatrix}|$.

Assume basis of L' is oriented $\Rightarrow \det > 0$.
So $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = n$. We have a map: $M_n = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \det = n\right\} \to$ Sublattices L' of index n.
When do two matrices give same lattice L'?
Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv$ knowing L' and oriented basis of L'
Change of basis of L' can be described by a matrix of determinant ± 1. Oriented basis $\Rightarrow \det = +1$.
This corresponds to changing $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $\begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, where $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ is the change of basis.
So lattices L' of index $n \leftrightarrow$ cosets $SL_2(\mathbb{Z}) \backslash M_n$.

Now we want to find cosets $SL_2(\mathbb{Z}) \backslash M_n$. (This gives row operations on M_n).
Can we turn $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ into some canonical form using row operations?
First, by row operations, make c as small as possible. This means $c = 0$. Otherwise, change $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ to $\begin{pmatrix} a' & b' \\ c & d \end{pmatrix}$ with $|a'| < c$, then to $\begin{pmatrix} c & d \\ -a' & -b' \end{pmatrix}$ - $\#$ as $|a'| < c$.
Secondly, multiply by -1 (if necessary) to make $a > 0$. So have $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, $a > 0$, $ad = n$.
Subtract multiples of second row from first $\Rightarrow 0 \leq b < d$.
Summary: every coset is represented by (at least) one matrix $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$: $a > 0$, $ad = n$, $0 \leq b < d$. - $(*)$

Suppose that $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} A & B \\ C & D \end{pmatrix}\begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$ for a, b, d, a', b', d' as above and $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in SL_2(\mathbb{Z})$.
$= \begin{pmatrix} Aa' & Ab' + Bd' \\ Ca' & Cb' + Dd' \end{pmatrix}$.
$0 = Ca' \Rightarrow C = 0$.
$Aa' = a$, $a > 0 \Rightarrow A > 0$. $AD - BC = 1$, $A > 0$, $C = 0 \Rightarrow A = D = 1$.
Then $a = a'$, $d = d'$, $b' + Bd = b$. But $0 \leq b, b' < d \Rightarrow b = b'$.
Summary: Sublattices L' of index n in $L = \langle w_1, w_2 \rangle$ are exactly the lattices $\langle aw_1 + bw_2, dw_2 \rangle$ with $ad = n$, $a > 0$, $0 \leq b < d$.

We now use this to find the operator. Apply operator to f.
Value at $\tau \in H = \sum_{L : L' = n} f(\langle \tau, 1 \rangle)$ $\qquad f(\langle w_1, w_2 \rangle) = w_2^{-k} . f(w_1/w_2)$.
$$= \sum_{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} (*)} f(\langle a\tau + b, d \rangle) = \sum_{\text{same}} d^{-k} . f\left(\left\langle \frac{a\tau+b}{d}, 1 \right\rangle\right) = \sum_{\text{same}} d^{-k} f\left(\frac{a\tau + b}{d}\right).$$

The mth Hecke operator $T_k(m)$ acting on forms of weight k is defined to be m^{k-1} times the operator above: $(T_k(m) f)(\tau) = m^{k-1} . \sum_{\substack{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} | a > 0, \\ ad = m, 0 \leq b < d}} d^{-k} f\left(\frac{a\tau + b}{d}\right)$.

It is obvious from the above that if f transforms like a modular form of weight k then so does $T_k(m) f$.

What is Fourier expansion of $T_k(m) f$ if $f(\tau) = \sum c(n) q^n$? $T_k(m) f(\tau) = m^{k-1} . \sum_{(*)} d^{-k} \sum_{n \in \mathbb{Z}} c(n) e^{2\pi i \left(\frac{a\tau + b}{d}\right) n}$
Look at sum over b: $\sum_{0 \leq b < d} e^{2\pi i bn/d} \times \{\text{fudge}\}$. This is zero unless $n/d \in \mathbb{Z}$, in which case it is d.
So sum becomes $m^{k-1} \sum_{\substack{ad = m \\ a > 0}} d^{-k} . \sum_{\substack{n \in \mathbb{Z} \\ d | n}} d . c(n) . e^{2\pi i a \tau n/d} = m^{k-1} . \sum_{\substack{ad = m \\ a > 0}} d^{-k} . \sum_n d\, c(nd) . \underbrace{e^{2\pi i a n \tau}}_{= q^{an}}$

$$= \sum_n \sum_{\substack{ad = m \\ a > 0}} \left(\frac{m}{d}\right)^{k-1} c(nd)\, q^{an} = \sum_n q^n . \sum_{\substack{ad = m \\ a | n}} a^{k-1} . c\left(\frac{nd}{a}\right) \quad \text{(change } n \text{ to } n/a\text{)}.$$

$$= \sum_n q^n . \left[\sum_{a | (m,n)} a^{k-1} . c\left(\frac{mn}{a^2}\right)\right]$$

↖ Fourier coefficient of $T_k(m) f$.

Application: If $c(n)=0$ for $n<0$ then coefficients of q^n for $n<0$ of $T_k(m)f$ are also 0.
$\therefore$ If f holomorphic at $i\infty$, so is $T_k(m)f$. So $T_k(m)$ takes modular forms to modular forms.
Also note that if $c(0)=0$ (ie, f vanishes at $i\infty$), then coefficient of q^0 in $T_k(m)f$ vanishes.
We say f is a cusp form if its constant coefficient vanishes.
Eg: $\Delta(\tau)=q-24q^2+\cdots$ is a cusp form.
Any form of weight k = const. $\times E_k(\tau)$ + cusp form.

The function $\Delta(\tau)$ is an eigenvector of all Hecke operators.
Proof: Hecke operators act on the space of cusp forms of weight 12. This is a 1-dimensional space spanned by Δ.

What is the eigenvalue of $T_{12}(m)$ on $\Delta(\tau)$?
Coefficient of q^n of $T_{12}(m)\Delta$ is $\sum_{d|(m,n)} d^{k-1}.c(\frac{mn}{d^2})$. Put $n=1$: $\sum_{d|(m,1)} d^{12-1}\,c\left(\frac{m\times 1}{d^2}\right) = c(m)$.
So $T_{12}(m)\Delta = c(m)q+\cdots$, $\Delta=\sum c(n)q^n$. So $T_{12}(m)\Delta = c(m)\Delta$, as Δ is an eigenform of $T_{12}(m)$.
Use this to prove that coefficients of Δ are multiplicative: $\Delta=\sum\tau(n)q^n$, $\tau(m)\tau(n)=\tau(mn)$ when $(m,n)=1$.

Lemma: $T_k(m)T_k(n)=T_k(mn)$ whenever $(m,n)=1$.
Proof: Look at operators on functions of lattices. $T(m)f=\sum_{L:L'=m} f(L')$, f a function of lattices.
So we want to prove $T(m)T(n)=T(mn)$. $T(mn)f=\sum_{L:L'=mn} f(L')$.
Look at group L/L' of order mn. m,n coprime $\Rightarrow$ this has unique subgroup of order m.
So there's only one way to find a lattice L'' with $L/L''=m$, $L''/L'=n$.
So $T(mn) = T(m)T(n)$ take all lattices L'' with $L/L''=n$
then take all sublattices L' of L'' with $L''/L'=m$.

We know: (i) $T_k(m)T_k(n)=T_k(mn)$, when $(m,n)=1$
(ii) $T_k(m)\Delta=\tau(m)\Delta$
$\Rightarrow \tau(mn)\Delta = T_k(mn)\Delta = T_k(m)T_k(n)\Delta = \tau(m)\tau(n)\Delta$.
$\Rightarrow \tau(mn)=\tau(m)\tau(n)$ for $(m,n)=1$.

Look at $T_{12}(2)$ on $\Delta(\tau)=q-24q^2+252q^3-\underset{\text{NOT }(-24)\times(-24)}{1472}q^4+4830q^5-\underset{=(-24)\times(252)}{6048}q^6\cdots$

$(-24)^2 = (-1472)+2^{11}\times 1.$

$$T_{12}(2)\Delta(\tau) = 2^{12-1}\Big(\underset{\sum\tau(n)q^{2n}}{\Delta(2\tau)} + \underbrace{\Delta(\tau/2)\,2^{-12}+2^{-12}.\Delta(\tfrac{\tau+1}{2})}_{2^{-11}.\sum\tau(2n)q^n.}\Big)$$

$$T_{12}(2)\Delta(\tau) = \sum 2^{11}\tau(n)q^{2n} + \sum\tau(2n)q^n.$$

Δ	q	q^2	q^3	q^4
$\Delta(\tau)$	$\tau(1)=1$	$\tau(2)$	$\tau(3)$	$\tau(4)$
$2^{11}\Delta(2\tau)$		$2^{11}\tau(1)$		$2^{11}\tau(2)$
$\frac{1}{2}(\Delta(\frac{\tau}{2})+\Delta(\frac{\tau+1}{2}))$	$\tau(2)$	$\tau(4)$	$\tau(6)$	$\tau(8)$
$T_{12}(2)\Delta(\tau)$	$\tau(2)$	$2^{11}\tau(1)+\tau(4)$	$\tau(6)$	$2^{11}\tau(2)+\tau(8)$
	$\updownarrow$	$\updownarrow$	$\updownarrow$	$\updownarrow$ equal.
$=$const. $\Delta(\tau)$	$\tau(2)\times\tau(1)$	$\tau(2)\times\tau(2)$	$\tau(2)\times\tau(3)$	$\tau(2)\times\tau(4)$

$\tau(2).\Delta(\tau)$

Summary: $\tau(2)^2 = \tau(4) + 2^{11}\tau(1)$. $\quad \tau(2)\tau(4) = \tau(8) + 2^{11}\tau(2)$

$\tau(2)\,\tau(2^n) = \tau(2^{n+1}) + 2^{11}\tau(2^{n-1})$

For other primes, we guess that $\tau(p)\,\tau(p^n) = \tau(p^{n+1}) + p^{11}\tau(p^{n-1})$.

This follows if $T_{12}(p)\,T_{12}(p^n) = T_{12}(p^{n+1}) + p^{11}.T_{12}(p^{n-1})$.

Guess: $T_k(p).T_k(p^n) = T_k(p^{n+1}) + p^{k-1}.T_k(p^{n-1})$ for primes p.

We look at sublattices of a lattice L.

Put $T(n)(L) = \Sigma$ all lattices L' with $L:L' = n$.

$\uparrow$ operator acting on free abelian group generated by lattices in $\mathbb{C}$.

We showed that $T(m)\,T(n) = T(mn)$ if $(m,n) = 1$.

Lemma: $T(p^n)\,T(p) = T(p^{n+1}) + p\,T(p^{n-1})R(p)$, $\quad R(p)$ takes a lattice L to pL.

Proof: Consider any lattice L' of index p^{n+1} in L. Have to show coefficient of L' of both sides is the same.

Case (i): Suppose $L' \subset pL$ $\left({}^{L}/_{L'} \cong {}^{\mathbb{Z}}/_{p^i\mathbb{Z}} \times {}^{\mathbb{Z}}/_{p^{n-i}\mathbb{Z}},\ 0<i<n \right)$.

Then the coefficient of L' in $T(p^n)\,T(p)\,L = p+1$ as L' is contained in all the $\underset{\uparrow}{p+1}$ lattices of $T(p)L$ of index p in L.

For: $ad = p$, $0 \leq b < d$
(i) $a = p$, $d = 1$, $b = 0$
(ii) $a = 1$, $d = p$, $0 \leq b < p$
$(= p+1)$

On the right hand side, get a factor of 1 from $T(p^{n+1})$

get a factor of 1 from $R(p)\,T(p^{n-1}) = T(\underset{\uparrow}{p^{n-1}})\,R(p)$

L' now has index p^{n-1} in pL.

Total is $1 + p\times 1 = p+1$.

Case (ii): Suppose $L' \not\subset pL$. $\left({}^{L}/_{L'} \cong {}^{\mathbb{Z}}/_{p^n\mathbb{Z}},\ \text{cyclic} \right)$.

Coefficient coming from $R(p)\,T(p^{n-1})$ is 0, L' not in $R(p) = pL$. Coefficient coming from $T(p^{n+1})$ is 1 (L' has index p^{n+1} in L). Note that L' is contained in only one sublattice of index p. (otherwise L' would be in pL, as intersection of two different sublattices of index p is pL). So coefficient of $T(p^n)T(p)L$ is just 1.

So in both cases, coefficient of L' in LHS and RHS is same, which proves the lemma.

$T(m)$, $R(m)$ act on lattices, so on functions on lattices.

On functions of lattices of degree $-k$, $R(m)$ is just multiplication by m^{-k}.

So on functions of lattices of degree $-k$, we have $T(p^n)\,T(p) = T(p^{n+1}) + p^{1-k}.T(p^{n-1})$.

Function of lattices of degree $-k \leftrightarrow$ modular form of weight k.

$T_k(m) = m^{1-k} \times T(m)$ (acting on functions of lattices).

So we find $T_k(p^n)\,T_k(p) = T_k(p^{n+1}) + p^{1-k}.(p^{k-1})^2.T_k(p^{n-1}) = T_k(p^{n+1}) + p^{k-1}.T_k(p^{n-1})$.

Note that $T_k(p^2) = T_k(p)^2 + \text{constant}$.

$T_k(p^3) = T_k(p^2).T_k(p) + \text{constant}.T_k(p)$.

$T_k(p^4) = T_k(p^3).T_k(p) + \cdots$

$T_k(p^n)$ are all in algebra generated by $T_k(p)$. $T_k(p_1^{n_1} \cdots p_L^{n_L}) = T_k(p_1^{n_1}) \cdots T_k(p_L^{n_L})$ if $p_1, \ldots, p_L$ prime.

Hecke algebra, generated by all $T_k(m)$'s for $m>0$, k fixed, is generated by $T_k(p)$, p prime

We know $T_k(p_1).T_k(p_2) = T_k(p_2)\,T_k(p_1)$ for any primes p_1, p_2 (both sides are $T_k(p_1p_2)$ if $p_1 \neq p_2$).

So Hecke algebra is generated by commuting elements $T_k(p)$, so it is a commutative algebra.

We want to study action of Hecke algebra on space of cusp forms of weight k.

Can we find some eigenforms of algebra? (All eigenforms have multiplicative coefficients)
$(\uparrow$ modular forms, eigenvector of all Hecke operators$)$

Eg: $k=12$: Yes, Δ is eigenform, as space of cusp forms of weight 12 has dimension $=1$.

$$k = \begin{array}{ccccc} 16, & 18, & 20, & 22, & 26 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ \Delta E_4 & \Delta E_6 & \Delta E_8 & \Delta E_{10} & \Delta E_{14} \end{array}$$
- space of cusp forms has dimension 1.
$\leftarrow$ all have multiplicative coefficients.

Lemma: Suppose S is a commutative set of operators acting on a finite dimensional vector space over $\mathbb{C}$, of dimension ≥ 1. Then there is at least 1 eigenvector common to all the operators.

Proof: $S = S_1, S_2, \ldots$ Choose any eigenvalue λ_1 of S_1. Look at eigenspace V_{λ_1} of λ_1. Then V_{λ_1} is fixed by all S_i: If $v \in V_{\lambda_1}$, $S_1 v = \lambda_1 v$. $S_1 S_2 v = S_2 S_1 v = S_2 \lambda_1 v = \lambda_1 S_2 v$, so $S_2 v \in V_{\lambda_1}$.
Repeat this: find an eigenvalue λ_2 of S_2 on V_{λ_1}. Eigenspace V_{λ_1,λ_2}. Get a decreasing sequence of spaces: $V_{\lambda_1} \geqslant V_{\lambda_1\lambda_2} \geqslant V_{\lambda_1\lambda_2\lambda_3} \geqslant \cdots$
As V is finite dimensional and non-zero, intersection is non-zero and is common eigenvector of all S_i's.

Corollary: For any k with non-zero cusp forms we can find at least one eigenform of all Hecke operators.

Note: We cannot always find a basis of a finite dimensional space which consists of eigenvectors for a commutative algebra acting on it. Eg: algebra generated by $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

Lemma: Suppose S is a commutative algebra acting on a finite dimensional complex vector space V. Suppose
(i) V has hermitian inner product
(ii) S closed under hermitian adjoints.
Then V has a basis of eigenvectors.

Proof: Choose any common eigenvector v (by previous lemma). Look at orthogonal complement $v^\perp$.
So $V = \langle v \rangle + v^\perp$. Space $v^\perp$ is also fixed by S:
If $w \in v^\perp$ and $s \in S$ then $(sw, v) = (w, \underset{\uparrow \text{ hermitian adjoint}}{s^+ v}) = (w, \text{const.} v) = 0$ as $(w,v)=0$

By induction, $v^\perp$ has a basis of eigenvectors, so V does.

Hecke algebra = algebra generated by Hecke operators acting on space of cusp forms of weight k.

1. $T_k(m)T_k(n) = T_k(mn)$ if $(m,n)=1$. $T_k(p^n)T_k(p) = T_k(p^{n+1}) + p^{k-1}T_k(p^{n-1})$.
2. If f is an eigenvector of all $T_k(m)$, $f(\tau) = \Sigma c(n) q^n$, then eigenvalue is $c(n)$, so $c(m)c(n) = c(m\,n)$, if $(m,n)=1$, $c(p^n)c(p) = c(p^{n+1}) + p^{k-1}c(p^{n-1})$.

Recall the above lemma - we want to find a hermitian form on the space of cusp forms.

So we want a form taking $f,g \to \underset{\text{linear in } f}{(f,g)} = \underset{\nwarrow \text{ antilinear in } g}{\overline{(g,f)}}$, $\quad (f,f) > 0$ for $f \neq 0$.

Try to define $(f,g) = \displaystyle\int_{\substack{\text{Fundamental} \\ \text{domain of } SL_2(\mathbb{Z}) \text{ on } H}} f(\tau)\overline{g(\tau)}\,dx\,dy \times (\text{Fudge factor of } \tau)$.

Obviously linear in f, antilinear in g, $(f,g) = \overline{(g,f)}$ if fudge factor is real. Satisfies $(f,f) > 0$ if fudge factor > 0. Integrating something over a fundamental domain of $SL_2(\mathbb{Z})$, so only makes sense for things invariant under $SL_2(\mathbb{Z})$.

So $f(\tau)\overline{g(\tau)}\,dx\,dy \times$ (fudge factor) should be invariant under $SL_2(\mathbb{Z})$.

Under $SL_2(\mathbb{Z})$: $f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau)$, weight $(k,0)$

$\overline{g\left(\frac{a\tau+b}{c\tau+d}\right)} = \overline{(c\tau+d)}^{k'}\,\overline{g(\tau)}$, weight $(0,k')$.

Say f has weight (k,k') if $f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k (c\bar{\tau}+d)^{k'} f(\tau)$.

If f,g have weights (k_1,k_1'), (k_2,k_2'), then fg has weight $(k_1+k_2,\ k_1'+k_2')$.

$d\tau = dx + i\,dy$, $d\bar{\tau} = dx - i\,dy$. $d\tau\wedge d\bar{\tau} = -2i\,dx\wedge dy$.

$d\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{ad-bc}{(c\tau+d)^2}\,d\tau = (c\tau+d)^{-2}\,d\tau$, so $d\tau$ has weight $(-2,0)$.

So $f\bar{g}\,d\tau\wedge d\bar{\tau}$ has weight $(k-2,k-2)$.

We want $f\bar{g}\,d\tau\wedge d\bar{\tau} \times$ (fudge factor) to be invariant - ie, have weight $(0,0)$. So fudge factor should have weight $(-k+2,-k+2)$. Try $(k-2)$th power of a function of weight $(-1,-1)$.

So we want a function on H which is real, of positive weight $(-1,-1)$.

The function $\mathrm{Im}(\tau)$ has these properties.

Check that $\mathrm{Im}\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{-1}(c\bar{\tau}+d)^{-1}\,\mathrm{Im}\,\tau$:

$$\mathrm{Im}\left(\frac{a\tau+b}{c\tau+d}\right) = \mathrm{Im}\,\frac{(a\tau+b)(c\bar{\tau}+d)}{(c\tau+d)(c\bar{\tau}+d)} = |c\tau+d|^{-2}\,\mathrm{Im}\,(a\tau+b)(c\bar{\tau}+d) = |c\tau+d|^{-2}.(ad-bc).\mathrm{Im}\,\tau = |c\tau+d|^{-2}.\mathrm{Im}\,\tau.$$

So we define Peterson inner product by: $(f,g) = \int_{SL_2(\mathbb{Z})\backslash H} f(\tau)\overline{g(\tau)}.\,\mathrm{Im}(\tau)^{k-2}\,dx\,dy$.

We now want to show that the Hecke operators $T_k(n)$ are self-adjoint wrt $(\,,\,)$.

In other words, $(T_k(n)f, g) = (f, T_k(n)g)$.

(This obviously implies that Hecke algebra is closed under adjoints).

We would like to decompose (say) $T(2)$ as sum of 3 operators, $f(\tau)\mapsto f(2\tau)$, $f(\tau)\mapsto \text{const.}\,f(\tau/2)$, etc, and work out adjoints of these three operators.

Problem: $f(2\tau)$ not a modular form for $SL_2(\mathbb{Z})$, so $f(\tau)\to f(2\tau)$ not an operator on space of cusp forms. We will enlarge the space of cusp forms, to include functions like $f(2\tau)$.

Note that $f(2\tau)$ still invariant under $\tau\mapsto\frac{a\tau+b}{c\tau+d}$ for $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\begin{pmatrix}2&0\\0&1\end{pmatrix}^{-1}SL_2(\mathbb{Z})\begin{pmatrix}2&0\\0&1\end{pmatrix}$

Intersection of this group with $SL_2(\mathbb{Z})$ contains subgroup $\Gamma(2) = \left\{\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2,\ \begin{pmatrix}a&b\\c&d\end{pmatrix}\equiv\begin{pmatrix}1&0\\0&1\end{pmatrix} \bmod 2\right\}$.

We define a modular form of level N to be a holomorphic function on H such that:

1. $f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k f(\tau)$ for $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma(N) = \left\{\begin{pmatrix}a&b\\c&d\end{pmatrix} : \begin{pmatrix}a&b\\c&d\end{pmatrix}\equiv\begin{pmatrix}1&0\\0&1\end{pmatrix} \bmod N\right\}$.
2. Fourier expansion of $f\left(\frac{a\tau+b}{c\tau+d}\right)$ should be of form $\sum_{n\in\mathbb{Z}} c(n)q^n$, with $c(n)=0$ for $n<0$, for all $\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{Z})$.

   (All conjugates of f under $SL_2(\mathbb{Z})$ are holomorphic at $i\infty$).

If f is a modular form of level N, then $f(n\tau)$ is a modular form of level nN. So union of all modular forms of all levels $N\geq 1$ is closed under $f(\tau)\to f(n\tau)$, more generally, closed under $f(\tau)\to f\left(\frac{a\tau+b}{d}\right)$ for any $a,b,d\in\mathbb{Z}$.

We extend Peterson inner product to this larger space. Define:

$$(f,g) = \frac{1}{|\Gamma(1):\Gamma(N)|}.\int_{\Gamma(N)\backslash H} f(\tau)\overline{g(\tau)}.\,\mathrm{Im}(\tau)^{k-2}\,dx\,dy,$$

N chosen so that f,g are modular forms for $\Gamma(N)$. Have to check this does not depend on N.

Suppose f,g are modular forms for $\Gamma(N)$ and $\Gamma(M)$. We may assume $M|N$ (otherwise compare M with MN and N with MN). If $M|N$ then $\Gamma(N)\subseteq\Gamma(M)$. Find domain for $\Gamma(M)$ = union of $\left|\frac{\Gamma(M)}{\Gamma(N)}\right|$ fundamental domains for $\Gamma(N)$, so $\frac{1}{|\Gamma(1):\Gamma(N)|}\int_{\Gamma(N)\backslash H} * = \frac{1}{|\Gamma(1):\Gamma(N)|}\int_{\Gamma(M)\backslash H} \times\frac{1}{|\Gamma(M)/\Gamma(N)|} * = \frac{1}{|\Gamma(1):\Gamma(M)|}.\int_{\Gamma(M)\backslash H} *.$

Now look at action of matrices in $GL_2(\mathbb{Q})^+$ on this space. ($+ \leftrightarrow \det > 0$).

Suppose $\alpha \in GL_2(\mathbb{Q})^+$, $f \in$ modular forms of some level. Define $f|_\alpha$ by $f|_\alpha(\tau) = f\left(\frac{a\tau+b}{c\tau+d}\right).(c\tau+d)^{-k}.\det\begin{pmatrix} a & b \\ c & d\end{pmatrix}^{k/2}$ for $\alpha \in GL_2(\mathbb{Q})^+$, $= \begin{pmatrix} a & b \\ c & d\end{pmatrix}$.

$f|_\alpha \overset{\uparrow}{=} f$ for $\alpha = \begin{pmatrix} * & 0 \\ 0 & *\end{pmatrix}$.

$f|_\alpha = f$ for all $\alpha \in SL_2(\mathbb{Z})$ just says f is a modular form for $SL_2(\mathbb{Z})$.

Similarly, functions fixed by action of $\Gamma(N)$ are just modular forms of level N.

Theorem: The action of $GL_2(\mathbb{Q})^+$ on space of cusp forms of all levels is unitary - ie $(f|_\alpha, g|_\alpha) = (f,g)$.

Look at $(f,g) = \int f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^{k-2}\,dx\,dy$.

Look at action of $\alpha \in GL_2(\mathbb{Q})^+$ on this:

$$\left.\begin{aligned} f|_\alpha(\tau) &= f(\alpha\tau)\,(c\tau+d)^{-k}.(\det\alpha)^{k/2} \\ \overline{g|_\alpha(\tau)} &= \overline{g(\alpha\tau)}.\overline{(c\tau+d)}^{-k}.(\det\alpha)^{k/2}. \end{aligned}\right\} \Rightarrow f|_\alpha\overline{g|_\alpha} = f(\alpha\tau)\overline{g(\alpha\tau)}\,|c\tau+d|^{-2k}(\det\alpha)^k$$

$$d(\alpha\tau) = (c\tau+d)^{-2}.(\det\alpha).d\tau \quad . \quad d(\alpha\bar\tau) = \text{complex conjugate.}$$

$\Rightarrow d\tau\wedge d\bar\tau = (c\tau+d)^2\overline{(c\tau+d)}^2.(\det\alpha)^2\,d(\alpha\tau)\wedge d(\alpha\bar\tau)$

$\mathrm{Im}(\alpha\tau) = \mathrm{Im}(\tau).\det(\alpha)\times|c\tau+d|^{-2}$. $\Rightarrow \mathrm{Im}\tau = \mathrm{Im}\,\alpha\tau.(\det\alpha)^{-1}.|c\tau+d|^2$

$f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^{k-2}\,dx\,dy$ invariant under action of $GL_2(\mathbb{Q})^+$. For: $f|_\alpha\overline{g|_\alpha}\,(\mathrm{Im}\tau)^{k-2}\,d\tau\wedge d\bar\tau$

$= f(\alpha\tau)\overline{g(\alpha\tau)}.(\mathrm{Im}\,\alpha\tau)^{k-2}\,d(\alpha\tau)\wedge d(\alpha\bar\tau)$

This appears to imply $(f,g) = (f|_\alpha, g|_\alpha)$.

The adjoint of $\begin{pmatrix} a & b \\ c & d\end{pmatrix} \in GL_2(\mathbb{Q})^+$ is $\begin{pmatrix} d & -b \\ -c & a\end{pmatrix} = \det\begin{pmatrix} a & b \\ c & d\end{pmatrix}.\begin{pmatrix} a & b \\ c & d\end{pmatrix}^{-1}$.

Proof: $(f|_\alpha, g) = (f, g|_{\alpha^{-1}})$ (as α is unitary).

$= (f, g|_{\det\alpha.\alpha^{-1}})$ (as $\det\alpha$ acts trivially).

and $\det\alpha.\alpha^{-1} = \begin{pmatrix} d & -b \\ -c & a\end{pmatrix}$ if $\alpha = \begin{pmatrix} a & b \\ c & d\end{pmatrix}$.

Corollary: Suppose f, g level 1 modular forms of $SL_2(\mathbb{Z})$. Then $(f|_\alpha, g)$ depends only on double coset $\Gamma\alpha\Gamma$, where $\Gamma = SL_2(\mathbb{Z})$.

Proof: $\beta \in SL_2(\mathbb{Z})$. Suppose $(f|_{\beta\alpha}, g) = (f|_\beta|_\alpha, g) = (f|_\alpha, g)$, as $f|_\beta = f$.

$(f|_{\alpha\beta}, g) = (f, g|_{(\alpha\beta)^{-1}}) = (f, g|_{\beta^{-1}}|_{\alpha^{-1}}) = (f, g|_{\alpha^{-1}}) = (f|_\alpha, g)$

Summary: Hecke operators acting on space of cusp forms.

Peterson inner product: $(f,g) = \int_{SL_2(\mathbb{Z})\backslash H} f(\tau)\overline{g(\tau)}.\mathrm{Im}(\tau)^{k-2}\,dx\,dy$.

Want to prove $T_k(n)$ self-adjoint. Enlarge space of cusp forms to ∞-dimensional space of cusp forms for some subgroup $\Gamma(N) = \left\{\begin{pmatrix} a & b \\ c & d\end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1\end{pmatrix} \bmod N\right\}$. We defined action of $GL_2(\mathbb{Q})^+$ on this space by $f|_\alpha(\tau) = f(\alpha\tau)(c\tau+d)^{-k}.(\det\alpha)^{k/2}$

Main result: Hermitian adjoint of α is α^{-1}. (So we have a unitary representation of $GL_2(\mathbb{Q})^+$).

Corollary: Adjoint of $\begin{pmatrix} a & b \\ c & d\end{pmatrix}$ is $\begin{pmatrix} d & -b \\ -c & a\end{pmatrix} = \det\begin{pmatrix} a & b \\ c & d\end{pmatrix}\times\begin{pmatrix} a & b \\ c & d\end{pmatrix}^{-1}$.

Corollary: If f, g cusp forms for $SL_2(\mathbb{Z})$, then $(f|_\alpha, g)$ depends only on coset $\Gamma\alpha\Gamma$ ($\Gamma = SL_2(\mathbb{Z})$).

$$\begin{aligned}(T_k(p)f, g) &= \text{const.}\Big(\sum_{\alpha\in\Gamma\backslash M_p} f|_\alpha, g\Big) = \text{const.}(p+1).\Big(f|_{\begin{pmatrix} p & 0 \\ 0 & 1\end{pmatrix}}, g\Big) = \text{const.}(p+1)\Big(f, g|_{\begin{pmatrix} 1 & 0 \\ 0 & p\end{pmatrix}}\Big) \\ &= \text{const.}\Big(f, \sum_{\alpha\in\Gamma\backslash M_p} g|_\alpha\Big) = (f, T_k(p)g)\end{aligned}$$

So $T_k(p)$ is self-adjoint for p prime.

$T_k(p)$ generate algebra of all $T_k(m)$'s, so $T_k(m)$ is self-adjoint for all m.

Application 1: Hecke algebra generated by all $T_k(m)$'s is commutative and closed under taking adjoints, so its action on cusp forms is diagonalisable. We can find a canonical basis for space of cusp forms given by eigenvectors of form $q + O(q^2)$

$\uparrow$ normalise so that coefficient of q is 1.

We check that eigenspace of Hecke algebra is one-dimensional.
Suppose we have two eigenforms: $f(\tau) = \sum c(n) q^n$, $g(\tau) = \sum c(n)' q^n$.
$T_k(m) f = \lambda_m f$, $T_k(m) g = \lambda_m g$ for all m. Using fact that $c(1)\lambda_m = c(m)$, $c(1)'\lambda_m = c(m)'$, we see f, g are proportional. So all eigenspaces are one-dimensional.

We can also find structure of Hecke algebra (over $\mathbb{C}$) = algebra over $\mathbb{C}$ generated by action of Hecke operators on cusp forms (of weight k).
If any algebra A acts on a finite-dimensional vector space V, so that V is the direct sum of one-dimensional eigenspaces, then $A = \mathbb{C} \times \cdots \times \mathbb{C}$ (one copy for each eigenvector).
[Isomorphism: $A \to \mathbb{C} \times \cdots \times \mathbb{C}$
$a \mapsto$ (eval. of v_1, .., eval. of v_r), $v_1, v_2, ..$ a basis of V consisting of eigenvectors)]

So Hecke algebra = $\oplus \mathbb{C}$, number of copies = dimension of space of cusp forms.

Warning: in higher levels (eg. cusp forms for some group other than $SL_2(\mathbb{Z})$, say $\Gamma(N)$), Hecke operators are not always self-adjoint.
For $\Gamma(N)$ we find Hecke operators $T_k(m)$ are self-adjoint only for $(m, N) = 1$.
Algebra generated by $T_k(m)$ for $(m, N) = 1$ are commutative, self-adjoint, but eigenspaces are not always one-dimensional.

Remark: Wiles' proof of Fermat's Last Theorem was largely about structure of some Hecke algebra: Look at cusp forms of weight 2, of some level $N > 1$. Look at algebra over $\mathbb{Z}$ generated by (some) Hecke operators and a few other operators.
Need to know structure of this algebra, after completing and localising it.
Eg: Taylor-Wiles proved this algebra was a complete intersection.

Summary: of all useful properties of Hecke operators (on forms of weight k).

1. $T_k(m) f = m^{k-1} \cdot \sum_{\substack{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right), a>0 \\ ad = m, 0 \le b < d}} f\left(\frac{a\tau + b}{d}\right) = \sum_n q^n . \sum_{a \mid (m,n)} \left(\frac{m}{a}\right)^{k-1} . c\left(\frac{mn}{a^2}\right)$.

2. $T(m)T(n) = T(mn)$ if $(m,n) = 1$.
$T(p^n)T(p) = T(p^{n+1}) + p^{k-1} T(p^{n-1})$ $\Big\}$ $\Rightarrow$ Hecke algebra is commutative.

3. $(f, g) = \int_{SL_2(\mathbb{Z}) \backslash H} f(\tau) \overline{g(\tau)} . \mathrm{Im}(\tau)^{k-2} \, dx \, dy$. $T_k(m)$ self-adjoint: $(T_k(m) f, g) = (f, T_k(m) g)$

4. Cusp forms have basis of eigenforms of Hecke algebra.

5. If $f(\tau) = \sum c(n) q^n$ with $c(1) = 1$ is eigenform, eigenvalues of $T_k(m)$ are $c(m)$.
(So, $c(m) c(n) = c(mn)$ if $(m,n) = 1$, $c(p^n) c(p) = c(p^{n+1}) + p^{k-1} c(p^{n-1})$)

Hecke operators acting on modular functions.
Recall $T_0(2)(j)$ = const. $\left(j(2\tau) + j(\tau/2) + j\left(\frac{\tau+1}{2}\right)\right)$ = polynomial in $j(\tau)$.
(We cannot find eigenvalues of Hecke operators on modular functions. If $f(\tau) = q^{-n} + \cdots$, then $T_0(m) f(\tau) = q^{-mn} + \cdots$).

Problem: We want to write each $T_0(m)\, j(\tau)$ "explicitly" as a polynomial in $j(\tau)$.

Look at $\sum_m p^m . T_0(m). (j(\tau) - 744)$ = "generating function" for $T_0(m)$.

- easier to study all $T_0(m)\, j$'s together than to study just one.

$$j(t) - 744 = \sum_n c(n)\, q^n, \quad q = e^{2\pi i \tau}.$$

$$\sum_{m>0} T_0(m). (j(t) - 744)\, p^m = \sum_{m>0} T_0(m). \Big(\sum_n c(n) q^n\Big) p^m = \sum_{m>0} \sum_{n\in\mathbb{Z}} \sum_{a|(m,n)} \tfrac{1}{a} . c\Big(\tfrac{mn}{a^2}\Big) . p^m . q^n$$

$$= \sum_{m>0} \sum_{n\in\mathbb{Z}} \sum_a \tfrac{1}{a}\, c(mn)\, p^{ma}\, q^{na} \quad \text{(replacing } m, n \text{ by } ma, na).$$

$$= \sum_{m>0} \sum_{n\in\mathbb{Z}} - \big(\log(1 - p^m q^n)\big) . c(mn)$$

$$= \log\Big(\prod_{\substack{m>0\\ n\in\mathbb{Z}}} (1 - p^m q^n)^{c(mn)}\Big)^{-1}$$

$\nwarrow$ we will calculate this product explicitly.

We now show $f(\sigma, \tau) := p^{-1} \prod_{m>0} . \prod_{n\in\mathbb{Z}} (1 - p^m q^n)^{c(mn)} = j(\sigma) - j(\tau)$, $p = e^{2\pi i \sigma}$, $q = e^{2\pi i \tau}$.

Properties of $f(\sigma, \tau)$:

1. $f(\sigma, \tau) = - f(\tau, \sigma)$

$f(\sigma, \tau) = p^{-1} (1 - pq^{-1}) . \prod_{\substack{m>0\\ n>0}} (1 - p^m q^n)^{c(mn)}$ (Only non-trivial term for $n < 0$ is $n = -1, m = 1$. $c(-1) = 1$).

$= (p^{-1} - q^{-1}) \times$ (symmetric in p, q).

2. $f(\sigma, \tau) = \sum_m p^m \times$ (modular function of τ)

Proof: $f(\sigma, \tau) = p^{-1} . \exp\big(\sum_{m>0} p^m \times T_0(m) . \text{(modular function of } \tau)\big)$

3. $f(\sigma, \tau) = p^{-1} - q^{-1} + \sum_{\substack{m\geq 0\\ n\geq 0}} a(m,n)\, p^m q^n$, $a(0,0) = 0$.

Proof: Multiply out first few terms.

These three properties characterise $f(\sigma, \tau)$.

Proof: Suppose f_1, f_2 are two functions with these properties.

Then $g(\sigma, \tau) = f_1(\sigma, \tau) - f_2(\sigma, \tau)$ has same properties, except that $g(\sigma, \tau) = \sum_{\substack{m\geq 0\\ n\geq 0}} a(m,n) p^m q^n$.

For each fixed m, $\sum_{n\geq 0} a(m,n) p^m q^n$ is a modular function by property 2.

So $\sum_{n\geq 0} a(m,n) q^n$ is constant (as any modular function with no poles is constant).

So $a(m,n) = 0$ if $n > 0$.

Using property 1, $f(\sigma, \tau) = - f(\tau, \sigma)$, we see $a(m,n) = 0$ if $m > 0$.

We know $a(0,0) = 0$, so $a(m,n) = 0$ for all m, n. So $f_1 = f_2$.

Note that $f_2(\sigma, \tau) = j(\sigma) - j(\tau)$ has same three properties. (Trivial to check).

So $p^{-1} \prod_{\substack{m>0\\ n\in\mathbb{Z}}} (1 - p^m q^n)^{c(mn)} = j(\sigma) - j(\tau)$.

On modular forms, we can find eigenvectors for the Hecke operators. On modular functions, eigenvectors do not exist, but instead we can say that $T(m)(j(\tau))$ = polynomial in $j(\tau)$.

Look at $\sum_{m>0} p^m T(m) (j(t) - 744) = - \log\big(\prod_{\substack{m>0\\ n\in\mathbb{Z}}} (1 - p^m q^n)^{c(mn)}\big)$. $j(\tau) - 744 = \sum c(n) q^n . = q^{-1} + 196884 q + \dots$

We also found $p^{-1} \prod_{\substack{m>0\\ n\in\mathbb{Z}}} (1 - p^m q^n)^{c(mn)} = j(\sigma) - j(\tau)$, $q = e^{2\pi i \tau}$, $p = e^{2\pi i \sigma}$.

Both sides satisfy:

$$\left.\begin{array}{l} \text{(i) } f(\sigma, \tau) = - f(\tau, \sigma) \\ \text{(ii) } f \text{ modular function in } \tau \\ \text{(iii) } f(\sigma, \tau) = p^{-1} - q^{-1} + \text{(non-singular)} \end{array}\right\} \text{unique function with these properties.}$$

Putting these together we get: $\sum_{m>0} p^m . T(m).(j(\tau)-744) = -\log\,(p(\overset{\nearrow = p^{-1}+\cdots}{j(\sigma)}-j(\tau)))$

$$= -\log\,(1 - p(j(\tau)-744) + p^2c(1) + p^3c(2) + p^4c(3) + \cdots)$$

So $T(m)(j-744)$ = coefficient of p^m in $(p(j-744)-p^2c(1)-p^3c(2)-\cdots) + (\cdots)^2/2 + (\cdots)^3/3 + \cdots$

Example: Take $m=2$. We must obtain the coefficient of p^2 in the above.

This coefficient is: $-c(1) + \frac{(j-744)^2}{2}$ = polynomial in $j(\tau)$.

Remark: Look at two formulas: $j(\sigma)-j(\tau) = p^{-1}\prod_{\substack{m>0\\ n\in\mathbb{Z}}}(1-p^mq^n)^{c(mn)}$.

Kac-Weyl denominator for simple Kac-Moody algebra: $\sum_{w\in W}\det(w)e^{w(\rho)} = e^{\rho}.\prod_{\alpha>0}(1-e^{\alpha})^{\mathrm{mult}(\alpha)}$

- denominator formula for a Lie algebra called the Monster Lie algebra.

Properties: (i) Monster Lie algebra = space of states of chiral string on orbitals of 26-d torus.

(ii) Monster simple group acts "nicely" on Monster Lie algebra.

Gap in theory of modular forms - Peterson inner product.

Peterson inner product only works for cusp forms: Look at $(f,g) = \int_{SL_2(\mathbb{Z})\backslash H} f(\tau)\overline{g(\tau)}\,.\,\mathrm{Im}(\tau)^{k-2}\,dx\,dy$.

Why does this converge?

Only problem is when $y\to+\infty$, $y=\mathrm{Im}(\tau)$, $y^{k-2}\to\infty$. f,g certainly bounded as $y\to\infty$.

if $f(\tau) = c(1)q+\cdots$ is a cusp form then $f(\tau) = O(q) = O(e^{-2\pi y})$ as $y\to\infty$, so $\int$ converges.

Modular Forms and Dirichlet Series.

A Dirichlet Series is one of the form $\sum_{n>0}\frac{c(n)}{n^s}$, $s\in\mathbb{C}$.

Suppose $c(n) = O(n^a)$, then $\frac{c(n)}{n^s} \leq \mathrm{const.}\times n^{a-s}$, so convergent if $\mathrm{Re}(s)>a+1$ ($\sum\frac{1}{n^s}$ converges if $\mathrm{Re}(s)>1$).

"Simplest" example: $\zeta(s) = \sum\frac{1}{n^s}$, converges for $\mathrm{Re}(s)>1$. $\zeta(s)$ extends to a meromorphic function for all $s\in\mathbb{C}$.

Properties: (i) Euler Product: $\zeta(s) = \prod\frac{1}{(1-p^{-s})} = (1+2^{-s}+4^{-s}+\cdots)(1+3^{-s}+9^{-s}+\cdots)(1+5^{-s}+25^{-s}+\cdots)$

$= \sum_{n_1,n_2,\dots}(2^{n_1 s}.3^{n_2 s}\cdots)^{-1} = \sum\frac{1}{n^s}$ - fundamental theorem of arithmetic.

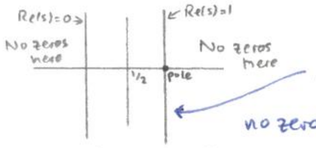
(ii) Functional Equation: Put $\zeta^*(s) = \pi^{-s/2}.\Gamma(s/2).\zeta(s)$. Then, $\zeta^*(1-s) = \zeta^*(s)$. (Proof later).

$\Gamma(s) = \int_0^\infty e^{-t}.t^{s-1}dt$, $\mathrm{Re}(s)>0$. $s\Gamma(s) = \Gamma(s+1)$.

(iii) Riemann hypothesis: All zeros of $\zeta(s)$ (other than $s=-2n$) have real part $1/2$.

$\prod(1-p^{-s})^{-1}$ converges for $\mathrm{Re}(s)>1$, so $\zeta(s)$ has no zeros for $\mathrm{Re}(s)>1$.

Using $\zeta^*(1-s) = \zeta^*(s)$ this shows that $\zeta(s)$ has no zeros for $\mathrm{Re}(s)<0$ except for "trivial" zeroes coming from poles of $\Gamma(s)$.



de la Valleé Poussin, Hadamard, proved no zeros with $\mathrm{Re}(s)=1 \Rightarrow$ Prime Number Theorem.

Computer calculations have shown that first 3×10^4 zeros of $\zeta(s)$ have $\mathrm{Re}(s) = 1/2$.

Question: How can computer calculation show that the real part of a zero is exactly $\frac{1}{2}$?

Answer: Instead of looking at $\zeta(s)$, look at $\zeta^*(s)$ (same zeros for $\mathrm{Re}(s)\geq 0$).

$\zeta^*(1-s) = \zeta^*(s)$. $\zeta^*(\bar{s}) = \overline{\zeta^*(s)}$. $\zeta(s)$ for real s.

$$\left.\begin{aligned}\zeta^*(\tfrac12+it) &= \overline{\zeta^*(\tfrac12-it)}\\ &\shortparallel\\ \zeta^*(1-(\tfrac12-it)) &= \zeta^*(\tfrac12-it)\end{aligned}\right\}\text{ so }\zeta^*(\tfrac12+it)\text{ is real.}$$

So if $\zeta^*(\frac12+it_1)>0$, $\zeta^*(\frac12+it_2)<0$, there is a zero of $\zeta(s)$ with $\mathrm{Re}(s)=\frac12$, $t_1<\mathrm{Im}(s)<t_2$.

Suppose $\sum_{n>0} \frac{c(n)}{n^s}$ is any Dirichlet series. When does this have Euler product of form $\prod_{p>0}$ (polynomial in p^{-s}, constant term $=1)^{-1}$?

1. $\sum \frac{c(n)}{n^s} = \prod_p \left(\sum \frac{c(p^k)}{p^{ks}}\right)$ is equivalent to $c(p_1^{n_1} p_2^{n_2} \ldots) = c(p_1^{n_1}) c(p_2^{n_2}) \ldots$
   In other words, $c(mn) = c(m)c(n)$ if $(m,n)=1$.
2. Suppose $\sum \frac{c(p^k)}{p^{ks}} = (1 + a(1)p^{-s} + \cdots + a(j)p^{-js})^{-1}$. This is equivalent to $\left(\sum_i^j a(i)p^{-is}\right)\left(\sum c(p^k)/p^{ks}\right) = 1$.
   In other words, $c(p^n) + a(1)c(p^{n-1}) + a(2)c(p^{n-2}) + \cdots = 0$

Recall that if $\Delta(\tau) = \sum_n \tau(n) q^n$ we showed that

1. $\tau(mn) = \tau(m)\tau(n)$ if $(m,n)=1$.
2. $\tau(p^n) = \tau(p)\tau(p^{n-1}) - p^{11}\tau(p^{n-2})$.

- equivalent to saying $\sum_n \frac{\tau(n)}{n^s} = \prod_p (1 - \tau(p)p^{-s} + p^{11}.p^{-2s})^{-1}$

Similarly if $\sum c(n)q^n$ is any eigenform of weight k for Hecke operators then $\sum \frac{c(n)}{n^s} = \prod_p (1 - c(p)p^{-s} + p^{2k-1-2s})^{-1}$. no ??

Check to see where $\sum \frac{c(n)}{n^s}$ converges; we need some bound $c(n) = O(n^*)$.

Easy to show $c(n) \leq n^{k+\varepsilon}$ using the fact that this is true for $E_k(\tau) = 1 + \text{const.}\left(\sum_n \sigma_{k-1}(n) q^n\right)$, $\sigma_{k-1}(n) = O(n^{k-1+\varepsilon})$.

We will prove a stronger bound: $c(n) = O(n^{k/2})$. ($\underline{\text{Eg}}$: $\tau(n) \leq \text{const.}\, n^6$).

$\underline{\text{Proof}}$: If $f(\tau) = \sum_n c(n) e^{2\pi i n\tau}$ then $c(n) = \int_{ai}^{ai+1} e^{-2\pi i n \tau} f(\tau)\, d\tau$ for any real $a>0$

$$\leq e^{2\pi n a} . \max_{\operatorname{Im}\tau = a} |f(\tau)|.$$

$\underline{\text{Lemma}}$: $|f(\tau)\overline{f(\tau)}.\operatorname{im}(\tau)^k|$ is bounded for $\operatorname{Im}(\tau)>0$ if f is a cusp form of weight k.

$\underline{\text{Proof}}$: (i) This is bounded in fundamental domain for $SL_2(\mathbb{Z})$ as $|f(\tau)| \to 0$ rapidly as $\operatorname{Im}(\tau) \to \infty$.

(ii) This function is invariant under $SL_2(\mathbb{Z})$ - so bounded on H.

$\underline{\text{Corollary}}$: $|f(\tau)| \leq \text{const.} \times \operatorname{Im}(\tau)^{-k/2}$, f a cusp form of weight k.

Substitute this bound in expression for $c(n)$: Find $c(n) \leq \text{const.} \times e^{2\pi n a} \times a^{-k/2}$ for any $a>0$.

Choose a to give best bound: minimum of $e^{2\pi n a} . a^{-k/2}$ is close to $a = 1/n$.

$c(n) \leq \text{const.} \times e^{2\pi} \times \left(\frac{1}{n}\right)^{-k/2} = \text{const.}\, n^{k/2}$, so $c(n) = O(n^{k/2})$.

$\underline{\text{Remark}}$: Ramanujan conjecture (proved by Deligne): $\tau(n) = O(n^{k/2 - \frac{1}{2} + \varepsilon})$.

$\underline{\text{Gamma Function: } \Gamma(s)}$.

Defined for $\operatorname{Re}(s)>0$ by $\Gamma(s) = \int_0^\infty e^{-t} t^{s-1}\, dt$ (Euler)

$\Gamma(s+1) = s\Gamma(s)$, $\Gamma(1) = 1$, so $\Gamma(1+m) = m!$

$\Gamma(s) = \int_0^\infty e^{-t} t^{s-1}\, dt = \left[-e^{-t}.\frac{t^s}{s}\right]_0^\infty + \int_0^\infty e^{-t}.\frac{t^s}{s}\, dt = \frac{1}{s}\int_0^\infty e^{-t}.t^s dt = \frac{1}{s}\Gamma(s+1)$.

Define $\Gamma(s)$ for $\operatorname{Re}(s) > -1$ by $\Gamma(s) = \frac{\Gamma(s+1)}{s}$. Same as original definition for $\operatorname{Re}(s)>0$ by functional equation.

$\Gamma(s)$ holomorphic for $\operatorname{Re}(s) > -1$ except for a pole at $s=0$. Define for $\operatorname{Re}(s) > -2$ by $\Gamma(s) = \frac{\Gamma(s+1)}{s}$.

Continue like this: $\Gamma(s)$ holomorphic for all $s \in \mathbb{C}$, except for poles $s = 0, -1, -2, \ldots$

$\Gamma(s) = \int_0^\infty e^{-t}.t^s.\left(\frac{dt}{t}\right)$ $\xrightarrow{}$ invariant under $t \mapsto at$. Change to $2\pi n t$: $\Gamma(s) = \int_0^\infty e^{-2\pi n t}.(2\pi n)^s.t^s.\frac{dt}{t}$.

$\underbrace{(2\pi)^{-s}.\Gamma(s).\sum \frac{c(n)}{n^s}}_{\text{Dirichlet Series}} = \int_0^\infty \sum_n (c(n)e^{-2\pi n t}).t^s.\frac{dt}{t}$ — power series in $q = e^{-2\pi t}$.

- order of sum and integral can be interchanged for $\operatorname{Re}(s)>a$ if $c(n) = O(n^{a-1})$

Remark: The function $g(s) = \int_0^\infty f(t).t^{s-1}\,dt$ is called the Mellin transform of $f(t)$.

Put $c(n) = \tau(n)$. So, $\sum c(n)e^{-2\pi n t} = \sum \tau(n)q^n = \Delta(it)$.

Put $L_\Delta(s) = \sum_n \frac{\tau(n)}{n^s}$. Then $\underbrace{(2\pi)^{-s}\Gamma(s).L_\Delta(s)}_{L^*_\Delta(s)} = \int_0^\infty \Delta(it).t^{s-1}\,dt$ ← This integral converges for all $s\in\mathbb{C}$ so $L^*(s)$ holomorphic for all $s\in\mathbb{C}$.

What does the functional equation $\Delta(i/t) = t^{12}\Delta(it)$ imply about $L_\Delta(s)$?

$L^*(12-s) = \int_0^\infty \Delta(it)\,t^{12-s-1}\,dt$

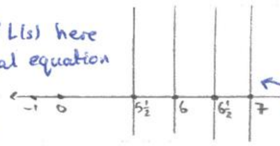
Change t to $\frac{1}{t}$: $\int_0^\infty \Delta(\frac{i}{t}).t^{s-12}.\frac{dt}{t} = \int_0^\infty \Delta(it).t^{s}\times.\frac{dt}{t} = L^*(s)$

Thus, $L^*(12-s) = L^*(s)$

Properties of $L(s) = \sum\frac{\tau(n)}{n^s} = \prod_p \underbrace{(1-p^{-s}\tau(p)+p^{11-2s})^{-1}}$

infinite product converges for $\mathrm{Re}(s) > 7$ as $\tau(p) = O(p^6)$

So $L(s)$ has no zeros for $\mathrm{Re}(s) > 7$. (Use Deligne's estimate: $\tau(p) \leq 2p^{11/2}$. See that there are no zeros for $\mathrm{Re}(s) > 6\frac{1}{2}$)



No zeroes of $L(s)$ here by functional equation except at poles of $\Gamma(s)$, $0,-1,-2,..$

no zeroes here by ∞ product.

$L^*(s) = (2\pi)^{-s}.L(s).\Gamma(s)$.

↑ holomorphic, so if $\Gamma(s)$ has a pole, $L(s)=0$. So $L(s)=0$ at $0,-1,-2,..$ So all non-trivial zeros of $L(s)$ have $5\frac{1}{2} \leq \mathrm{Re}(s) \leq 6\frac{1}{2}$. $L^*(s)$ is real for $\mathrm{Re}(s)=6$ as $L^*(\bar{s}) = \overline{L^*(s)}$, and $L^*(12-s) = L^*(s)$, so $L^*(6+it) = \overline{L^*(6+it)}$.

Riemann hypothesis for $L_\Delta(s)$: all zeros of $L_\Delta(s)$ have $s = 0,-1,-2,\cdots$ or $\mathrm{Re}(s)=6$.

Similarly, if $\sum c(n)q^n$ is any eigenform and cusp form of Hecke operators of weight k.

Then put $L(s) = \sum\frac{c(n)}{n^s}$. Then $L(s) = \prod(1-c(p)p^{-s}+p^{k-1-2s})^{-1}$

$L^*(k-s) = L^*(s)$. $L^*(s) = (2\pi)^{-s}\Gamma(s)L(s)$. Deligne: $c(n) = O(n^{(k-1)/2}) \Rightarrow$ all zeros have $|\mathrm{Re}(s) - k/2| < 1/2$.

Riemann hypothesis: all zeros lie on $\mathrm{Re}(s) = k/2$.

Look at function $\theta(\tau) = \sum_n q^{n^2/2} = 1 + 2q^{1/2} + 2q^2 + 2q^{9/2} + \ldots$

Recall that we've proved $\theta(-\frac{1}{\tau}) = (\tau/i)^{1/2}.\theta(\tau)$.

Look at Mellin transform of $\theta(it)$. $\int_0^\infty (1 + 2\sum_{n>0} q^{n^2/2})t^{s-1}\,dt$, $q = e^{-2\pi t}$

?↙ ↳ $2\Gamma(s).(2\pi)^{-s}.\frac{1}{(n^2/2)^s}$

So Mellin transform of $\theta(it)$ appears to be

$$2\sum_{n>0}\Gamma(s)(2\pi)^{-s}.\frac{1}{n^{2s}}.2^s = 2\Gamma(s).\pi^{-s}\zeta(2s) = 2\zeta^*(2s)$$

Functional equation $\theta(i/t) = t^{1/2}\theta(it)$ should imply $\zeta^*(2(\frac{1}{2}-s)) = \zeta^*(2s)$, ie $\zeta^*(1-2s) = \zeta^*(2s)$

When does $\int_0^\infty \theta(it)t^{s-1}\,dt$ converge?

For t large, $\theta(it) \doteq 1$ + small terms. $\int^\infty 1\times t^{s-1}\,dt$ converges for $\mathrm{Re}(s) < 0$.

For t small, $\theta(it) = t^{-1/2}\theta(i/t) \simeq t^{-1/2}$. $\int_0 \theta(it)t^{s-1}\,dt \simeq \int_0 t^{s-3/2}\,dt$ converges for $\mathrm{Re}(s) > 1/2$.

The integral converges for no values of s!

$2\zeta^*(2s)$ is not the Mellin transform of $\theta(it)$, but $\underbrace{\theta(it)-1}$

tends to 0 rapidly as $t\to\infty$, so for $\mathrm{Re}(s)$ large (in fact $\mathrm{Re}(s) > \frac{1}{2}$)

Define $f(it) = \begin{cases} \theta(it) - 1 & \text{for } t>1 \\ \theta(it) - t^{-1/2} & \text{for } t<1 \end{cases}$ $f(it) \to 0$ rapidly as $t \to \infty$ or 0.

So $\int_0^\infty f(it)\, t^{s-1}\,dt$ converges for all $s \in \mathbb{C}$ to a holomorphic function.

Note $\int_0^\infty f(it)\, t^{s-1}\,dt$ is holomorphic for all s if f is continuous, and tends to zero rapidly (ie, super-polynomially) as $t \to \infty$, $t \to 0$.

$f(i/t) = t^{1/2} f(it)$.

$$2\zeta^*(2s) = \int_0^\infty (\theta(it)-1)\, t^s.\frac{dt}{t} = \underbrace{\int_0^\infty f(it)\, t^s.\frac{dt}{t}}_{\substack{\text{holomorphic } \forall s \in \mathbb{C} \\ \text{Invariant under } s \mapsto \frac{1}{2}-s}} + \underbrace{\int_0^1 (t^{-1/2}-1)\, t^s.\frac{dt}{t}}_{} \quad \text{for } Re(s) > 1/2$$

$= \int_0^1 t^{s-3/2} - t^{s-1}\,dt = \frac{1}{(s-\frac{1}{2})} - \frac{1}{s}$ for $Re(s) > 1/2$.

- extends to a meromorphic function invariant under $s \mapsto \frac{1}{2} - s$.

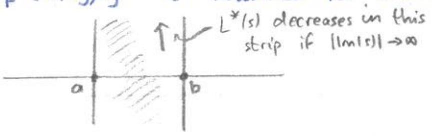
So this shows: (i) $\zeta^*(2s)$ can be extended to a meromorphic function of all $s \in \mathbb{C}$, whose only poles are at $s=0$, $s = \frac{1}{2} \to \theta(it)$ not a cusp form at $t=0$.

↑ $\theta(it)$ not a cusp form at $t=\infty$

(ii) $\zeta^*(2(\frac{1}{2}-s)) = \zeta^*(2s)$, so $\zeta^*(1-s) = \zeta^*(s)$, $\zeta^*(s) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$.

Hecke Converse Theorem.

If f is a cusp form then $L_f^*(s)$ is rapidly decreasing in vertical strips: ie, if $a<b$, $a,b \in \mathbb{R}$, then $L_f^*(x+iy)\,y^N$ is bounded for $a \le x \le b$.



– dull exercise.

Theorem: Image of cusp forms of weight k under $\Sigma c(n) q^n \to \Sigma \frac{c(n)}{n^s}$ is space of holomorphic functions on $\mathbb{C}$, $L(s)$ with following properties:

(i) $L(s)$ is a Dirichlet Series for $Re(s) \gg 0$.

(ii) If $L^*(s) = (2\pi)^{-s}\Gamma(s)L(s)$ then $L^*(k-s) = L^*(s)$

(iii) $L^*(s)$ decreases rapidly in vertical strips.

Proof: Recall that if $g(s) = \int_0^\infty f(t)\, t^{s-1}\,dt$ is Mellin transform, then $f(t) = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} g(s)\, t^{-s}\,ds$ is inverse Mellin transform, under suitable conditions on f and g.

(If we put $t = e^{iu}$ then these are formally Fourier transform and its inverse.)

Condition about $L^*(s)$ decreasing rapidly in strips implies we can define $f(\tau) = \int_{a-i\infty}^{a+i\infty} L^*(s).\frac{\tau}{i-s}\,ds$, for any real a.

Then $f(\tau) = \Sigma c(n) q^n$ (by taking a large and calculating using $L^*(s) = (2\pi)^{-s}\Gamma(s).\Sigma\frac{c(n)}{n^s}$).

So $f(\tau) = f(\tau+1)$. $L(s)$ is a Dirichlet series.

$L^*(k-s) = L^*(s) \Rightarrow f(\frac{-1}{\tau}) = \tau^k f(\tau)$ (Reverse of previous argument.

So $f(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^k f(\tau)$, for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ as $\tau \mapsto \tau+1$, $\tau \mapsto -1/\tau$ generate $SL_2(\mathbb{Z})$.

A few routine estimates (eg: $f(\tau) \to 0$ as $Im(\tau) \to \infty$) imply that $f(\tau)$ is a cusp form of weight k.

Langlands' Conjecture (vastly simplified version).

We have seen that a Dirichlet series with various nice properties comes from a modular form.

Langlands: Any 'reasonable' Dirichlet series in mathematics comes from an automorphic form (= generalisation of modular form) in a similar way.

Example: If V is an algebraic variety over $\mathbb{Q}$ then it has a zeta function $\zeta(s) = \prod_p \zeta_p(s)$.

$\zeta_p(s) = \zeta$-function of V reduced mod p. Coefficient of $\zeta_p(s)$ counts number of points of V over finite fields of order p^n.

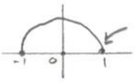
We expect that this zeta function is a Mellin transform of some automorphic form.

Special case: $V =$ elliptic curve, $\zeta(s)$ should be Mellin transform of a modular form of weight 2, level >1. This is Taniyama-Shimura-Weil conjecture, partly proved by Wiles.

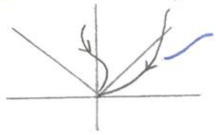
Example: We will "prove" that $L_\Delta(\tau)$ has infinitely many zeroes with $\mathrm{Re}(s) = 6$ (critical line).

Remark: similar proof shows $\zeta(s)$ has infinitely many zeros s with $\mathrm{Re}(s) = 1/2$.

Proof: Look at $L_\Delta(\tau)$ for $\tau \in$ unit circle close to 1 or -1



1. If $\tau \to 1$, $|\tau| = 1$, then $\Delta(\tau) \to 0$ very rapidly. We know $\Delta(\tau) \to 0$ rapidly as $\mathrm{Im}(\tau) \to +\infty$. $\Delta(-\frac{1}{\tau}) = \tau^{12}\Delta(\tau)$, so $\Delta(\tau) \to 0$ as $\tau \to 0$, provided τ in a sector.



note if $\tau \to 0$ along a strange path then $\Delta(\tau) \not\to 0$.

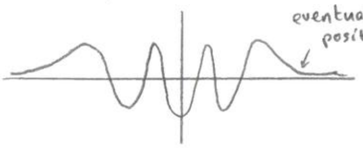
Similarly, $\Delta(\tau) \to 0$ rapidly as $\tau \to$ any cusp in a "sensible" way (ie τ in some sector).

We also know $\underset{\text{on unit circle}}{\Delta(ie^{iu})} = \frac{1}{2\pi i}\int_{a-i\infty}^{a+i\infty} L^*(s)(e^{ia})^{-s}\,ds$ (inverse Mellin).

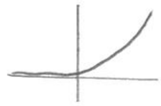
Take $a = 6$, u real, $-\frac{\pi}{2} < u < \frac{\pi}{2}$. $u \to \pm\frac{\pi}{2} \Rightarrow ie^{iu} \to \mp 1$.

Put $s = 6 + it$. We get $(\text{const})\int_{-\infty}^{\infty} L^*(6+it)(e^{iu})^{6+it}\,dt = (\text{const.})\int_{-\infty}^{\infty} L^*(6+it)e^{-ut}\,dt$.

Now suppose $L(6+it)$ has only finitely many zeros. $L^*(6+it)$ is real so it looks like



We are multiplying by e^{-ut}, u close to $-\pi/2$



$\int L^*(6+it)e^{-\frac{\pi}{2}t}\,dt$ diverges (otherwise $\Delta(\tau)$ is bounded for $\mathrm{Im}(\tau) > 0$ - contradiction).

So as $u \to -\pi/2$, $\int L^*(6+it)e^{-ut}\,dt \to \infty$ if $L^*(6+it) > 0$ for $t >> 0$. So this would imply $\Delta(ie^{iu}) \to \infty$ as $e^{iu} \to \pm 1$

Remark: Suppose we choose k so that space of cusp forms has dimension ≥ 2. Choose two cusp forms f_1, f_2, weight k. Previous argument shows $L_{af_1+bf_2}(s)$ has infinitely many zeros on critical line. But for suitable a, b $L_{af_1+bf_2}$ can be given a zero at any $s \in \mathbb{C}$.

Eg: $a = L^*_{f_2}(s_0)$, $b = -L^*_{f_1}(s_0)$, then $aL_{f_1}(s) + bL_{f_2}(s)$ has a zero at $s = s_0$.

Riemann hypothesis is false for such functions.

Riemann hypothesis seems to hold when $L(s)$ also has an Euler product.

Values of $j(\tau)$ for special values of τ. (or "why is $j(-\frac{1}{2} + \frac{i\sqrt{163}}{2})$ an integer?)

Recall $j(\tau) = E_4(\tau)^3/\Delta(\tau)$, $E_4\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k . E_4(\tau)$. Take $\tau = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ (= cube root of 1).

Then τ is fixed by element of order 3 is $SL_2(\mathbb{Z})$, which implies $E_4(-\frac{1}{2} + \frac{\sqrt{3}}{2}i) = 0$.

So $j(-\frac{1}{2} + \frac{\sqrt{3}}{2}i) = 0$.

We can evaluate $j(i)$ in a similar manner: $\Delta(\tau) = \dfrac{E_4(\tau)^3 - E_6(\tau)^2}{1728}$, so $j(\tau) = 1728 + \dfrac{E_6(\tau)^2}{\Delta(\tau)}$.

$E_6(i)=0$ as we know $E_6(\frac{-1}{\tau}) = \tau^6 E_6(\tau)$, and putting $\tau=i$ gives $E_6(i) = i^6 E_6(i) = -E_6(i)$.
So $j(i) = 1728$.
We know any point of H fixed by some element of $SL_2(\mathbb{Z})$ is conjugate to either i or $-\frac{1}{2}+\frac{\sqrt{3}}{2}i$.
So if τ is fixed by a 2×2 matrix of $\det = 1$, then $j(\tau)$ is an integer.
If τ is fixed by a 2×2 integral matrix, then $j(\tau)$ is an algebraic integer.

Properties of $j(\tau)$: Any modular function with no poles on H is a polynomial in $j(\tau)$. If the coefficients of $f(\tau) = \sum c(n) q^n$ are integers, then $f(\tau)$ is a polynomial in $j(\tau)$ with integral coefficients (Proof by induction on something...). They are awful integers though.

Recall:
$$\begin{tikzcd} j(\tau/2) \arrow[r, leftrightarrow, bend left] \arrow[rr, leftrightarrow, bend right=40] & j(\frac{\tau+1}{2}) \arrow[loop below] & j(2\tau) \arrow[loop below] \end{tikzcd}$$
are permuted by $SL_2(\mathbb{Z})$
: $\tau \mapsto \tau+1$
: $\tau \mapsto -1/\tau$.

So $j(\tau/2) + j(\frac{\tau+1}{2}) + j(2\tau) =$ modular function $(= \text{const.} \times T_2\, j(\tau))$

More generally, any symmetric function of $j(\tau/2)$, $j(\frac{\tau+1}{2})$, $j(2\tau)$ is also a modular function.
In particular,
$$\left.\begin{array}{l} j(\tau/2) + j(\frac{\tau+1}{2}) + j(2\tau) \\ j(\tau/2)\,j(\frac{\tau+1}{2}) + j(\frac{\tau+1}{2})\,j(2\tau) + j(2\tau)\,j(\tau/2) \\ j(\tau/2)\,j(\frac{\tau+1}{2})\,j(2\tau) \end{array}\right\}$$
are modular functions.

Take $x = j(\sigma)$. Now look at: $(j(\sigma) - j(\tau/2))(j(\sigma) - j(\frac{\tau+1}{2}))(j(\sigma) - j(2\tau))$
Properties: (i) This is a polynomial in $j(\sigma)$.
(ii) Coefficients are modular functions in τ with no poles on H, hence polynomials in $j(\tau)$.
So it is a polynomial $P(j(\sigma), j(\tau))$ in 2 variables over $\mathbb{C}$. This P is called the modular polynomial.

Now put $\sigma=\tau$: $(j(\tau) - j(\tau/2)).(j(\tau) - j(\frac{\tau+1}{2})).(j(\tau) - j(2\tau))$
(i) $(q^{-1} + \dots - q^{-1/2} + \dots)(q^{-1} + \dots - q^{1/2} \dots)(q^{-1} + \dots - q^{-2} \dots)$
$= q^{-4}$ + higher terms in q with integer coefficients
= polynomial in $j(\tau)$
$= -j(\tau)^4 + a(3)\,j(\tau)^3 + a(2)\,j(\tau)^2 + a(1)\,j(\tau) + a(0)$, $a(i) \in \mathbb{Z}$, possibly very big.

(ii) This polynomial vanishes if $j(\tau) = j(2\tau)$, $j(\tau/2)$, $j(\frac{\tau+1}{2})$
$j(\tau) = j(\tau/2) \iff \tau$ and $\tau/2$ are conjugate under $SL_2(\mathbb{Z})$.
$\iff \frac{a\tau+b}{c\tau+d} = \tau/2$.
Eg: $\tau = \sqrt{2}i$. Then $-\frac{1}{\tau} = \frac{1}{\sqrt{2}}i = \tau/2$. So modular polynomial vanishes if $\tau = \sqrt{2}i$.
So $j(\sqrt{2}i)$ is the root of a polynomial of degree 4 with integer coefficients and leading coefficient ±1.

Work out $j(\sqrt{2}i)$ using program gp (PARI on unix?).
$j(\sqrt{2}i) = 287485.9999\dots \overset{?}{=} 287496 = 2^3.3^3.11^3$
Why is $j(\sqrt{2}i)$ of degree 4 rather than degree 1?

Try to find other roots of modular polynomial.

Roots are points τ with $\frac{a\tau+b}{c\tau+d} = 2\tau, \frac{\tau+1}{2}, \tau/2$ with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

points with $\frac{a\tau+b}{c\tau+d} = \tau$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ having det 2, $a, b, c, d \in \mathbb{Z}$.

$\left[\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}; \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \right.$ are cost representatives for $\left. \frac{\text{det 2 matrices}}{\text{det 1 matrices}} \right]$

So roots are points τ with: $\underset{\overset{\shortparallel}{A}}{c}\tau^2 + \underset{\overset{\shortparallel}{B}}{(d-a)}\tau \underset{\overset{\shortparallel}{C}}{-b} = 0$, $ad-bc = 2$, $a, b, c, d \in \mathbb{Z}$.

Discriminant is $(d-a)^2 + 4bc \; (= B^2 - 4AC)$

$= (d+a)^2 - 4(ad-bc) = (d+a)^2 - 8 \geqslant -8$.

Discriminant <0 as τ not real.

So discriminant $= -8, \; 1^2-8 = -7, \; 2^2-8 = -4; \; 3^2 \cancel{-8} = 1$

Note: $(\sqrt{2}i)^2 + 2 = 0$, so discriminant $= -8$ in this case.

Suppose τ is a root of $A\tau^2 + B\tau + C = 0$, $A, B, C \in \mathbb{Z}$, coprime, $A>0$.

Define discriminant of τ to be $D := B^2 - 4AC$. Note $D<0$ if $\tau \in H$, and $D \equiv 0, 1 \bmod 4$.

So $D = -3, -4, -7, -8, -11, \ldots$

Problem: for fixed D, find all $\tau \in H$ of discriminant D.

If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, then $\frac{a\tau+b}{c\tau+d}$, τ have same discriminant.

Proof: Suppose $A\tau^2 + B\tau + C = 0$, $(A, B, C) = 1$.

Then $A - B(\frac{-1}{\tau}) + C(\frac{-1}{\tau})^2 = 0$, has same discriminant.

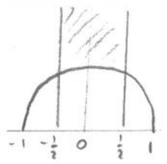
$A(\tau+1)^2 + B(\tau+1) + C = A\tau^2 + (2A+B)\tau + (A+B+C)$ - same discriminant.

So we try to find all $\tau \in$ fundamental domain of $SL_2(\mathbb{Z})$ of discriminant D.

What are conditions on A, B, C for $\tau \in$ fundamental domain?

$\tau = \frac{-B \pm \sqrt{B^2-4AC}}{2A}$. $\text{Re}\,\tau = \frac{-B}{2A} \Rightarrow |B| \leq A$ (Recall $A>0$).

$\tau\bar{\tau} = \frac{C}{A}$, so $|\tau| \geqslant 1 \Rightarrow A \leqslant C$.



So condition for a root τ of $A\tau^2 + B\tau + C$ to be in fundamental domain is: $|B| \leq A \leq C$.

Theorem: Fundamental Domain contains only a finite number of τ with discriminant D

Proof: (i) $|B| \leq A \leq C$

(ii) $B^2 - 4AC = D$ - fixed.

(iii) $A, B, C \in \mathbb{Z}$, $A>0$.

These equations have only a finite number of solutions:

$|B| \leq A$, $C \geqslant A \Rightarrow B^2 - 4AC \leq -3A^2$. So $3A^2 \leqslant -(B^2-4AC) = -D$.

$$\left.\begin{array}{l} \therefore \; |A| \leq \sqrt{-D/3} \Rightarrow <\infty \text{ values for } A. \\ |B| \leq A \Rightarrow <\infty \text{ values for } B. \\ C = \frac{B^2-D}{4A} \Rightarrow <\infty \text{ values for } C. \end{array}\right\} = <\infty \text{ solutions.}$$

$\Rightarrow <\infty$ number of $\tau \in$ fundamental domain.

Example: Find all $\tau \in H$ of discriminant D with $|D| \leq 20$ ($\Rightarrow A \leq \sqrt{\frac{20}{3}} < 3$)

We systematically write out values of $B^2 - 4AC$.

$A =$		1	2	3	. . .
$B =$		$0, \pm 1$	$0, \pm 1, \pm 2$	$0, \pm 1, \pm 2, \pm 3$	
$C =$ 1	$-D =$	4, 3	—	—	
2		8, 7	16, 15, 12	—	
3		12, 11	~~24~~, ~~23~~, 20	~~36~~, ~~35~~, ~~32~~, ~~27~~	
4		16, 15	~~32~~, ~~31~~, ~~28~~	-X.	
5		20, 19	- X.	Y	

$D = -3$: $\tau^2 + \tau + 1 = 0 \Rightarrow \tau = \frac{-1 \pm \sqrt{3}i}{2}$

-4: $\tau^2 + 1 = 0 \Rightarrow \tau = i$.

-7: $\tau = \frac{1}{2}(1 + \sqrt{7}i)$

-8: $\tau = \sqrt{2}i$

-11: $\tau = \frac{1}{2}(1 + \sqrt{11}i)$

-12: $\tau = \sqrt{3}i$ or $2\tau^2 + 2\tau + 2 = 0$ - ie disc -3 case.

-15: $\tau = \frac{1}{2}(1 + \sqrt{15}i)$ or $2\tau^2 \pm \tau + 2 = 0 \Rightarrow \tau = \frac{1}{4}(\pm 1 - \sqrt{15}i)$

-16: $\tau = 2i$ or i (disc -4)

-19: $\tau = \frac{1}{2}(1 + \sqrt{19}i)$

-20: $\tau = \sqrt{5}i$ or τ is a root of $2\tau^2 \pm 2\tau + 3 = 0 \Rightarrow \tau = \frac{1}{2}(\pm 1 + \sqrt{5}i)$

So our modular polynomial has roots at τ of discriminant $\underset{\sqrt{2}i}{\uparrow}{-8}$, $\underset{\frac{1}{2}(1+\sqrt{7}i)}{\uparrow}{-7}$, $\underset{i}{\uparrow}{-4}$

(double root)

So polynomial has roots at $j(\sqrt{2}i)$, $j(\frac{1}{2}(1+\sqrt{7}i))$, $j(\frac{1}{2}(1+\sqrt{7}i))$, $j(i)$

$j(i)$ is an integer.

If $x^3 + ax^2 + bx + c = (x-\alpha)(x-\beta)^2$, $a, b, c \in \mathbb{Z}$, then $\alpha, \beta \in \mathbb{Z}$, since $x - \beta$ = highest common factor of $(x^3 + ax^2 + bx + c)$ and its derivative.

Hence $j(\sqrt{2}i)$, $j(\frac{1}{2}(1+\sqrt{7}i))$ are integers.

Summary:

1. If $\tau \in H$, $A\tau^2 + B\tau + C = 0$, $A, B, C \in \mathbb{Z}$, $(A,B,C) = 1$, then τ has discriminant $B^2 - 4AC$.

(a) $\text{disc}(\tau) = \text{disc}\left(\frac{a\tau+b}{c\tau+d}\right)$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$

(b) for fixed $D < 0$, only a finite number of τ in fundamental domain with $\text{disc}(\tau) = D$, and these are easy to find.

permuted by $SL_2(\mathbb{Z})$

Modular polynomial: $(j(\tau) - j(2\tau))(j(\tau) - j(\tau/2))(j(\tau) - j(\frac{\tau+1}{2}))$

$=$ modular function $=$ polynomial in $j(\tau) = j(\tau)^4 + a(3)j(\tau)^3 + \cdots + a(0)$, $a(i) \in \mathbb{Z}$.

Roots of modular polynomial: points of $j(\tau)$ with $\frac{a\tau+b}{c\tau+d} = \tau$, $\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = 2$.

$c\tau^2 + (d-a)\tau - b = 0$. Disc. $= (d-a)^2 + 4bc = (d+a)^2 - 4\det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (d+a)^2 - 8 = -8, -7, -4$.

Lemma: Suppose $f(x)$ is a polynomial with integer coefficients, $f(x) = (x-\alpha_1)\cdots(x-\alpha_m)(x-\beta_1)^2\cdots(x-\beta_n)^2$, α_i, β_i distinct, then $(x-\alpha_1)\cdots(x-\alpha_m)$ and $(\alpha-\beta_1)\cdots(\alpha-\beta_n)$ also have integer coefficients.

Proof: $(x-\beta_1)\cdots(x-\beta_n)$ = hcf of $f(x)$, $f'(x)$, both of which have integer coefficients.

Modular polynomial is: $\underbrace{(j(\tau)-j(\sqrt{2}i))}_{\text{disc.}=-8}\underbrace{(j(\tau)-j(\tfrac{1+\sqrt{7}i}{2}))^2}_{\text{disc.}=-7}\underbrace{(j(\tau)-\overset{=1728}{j(i)})}_{\text{disc}=-4.}$

Eg: Look at disc $=-7$ $\qquad (d+a)^2-8=-7$, $(d+a)^2=1$.

τ is a root of $x^2+x+2=0$ $\qquad c=1$, $d-a=1$, $b=-2$, so $c=1$, $b=-2$, $d=1$, $a=0$

$=c\tau^2+(d-a)\tau-b$ $\qquad$ or $d=0$, $a=-1$.

So $j(\frac{1+\sqrt{7}i}{2})$ occurs twice.

Since $j(i)=1728$, we have that $(j(\tau)-j(\sqrt{2}i))(j(\tau)-j(\frac{1+\sqrt{7}i}{2}))^2$ is a polynomial in $j(\tau)$ with integer coefficients.

Apply lemma: $j(\sqrt{2}i)$, $j(\frac{1+\sqrt{7}i}{2})$ are both integers! We can calculate $j(\sqrt{2}i)$ exactly by calculating it up to an error $<\frac{1}{2}$. This determines it, as we know it is an integer.

N=3, $N=\det\begin{pmatrix}a&b\\c&d\end{pmatrix}$.

Look at $j(3\tau)$, $j(\tau/3)$, $j(\frac{\tau+1}{3})$, $j(\frac{\tau+2}{3})$, $j(\frac{a\tau+b}{c\tau+d})$: $\det\begin{pmatrix}a&b\\c&d\end{pmatrix}=3$.

Modular polynomial: $\underbrace{(j(\tau)-j(3\tau))}_{-q^{-6}}\underbrace{(j(\tau)-j(\tau/3))}_{q^{-1}}\underbrace{\cdots}_{\cdots}$

$=-q^{-6}+\cdots=-j(\tau)^6+a(5)j(\tau)^5+\cdots+a(0)$.

Zeros at $j(\tau)$ for $\frac{a\tau+b}{c\tau+d}=\tau$, $\det\begin{pmatrix}a&b\\c&d\end{pmatrix}=3 \Rightarrow \tau$ with discriminant $(a+d)^2-4\times\overset{N}{3}=-12, -11, -8, -3.$

-12: $(a+d)^2=0$, $a+d=0$ $\Rightarrow$ roots mult.$=1$; -11: $(a+d)^2=1$, $a+d=\pm1$ $\Rightarrow$ mult$=2$; -8: $(a+d)=\pm2$ $\Rightarrow$ mult$=2$

We know values of $j(\tau)$ for disc$(\tau)=-8,-3,\ldots$ are integers. So we find

$$\prod_{-\text{disc}(\tau)=12}(x-j(\tau))\times\prod_{-\text{disc}(\tau)=11}(x-j(\tau))^2 \quad \text{has integer coefficients.}$$

Apply lemma: $\prod_{\text{disc}(\tau)=-12}(x-j(\tau))$, $\prod_{\text{disc}(\tau)=-11}(x-j(\tau))$ have integer coefficients $\Rightarrow (x-j(\sqrt{3}i))$, $(x-j(\frac{1+\sqrt{11}i}{3})),\ldots$

Extra complication for N=4: Look at

$$\begin{tikzcd}
j(4\tau) \arrow[loop below, "T"] \arrow[rrr, leftrightarrow, bend left, "S"] & j(\frac{2\tau}{2}) \arrow[loop above, "S"] \arrow[loop right, "T"] \arrow[d] & j(\frac{2\tau+1}{2}) \arrow[loop below, "T"] \arrow[rrr, leftrightarrow, bend right, "S"] & j(\tau/4) \arrow[r, "T"] & j(\frac{\tau+1}{4}) \arrow[r, "T"] \arrow[rr, leftrightarrow, bend right, "S"] & j(\frac{\tau+2}{4}) \arrow[r, "T"] & j(\frac{\tau+3}{4}) \arrow[lll, bend right, "T"'] \\
 & j(\tau)-j(\frac{2\tau}{2})=0 & & & & &
\end{tikzcd}$$

Miss out term $j(\tau)-j(\frac{2\tau}{2})$. (Note that all the values other than $j(\tau)=j(\frac{2\tau}{2})$ are permuted amongst each other by $SL_2(\mathbb{Z})$).

Second problem: Look at term: $j(\tau)-j(\frac{2\tau+1}{2}) \longrightarrow j(\tau+\frac{1}{2})=-q^{-1}+744$

$=(q^{-1}+744)-(-q^{-1}+744) = \underset{\uparrow \text{ Leading coefficient} \neq 1.}{2}q^{-1}+\cdots$

Coefficient of q^n is: const. $\times(1-(-1)^n)=$ const. $\times$ 2 or 0.

So all coefficients are divisible by 2. So we can take out a factor of 2 to make leading coefficient 1. So we can still find a polynomial in $j(\tau)$, integer coefficients, leading coefficient 1.

Roots are $j(\tau)$: disc$(\tau)=$ -16 (mult 1)

-15 (mult 2)

-12 (mult 2) $\qquad 2\tau^2+2\tau+2=0$, $D=2^2-4.2.2=-12$, τ really disc $=-\frac{12}{4}=-3$.

-7 (mult 2)

-3

Theorem: If τ is an imaginary quadratic irrational of disc $= -D$, then $j(\tau)$ is an algebraic integer and conjugates of $j(\tau)$ for other τ with $\mathrm{disc}(\tau) = -D$.

Proof: Induction on $-D$. We checked for $D = -3, -4$. Suppose true for $D = -3, -4, \dots, -4(N-1)$.

Prove it simultaneously for $D = -4N, 1-4N$.

Look at all values of $j\left(\frac{a\tau+b}{d}\right)$, $ad = N$, $0 < a$, $0 \le b \le d$, and form $\prod_{a,b,d}\left(j(\tau) - j\left(\frac{a\tau+b}{d}\right)\right) =$ polynomial in $j(\tau)$.

If $N = d^2$ for $d > 0$, modify this, as for case $N = 4$ (miss out $j(\tau) - j(d\tau/d)$, factors of $(\zeta^n - 1)/(\zeta - 1)$ for ζ a root of 1), and we get a polynomial in $j(\tau)$ with integer coefficients, leading coefficient 1.

As before, we find roots: $j(\tau)$, $\mathrm{disc}(\tau) =$

$$\begin{array}{ll} -4N & (\text{mult}\ 1) \\ 1-4N & (\text{mult}\ 2) \\ 4-4N & (\text{mult}\ 2) \\ 9-4N & \vdots \\ \vdots & \end{array} \left.\vphantom{\begin{array}{l} 1\\1\\1 \end{array}}\right\} \text{by induction, we can divide out all these terms.}$$

So $\prod_{\mathrm{disc}(\tau) = -4N}(x - j(\tau)) \cdot \prod_{\mathrm{disc}(\tau) = 1-4N}(x - j(\tau))^2$ has integer coefficients.

So $\prod_{\mathrm{disc} = -4N}(x - j(\tau))$, $\prod_{\mathrm{disc} = 1-4N}(x - j(\tau))$ have integer coefficients.

Example: Calculate $j(\sqrt{5}i)$. Disc $(\sqrt{5}i)$: root of $\tau^2 + 5 = 0$, so $D = -20$.

Find all $\tau \in$ Fundamental Domain with $D = -20$. 2 solutions: $\tau^2 + 5 = 0$: $\tau = \sqrt{5}i$

$2\tau^2 + 2\tau + 3 = 0$: $\tau = \frac{1+\sqrt{5}i}{2}$

So by the theorem, $(x - j(\sqrt{5}i))\left(x - j\left(\frac{1+\sqrt{5}i}{2}\right)\right) = x^2 - \left(j(\sqrt{5}i) + j\left(\frac{1+\sqrt{5}i}{2}\right)\right)x + j(\sqrt{5}i)\, j\left(\frac{1+\sqrt{5}i}{2}\right)$ has integer coefficients.

$$\left.\begin{array}{l} \text{Work out } j(\sqrt{5}i) = 1264538{\cdot}90947\cdots \\ j\left(\frac{1+\sqrt{5}i}{2}\right) = -538{\cdot}90947\cdots \end{array}\right\} \text{from power series for } j(\tau).$$

Sum: $1264000{\cdot}000$ (error < 0.5)

$= 1264000$

Product $= -681472000$.

So $j(\sqrt{5}i)$, $j\left(\frac{1+\sqrt{5}i}{2}\right)$ satisfy $x^2 - 1264000x - 681472000 = 0$

Roots are: $632000 \pm 282880\sqrt{5}$ = values of $j(\sqrt{5}i)$, $j\left(\frac{1+\sqrt{5}i}{2}\right)$.

Explanation: of $e^{\pi\sqrt{163}} = 262537412640768743{\cdot}999999999999\cdots$

Look at $j(\tau)$, $\tau = \frac{1+\sqrt{163}i}{2}$. Root of $\tau^2 + \tau + 41 = 0$, $\mathrm{disc}(\tau) = -163$.

$q = e^{2\pi i\tau} = -e^{-\pi\sqrt{163}}$. So $j(\tau) = \underset{q^{-1}}{\underset{\shortparallel}{e^{\pi\sqrt{163}}}} + 744 + 196884\underset{\uparrow}{q} + \cdots$

very small, $< 10^{-12}$.

So we must show $j(\tau)$ is an integer. $\prod_{\mathrm{disc}(\tau) = -163}(x - j(\tau))$ has integer coefficients.

So we want to find all $\tau \in$ Fundamental domain of disc $= -163$. $A\tau^2 + B\tau + C = 0$.

$B^2 - 4AC = -163$, $|B| \le A \le C$. We know $A \le \sqrt{\frac{-D}{3}} = \sqrt{\frac{163}{3}} < 8$. So $|B| \le 8$.

$$B^2 + 163 = 4AC \Rightarrow B \text{ odd}: \quad \left.\begin{array}{lll} 1^2 + 163 = 4 \times 41 & \Rightarrow AC & = 41 \\ 3^2 + 163 = 4 \times 43 & & = 43 \\ 5^2 + 163 = 4 \times 47 & & = 47 \\ 7^2 + 163 = 4 \times 53 & & = 53 \end{array}\right\} \begin{array}{l} \text{primes, so } A = 1 \text{ as } A \le C. \\ \text{So } B = \pm 1 \text{ as } |B| \le A. \end{array}$$

So $\frac{1+\sqrt{163}i}{2}$ is only point of disc $= -163$ in Fundamental domain. So $j\left(\frac{1+\sqrt{163}i}{2}\right)$ is an integer.

Remarks: Proved by [Heequorl, Stark, Baker that 163 is largest integer $-D$ such that only one number of discriminant D lies in fundamental domain.

Schneider proved that if τ is algebraic and $j(\tau)$ is algebraic, then $A\tau^2 + B\tau + C = 0$ for some $A, B, C \in \mathbb{Z}$. - see Baker: Transcendental Number Theory.

$$\begin{tikzcd}
 & \text{$j(\tau)$ algebraic for τ imaginary quadratic} \arrow[dl, leftrightarrow] \arrow[dr, leftrightarrow] & \\
\text{imaginary quadratic fields} \arrow[rr, leftrightarrow] & & \text{elliptic curves with complex multiplication}
\end{tikzcd}$$

Imaginary quadratic field $\mathbb{Q}(\sqrt{N})$, $N<0$, N squarefree. Ring of algebraic integers: $\mathcal{O}$.

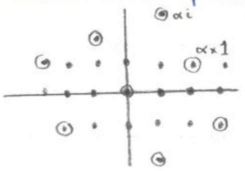
$\mathcal{O} = \mathbb{Z}[\sqrt{N}]$ if $N \not\equiv 1 \bmod 4$ Discriminant: $4N$ for $\mathbb{Z}[\sqrt{N}]$

$\mathbb{Z}[\frac{\sqrt{N}+1}{2}]$ if $N \equiv 1 \bmod 4$. N for $\mathbb{Z}[\frac{\sqrt{N}+1}{2}]$.

The ideal $\mathcal{O}$ is a subgroup closed under multiplication by $\mathcal{O}$. Fractional ideal of $\mathcal{O}$ is an ideal multiplied by some element of the field k.

Example: $N = -1$. $k = \mathbb{Q}(i)$, $D = -4$.

$\mathbb{Z}[i]$ is a principal ideal domain, so all ideals are generated by one element α.



So ideal (α) is "same shape" as $\mathbb{Z}[i]$. Fractional ideals are lattices invariant under multiplication by elements of $\mathcal{O}$.

Look at $\mathbb{Z}[\sqrt{-5}]$. $D = -20$. Not a UFD, eg $2\cdot 3 = (1+\sqrt{5}i)(1-\sqrt{5}i)$

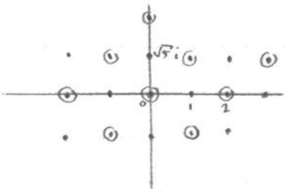
Ideals have unique factorisation: $(6) = (2)(3) = (1+\sqrt{5}i)(1-\sqrt{5}i)$. $(2) = (2, 1+\sqrt{5}i)^2$

$(2, 1+\sqrt{5}i)^2$ generated by $2(1+\sqrt{5}i)$, $(1+\sqrt{5}i)^2 = -4+2\sqrt{5}i$, $2+2\sqrt{5}i$ = ideal generated by 2.

If I, J are ideals, IJ is ideal generated by ab, $a \in I$, $b \in J$.

$(3) = (3, 1+\sqrt{5}i)(3, 1-\sqrt{5}i)$, $(1+\sqrt{5}i) = (2, 1+\sqrt{5}i)(3, 1+\sqrt{5}i)$

$\mathbb{Z}[\sqrt{5}i]$:



Any principal ideal is same shape as rectangular lattice. Ideal $(2, 1+\sqrt{5}i)$ is different shape - so not principal. What are possible shapes of fractional ideals of $\mathcal{O}$? If we have a fractional ideal, multiply it by a constant so it contains 1. We can assume that it is generated by $1, \tau$ as a $\mathbb{Z}$-module, some $\tau \in H$. Suppose $\mathcal{O}$ is generated as a $\mathbb{Z}$-module by $1, \lambda$. (eg, $\lambda = \sqrt{5}i$ for $\mathbb{Z}[\sqrt{5}i]$) $\mathbb{Z}$-module $\langle 1, \tau \rangle$ closed under multiplication by λ.

So $\left.\begin{aligned} \tau \times \lambda &= a\tau + b \\ 1 \times \lambda &= c\tau + d \end{aligned}\right\}$ $a, b, c, d \in \mathbb{Z}$.

Eliminate λ: $\tau(c\tau+d) = a\tau + b \Rightarrow c\tau^2 + (d-a)\tau - b = 0$. Discriminant: $(d-a)^2 + 4bc$.

Eliminate τ: $\tau = \frac{\lambda-d}{c} \Rightarrow (\frac{\lambda-d}{c})\lambda = a\frac{(\lambda-d)}{c} + b \Rightarrow \lambda^2 - (a+d)\lambda + (ad-bc) = 0$.

$(c \neq 0)$ Discriminant: $(a+d)^2 - 4ad + 4bc = (a-d)^2 + 4bc$ - the same number!

Hence $(1, \tau)$ is a fractional ideal of $\mathbb{Z}[\lambda]$ iff (check other way) τ is an imaginary quadratic irrational of discriminant D (D = disc. of $\mathbb{Z}[\lambda]$)

Eg: $\lambda = \sqrt{5}i$, $D = -20$. τ of discriminant -20 in fundamental domain are $\sqrt{5}i$, $\frac{1+\sqrt{5}i}{2}$.

$\Rightarrow$ Fractional ideals: $(1, \sqrt{5}i) \longrightarrow (1)$,

$(1, \frac{1+\sqrt{5}i}{2}) \longrightarrow (2, 1+\sqrt{5}i)$

Summary: Fractional $\underbrace{\text{ideals / mu}}_{\text{Ideal class group of }\mathcal{O}.}$ltiplication by constants in K $\equiv$ set of τ of $\underbrace{\text{disc. } D}_{\text{finite}}$ /action on $SL_2(\mathbb{Z})$ on H.

$(1,\tau) \leftarrow \tau$ $\updownarrow$

set of values of $j(\tau)$ which are all roots of some polynomial with integer coefficients.

The roots of this polynomial (= values $j(\tau)$, disc $\tau = -D$) generate an $\underset{\uparrow \atop \text{Gal}(L/K)\text{ abelian.}}{\text{abelian}}$ unramified extension L of quadratic field K.

Background: Class Field Theory = study of abelian extensions of algebraic number field K.

Eg: If $K = \mathbb{Q}$; if ζ is a root of 1, $\zeta^n = 1$, then $\mathbb{Q}[\zeta]$ is an abelian extension of $\mathbb{Q}$, $\text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ generated by $\zeta \mapsto \zeta^a$, $a \in (\mathbb{Z}/n\mathbb{Z})^*$

Converse (Kronecker-Weber): If L is a finite abelian extension of $\mathbb{Q}$, then $L \subseteq \mathbb{Q}(\zeta)$ for some ζ, $\zeta^n = 1$. In other words, macimal abelian extension generated by values of $e^{2\pi i x}$ for $x \in \mathbb{Q}$.

Abelian extensions of rational numbers are generated by special values of a certain transcendental function ($e^{2\pi i x}$).

Some abelian extensions of $\mathbb{Q}(\sqrt{-N})$ are generated by special values of elliptic function $j(\tau)$.

Kronecker "Jungendtraum": generated all abelian extensions of imaginary quadratic fields using special values of elliptic functions ($j(\tau)$ for disc$(\tau) = D$ generated by Hilbert class field of $\mathcal{O}$).

Example: What is Hilbert class field of $\mathbb{Q}[\sqrt{-5}]$?

It is generated by values $j(\tau)$, disc$(\tau) = -20$, $= j(\sqrt{5}i)$, $j\left(\frac{1+\sqrt{5}i}{2}\right)$, $= 632000 \pm 282880\sqrt{5}$.

So Hilbert class field is $\mathbb{Q}[\sqrt{5}, \sqrt{-5}] = \mathbb{Q}[\sqrt{5}, i] \leftarrow$ degree 4.

$$\left.\begin{matrix} \mathbb{Q}[\sqrt{5}, i] \\ \cup\!\text{I} \\ \mathbb{Q}[\sqrt{5}] \end{matrix}\right\} \text{degree } 2 = \#\tau \text{ of disc} = -20 \text{ in fundamental domain} = \text{order of ideal class group.}$$

$$\begin{matrix} \cup\!\text{I} \\ \mathbb{Q} \end{matrix}$$

Elliptic curves with "complex multiplication."

Such is just an endomorphism of an elliptic curve, eg: $y^2 = x^3 + a$. This has automorphism $y \to -y$, $x \to x$, or $y \to y$, $x \to \omega x$ $(\omega^3 = 1)$

Suppose elliptic curve is $\mathbb{C}/L$, $L = \langle 1, \tau \rangle$. When is multiplication by $\lambda \in \mathbb{C}$ an endomorphism?

λ is an endomorphism of $\mathbb{C}/L$ iff $\lambda L \subseteq L$, $\left.\begin{matrix} \lambda \times 1 = a\tau + b \\ \lambda \times \tau = c\tau + d \end{matrix}\right\}$ $a, b, c, d \in \mathbb{Z}$.

Same as conditions for L to be a fractional ideal of an imaginary quadratic field.

(If L is ideal of quadratic field $\mathbb{Z}[\lambda]$, then $\mathbb{C}/L$ is elliptic curve with $\mathbb{Z}[\lambda]$ acting as ring of endomorphisms).

Examples: (i) $\mathbb{Z}[\lambda] = \mathbb{Z}[i]$. Find all elliptic curves with $\mathbb{Z}[i]$ as ring of endomorphisms.

Solution: These correspond to $\mathbb{C}/L$ where L = ideal of $\mathbb{Z}[i]$. So only one (over $\mathbb{C}$) up to isomorphism, $y^2 = x^3 + x$, Automorphism: $\sigma: x \to -x$, $y \to iy$, $\sigma^4 = 1$.

(ii) Find all elliptic curves with ring of endomorphisms $\mathbb{Z}[\sqrt{-5}]$. τ with discriminant $\tau = -20$ are $\tau = \sqrt{5}i$, $\frac{1+\sqrt{5}i}{2}$. So elliptic curves are $\mathbb{C}/(1, \sqrt{5}i)$ or $\mathbb{C}/(2, 1+\sqrt{5}i)$

$\uparrow$ two ideal classes of $\mathbb{Z}[\sqrt{-5}]$

Jacobi Triple Product Identity.

Special Cases:

1. Euler: $(1-q)(1-q^2)(1-q^3)\ldots = 1 - q - q^2 + q^5 + q^7 - q^{12} - q^{15} + \ldots$

$\eta(\tau) = q^{1/2}(1-q)(1-q^2)\ldots = \Sigma (-1)^n q^{3/2\cdot(n+1/2)^2}$ ← slight modification of $\sum_n q^{n^2}$

$\eta(\tau)^{24} = \Delta(\tau)$. $\quad \Delta(\frac{-1}{\tau}) = \Delta(\tau).\tau^{12}$

$\eta(\frac{-1}{\tau}) = \text{const.} \sqrt{\frac{\tau}{i}}\,\eta(\tau)$. $\quad \tau = i \Rightarrow \text{const.} = 1$.

So $\eta(\frac{-1}{\tau}) = \sqrt{\frac{\tau}{i}}\,\eta(\tau)$

$\eta(\tau+1) = e^{2\pi i/24}\cdot\eta(\tau)$.

So $\eta\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^{1/2} \times (24\text{th root of } 1) \times \eta(\tau)$.

↑ hard to describe explicitly - it is a 1-dimensional character of a double cover of $SL_2(\mathbb{Z})$.

2. Gauss: $\theta(\tau) = \sum_n q^{n^2} = (1+q)^2(1-q^2)(1+q^3)^2(1-q^4)\ldots$

Corollary: $\theta(\tau)$ has no zeroes for $\tau \in H$, as infinite product converges.

Jacobi: $\prod_{n>0}(1-q^{2n})(1-q^{2n-1}z)(1-q^{2n-1}z^{-1}) = \sum_n (-1)^n q^{n^2}.z^n$.

Special cases: (i) $z = -1 \Rightarrow$ Gauss' identity

(ii) $z = q^{1/2} \Rightarrow$ Euler's identity (change q to $q^{3/2}$).

(iii) $z = \text{const.}\times q^* \Rightarrow$ other identities.

There are lots of different of Jacobi's identity.

Proof of Jacobi using Boson-Fermion correspondance.

Write it in the form: $\dfrac{\sum_n q^{n^2/2} z^n}{\prod_{n>0}(1-q^n)} = \prod_{n>0}(1+q^{\frac{2n-1}{2}}.z)(1+q^{\frac{2n-1}{2}}.z^{-1}) \qquad (z \to -z,\ q \to q^{1/2})$

We will show that coefficient of $q^{\varepsilon} z^n$ = # states of a certain physical system.

Very simple model for (say) electron. Suppose that energy of "electron" can be $\ldots -\frac{3}{2}, -\frac{1}{2}, \frac{1}{2}, \frac{3}{2}, \ldots$

Dirac: Assume most negative energy states are filled

Pauli: Cannot have two electrons in same state, ie, same energy.

Mathematical interpretation: A state is a subset of $\mathbb{Z}+\frac{1}{2} = \ldots, -\frac{3}{2}, \frac{-1}{2}, \frac{1}{2}, \frac{3}{2}, \ldots$, such that

(i) All but a finite number of negative elements are in S (Dirac)

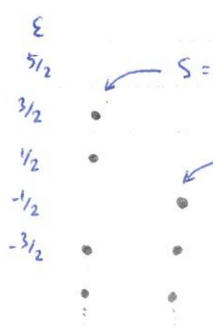
(ii) Only a finite number of positive elements are in S.

S = set of occupied energy levels.

Energy $\{s_1, s_2, \ldots\} \overset{?}{=} \cancel{s_1 + s_2 + \ldots} = -\infty$?

$:= \Sigma$ +ve elements in S $- \Sigma$ −ve elements not in S

$\geqslant 0$.



$S = \{\frac{3}{2}, \frac{1}{2}, -\frac{3}{2}, -\frac{5}{2}, \ldots\} \Rightarrow \text{energy} = \frac{3}{2} + \frac{1}{2} - (-\frac{1}{2}) = 5/2$

$\text{Vacuum} = \{-\frac{1}{2}, -\frac{3}{2}, -\frac{5}{2}, \ldots\} \Rightarrow \text{energy} = 0$, by definition.

particles of $S = \{s_1, s_2 \dots\}$

$\overset{?}{=}$ # ~~elements~~ of $S = \infty$?

$:=$ # (positive elements of S) $-$ # (negative elements not in S)

"electrons" "positrons"

How many states are there of energy ε, particle number n? Call the answer $c_{\varepsilon,n}$.

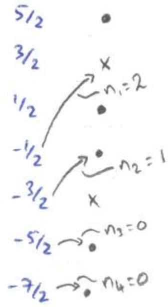
We want to find power series $\sum c_{\varepsilon,n} q^{\varepsilon} z^{n}$.

Look at electron with energy:

$$\begin{array}{lll} & \text{(exists)} & \text{(does not exist)} \\ \frac{1}{2} & (q^{1/2} z^{1} & + \quad 1) \\ \frac{3}{2} & (q^{3/2} z^{1} & + \quad 1) \\ -\frac{1}{2} & (1 & + \quad q^{\frac{1}{2}} z^{-1}) \\ -\frac{3}{2} & (1 & + \quad q^{3/2} z^{-1}) \end{array}$$

Form product: $(q^{\frac{1}{2}} z + 1)(q^{3/2} z + 1) \cdots \times (1 + q^{\frac{1}{2}} z^{-1})(1 + q^{3/2} z^{-1}) \cdots = \sum c_{\varepsilon,n} q^{\varepsilon} z^{n}$.

We count states of particle number 0 in different way.



If $S = \{s_1, s_2, \dots\}$ has particle number 0, then it can be written uniquely as $(-\frac{1}{2} + n_1, -\frac{3}{2} + n_2, -\frac{5}{2} + n_3, \dots)$, where

(i) $n_1 \geq n_2 \geq \cdots$

(ii) $n_i = 0$ for $i \gg 0$.

(iii) energy $= n_1 + n_2 + n_3 + \cdots$

$\Rightarrow$ set of photons with energies $n_1, n_2, n_3, \dots$ Note that we can have n_i's the same, ie many photons have same energy (Boson).

So # states, energy ε, particle number 0,

$= \#$ solutions of $\begin{cases} n_1 + n_2 + \cdots = \varepsilon \\ n_1 \geq n_2 \geq \cdot \end{cases}$

$= \#$ partitions of ε

Eg: $\varepsilon = 4$, $4 = 4, 3+1, 2+2, 2+1+1, 1+1+1+1$

So $c_{4,0} = 5$.

Euler: $\sum_n p(n) q^n = \prod_{n>0} \frac{1}{(1-q^n)} = (1 + q + q^2 + \dots)(1 + q^2 + q^4 \dots)(1 + q^3 + q^6 + \dots)$

So coefficient of z^0 in $\prod (1 + q^{n+1/2} z)(1 + q^{n+1/2} z^{-1})$ is $\prod_{n>0} \frac{1}{(1-q^n)}$

What about coefficient of z^N?

Argument similar, except we use lowest energy state of particle number N, instead of vacuum. Lowest state with three particles: $S = \{\frac{5}{2}, \frac{3}{2}, \frac{1}{2}, \frac{-1}{2}, \dots\}$, energy $= \frac{1}{2} + \frac{3}{2} + \frac{5}{2} = \frac{3^2}{2}$.

So number of states of particle number 3, energy ε, $=$ coefficient of q^n in $\frac{q^{3/2}}{\prod_{n>0}(1-q^n)}$

Similarly, number of states of energy ε, particle number N

$= $ coefficient of $q^{\varepsilon} z^{n}$ of $\prod (1 + q^{n+1/2} z)(1 + q^{n+1/2} z^{-1})$

$= $ coefficient of q^{ε} of $\frac{q^{N^2/2}}{\prod(1-q^n)}$

So, $\prod (1 + q^{n+1/2} z)(1 + q^{n+1/2} z^{-1}) = \frac{\sum q^{n^2} z^n}{\prod(1-q^n)}$ $-(*)$

states of "fermions" states of "bosons"

See Kac, "Vertex algebras", p. 93.

There are graded vector spaces, $V = \bigoplus_{\varepsilon, n} V_{\varepsilon, n}$, $\dim V_{\varepsilon, n} = c_{\varepsilon, n}$.

V has structure of a vertex algebra.

(*) corresponds to an isomorphism from "fermionic" vertex algebra to "boson" vertex algebra.