Introduction to Modular Forms.

Two examples

$D<0$ the disc. of an imaginary quadratic field

$h(D)$ = class number (size of class group).

A simple modular form: $\Theta(z) = \sum_{n=-\infty}^{+\infty} q^{n^2}$ where $z \in \mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im}(z) > 0\}$.
$q := e^{2\pi i z}$ (note $|q|<1$).

$(\Theta(z) = 1 + 2q + 2q^4 + 2q^9 + \cdots)$

Let $H(z) = \Theta(z)^3 = 1 + 6q + 12q^2 + \cdots + 24q^{163} + \cdots + 168q^{251} + \cdots$

$$H(z) = \sum_{n=0}^{\infty} r(n) q^n .$$

Fact: if $D \equiv 3\ (8)$, then $h(D) = \frac{1}{24} r(D)$. (and similar for other D).

Example 2:

$$f(z) := q \cdot \prod_{n=1}^{\infty} (1-q^n)^2 (1-q^{11n})^2 = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 + \cdots = \sum_{n=1}^{\infty} a(n) q^n$$

Facts:

- $a(nm) = a(n)a(m)$ whenever $(n,m) \equiv 1$.
- $|a(p)| \leq 2\sqrt{p}$ $\forall p$ prime.
- $E: y^2 + y = x^3 - x^2 - 10x - 20$

  Let $N(p)$ = # solution in $\mathbb{F}_p$. (don't count the point at ∞).

  Heuristic: RHS is "random" mod p
  There's a 50% chance that there's a solution (but they come in pairs). } $\sim$ expect $\sim p$ solutions.

  So $N(p) \approx p$.

  Theorem (Hasse): $|p - N(p)| \leq 2\sqrt{p}$.

  It turns out that $a(p) = p - N(p)$ $\forall p$. Say that "E is modular".

$$\begin{tikzcd} \text{Modular Forms} \arrow[r, bend left, "\text{\"Easy\" (in book)}"] & \text{Elliptic Curves} \arrow[l, bend left, "\text{Wiles}"] \end{tikzcd}$$

Modular Group

$\Gamma := SL_2(\mathbb{Z}) = \{ 2\times 2$ int. matrices with $\det = 1 \}$.

$\mathbb{H} =$ the upper half plane.

$\Gamma \curvearrowright \mathbb{H}$ by $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \sim \gamma . z = \dfrac{az+b}{cz+d}$ (check that it's an action)
Ex 1.1.2.

Half-definition: A modular form of weight $\overset{\in \mathbb{Z}}{k}$ for Γ is $f : \mathbb{H} \to \mathbb{C}$ such that

$$(T) \cdot f(\gamma z) = (cz+d)^k f(z) \quad \forall \gamma \in \Gamma$$

and (A) - an analytic property

Note: $\dfrac{d(\gamma z)}{dz} = (cz+d)^{-2}$

So $(T) \Leftrightarrow f(\gamma z)(d(\gamma z))^{k/2} = f(z)(dz)^{k/2}$

Hence $f(z)(dz)^{k/2}$ is invariant under Γ.

Note: This shows that if (T) holds for γ_1, γ_2 then (T) holds for $\gamma_1 \gamma_2$.

Lemma 1: Γ is generated by $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. (Ex: 1.1.1 or Koblitz).

So it's enough to check (T) for these two matrices:

$$f(z+1) = f(z) \quad \text{and} \quad f\left(\frac{-1}{z}\right) = z^k f(z)$$

Basic Example: Eisenstein series.

$k \geq 3$. Define:

$$G_k(z) := \sum_{(m,n)\in\mathbb{Z}^2}{}' \frac{1}{(mz+n)^k}$$

Fact: G_k converges absolutely $\forall z$ and uniformly on compact subsets.

Get that

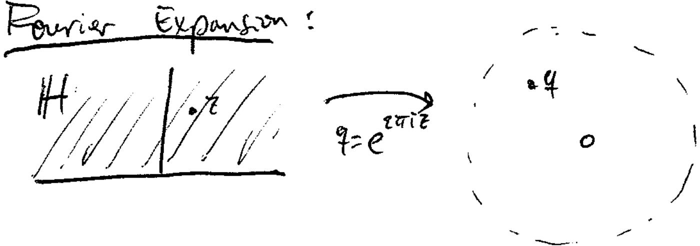
$$G_k(z+1) = \sum{}' \frac{1}{(mz+(m+n))^k} \overset{\substack{\text{can rearrange} \\ \downarrow}}{=} \sum{}' \frac{1}{(mz+n)^k} = G_k(z).$$

$$G_k\left(-1/z\right) = \sum{}' \frac{1}{\left(\frac{-m}{z}+n\right)^k} = z^k G_k(z).$$

Note: if k is odd, $G_k(z) \equiv 0$. For k even, $\lim_{z\to\infty} G_k(z) = \sum \frac{1}{n^k} = 2\zeta(k)$.

Recall: For $\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, (T) implies $f(z+1) = f(z)$, so f will have a Fourier expansion.

Fourier Expansion:



$D' = \{0 < |q| < 1\}$.

Suppose f is holomorphic of period 1.
Define $g(q) := f(z)$ where $q = e^{2\pi i z}$ (any choice).
(i.e. can define $g(q) := f\left(\frac{\log q}{2\pi i}\right)$ where log can be taken with any branch).
So g will be holomorphic on $D' \Rightarrow g(q) = \sum_{n=-\infty}^{+\infty} a(n) q^n$ (Laurent expansion).
(and so $f(z) = \sum_{n=-\infty}^{+\infty} a(n) e^{2\pi i n z}$).

Def: f is meromorphic at ∞ if $f(z) = \sum_{n \geq n_0} a(n) q^n$.
holomorphic at ∞ if $n_0 = 0$

To check that f is hol. at ∞ is the same as checking that $f(z)$ is bounded as $z \to i\infty$.

Def f vanishes at ∞ if $n_0 = 1$. (ie $f(z) = \sum_{n=1}^{\infty} a(n) q^n$). ($\Leftrightarrow f(z) \to 0$ as $z \to i\infty$).

Example: $G_K(z) \to 2\zeta(k)$ as $z \to \infty$ ($k \geq 4$, even). So it's Holomorphic at ∞.

Def: $k \in \mathbb{Z}$, $f: \mathbb{H} \to \mathbb{C}$ ~~holomorphic~~. Then f is a modular form of weight k for $SL_2(\mathbb{Z})$ if:
1) f is holomorphic
2) $f(\gamma z) = (cz+d)^k f(z)$ $\quad \forall \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.
3) f is holomorphic at ∞.

We write $f \in M_k(SL_2(\mathbb{Z})) = M_k$.

If f vanishes at ∞, then f is called a cusp form, $f \in S_k(SL_2(\mathbb{Z}))$.

Note: we can replace "holomorphic" by "meromorphic" to define meromorphic mod. forms. (Koblitz calls them "modular functions")

Notes:

0) These are $\mathbb{C}$-vectorspaces

1) Set $M := \bigoplus_{k \in \mathbb{Z}} M_k$ is a graded ring. (i.e. $M_k M_j \subseteq M_{k+j}$).

2) $f \in M_k$ with k odd, then $f(z) = (-1)^k f(z) \Rightarrow f(z) = 0$.
(so there are no odd-weight mod. forms)

Fourier expansion of G_k

$$G_k(z) = \sum_{m,n \in \mathbb{Z}^2} \frac{1}{(mz+n)^k} \qquad k \geq 4 \text{ even.}$$

- Bernoulli numbers: define B_k by $\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!} = 1 - \frac{1}{2}x + \frac{1}{12}x^2 - \frac{1}{720}x^4 + \dots$

So $B_2 = \frac{1}{6}$, $B_4 = -\frac{1}{30}$, ... (for $k \geq 2$ even, $\zeta(k) = \frac{-(2\pi i)^k}{2} \frac{B_k}{k!}$).

(Note: p regular if $p \nmid B_2, B_3, \dots, B_{p-3} \Rightarrow p \nmid h(\mathbb{Q}(\zeta_p))$. Kummer proved FLT for regular primes).

Thm 2: $k \geq 4$ even. Then

$$G_k(z) = 2 \cdot \zeta(k) \cdot E_k(z) \quad \text{where } E_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \in \mathbb{Q}[[q]]$$

$$\left(\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}\right).$$

Pf

write with exponentials

$$\pi \cot(\pi z) = \pi i - 2\pi i \sum_{m=0}^{\infty} q^m$$

$$\|$$

log deriv of $\left(\sin \pi z = \prod_{n=1}^{\infty}\left(1 - \frac{z^2}{n^2}\right)\right) = \frac{1}{z} + \sum_{d=1}^{\infty}\left(\frac{1}{z-d} + \frac{1}{z+d}\right)$

Now differentiate both sides $k-1$ times and the formula follows. //

Examples:

$$E_4 = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n \in M_4$$

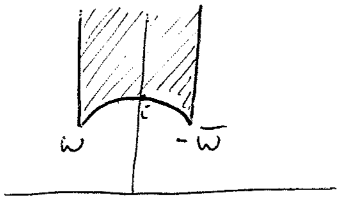
$$E_6 = 1 - 504 \cdot \sum_{n=1}^{\infty} \sigma_5(n) q^n \in M_6$$

Note that E_4^3 and $E_6^2 \in M_{12} \Rightarrow E_4^3 - E_6^2 \in M_{12}$:

$$E_4^3 - E_6^2 = (1 + 720 q + \cdots) - (1 - 1008 q + \cdots) = 1728 q + \cdots \in S_{12}$$

Define $\Delta(z) = \dfrac{E_4^3 - E_6^2}{1728} =$ ~~[illegible]~~ $q - 24q^2 + 252 q^3 + \cdots \quad \in S_{12}$

Valence Formula



$v_\tau(f)$: order of f at τ.

$v_\infty(f)$: order at ∞.

Thm 3: f a non-zero weakly modular of weight k on $\Gamma = SL_2(\mathbb{Z})$. Then:

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\omega(f) + \sum_{\substack{\tau \in \Gamma \backslash \mathbb{H} \\ \tau \neq i, \omega}} v_\tau(f) = \frac{k}{12}$$

This implies:

Thm 4:

- $M_0 = \mathbb{C}$
- $\left.\begin{array}{l} M_k = \mathbb{C} E_k \\ S_k = \{0\} \end{array}\right\} \quad 4 \leq k \leq 10, \quad k = 14$
- $M_k = \mathbb{C} E_k \oplus S_k \quad k \geq 4$
- $S_{12} = \mathbb{C}\Delta, \quad S_k = \Delta M_{k-12}, \quad k \geq 12$
- $\dim(M_k) = \begin{cases} 1 + \lfloor \frac{k}{12} \rfloor & k \equiv 2 \pmod{12} \\ \lfloor \frac{k}{12} \rfloor & \text{o.w.} \end{cases}$

$\leftarrow$ See pf in koblitz's handout.

Example:

$M_6 = \mathbb{C}E_6$

$M_{18} = \mathbb{C}E_{18} \oplus S_{18} = \mathbb{C}E_{18} \oplus \Delta M_6 = \mathbb{C}E_{18} \oplus \mathbb{C}\Delta E_6$

$M_{30} = \mathbb{C}E_{30} \oplus \mathbb{C}\Delta E_{18} \oplus \mathbb{C}\Delta^2 E_6$.

A "better" basis: $\{E_6^5, \Delta E_6^3, \Delta^2 E_6\}$.

Note that $E_6^5 = 1 + \cdots$, $\Delta E_6^3 = q + \cdots$, $\Delta^2 E_6 = q^2 + \cdots$ so they are l.i.

Hence, as all of them are in a 3 dim vectorspace, they are a basis.

Note: Suppose that $f(z)$ is a non-zero weakly-modular of weight 0 ("modular function").

Then $f(\gamma z) = f(z)$.

The valence formula $\Rightarrow$ f has the same number of zeros as poles, and this number is called the valence of f. (hence the name for the theorem).

Example:

Define $j(z) = \dfrac{E_4^3}{\Delta} = \dfrac{1+\cdots}{q+\cdots} = q^{-1} + 744 + 196884q + \cdots$

is weakly modular of wt 0, with a pole at ∞. (and hence has a triple zero at ω).

Take $c \in \mathbb{C}$. Then $j(z) - c = q^{-1} + 744 - c + \cdots$

Note that, as Δ has no zeros in $\mathbb{H}$, $j(z)$ is holomorphic on $\mathbb{H}$.

As $j(z) - c$ has one pole, it must have one zero.

So we obtain a ~~injection~~ bijection $j : \Gamma \backslash \mathbb{H} \to \mathbb{C}$.

Actually, get a bijection $j : \Gamma \backslash \mathbb{H} \cup \{\infty\} \to \mathbb{C} \cup \{\infty\}$.

• Product formula for $\Delta(z) = q + \cdots$ (in the book, there's an extra factor).

Weight-2 Eisenstein series: $G_2(z) = \sum_c \sum_d{}' \frac{1}{(cz+d)^2}$ does not converge absolutely.

It's not a weight-2 modular form (the only one is 0!).

But still get $G_2(z) = 2\zeta(2)E_2(z)$ where $E_2(z) := 1 - 24\sum_{n=1}^{\infty} \sigma(n) q^n$ $(\sigma = \sigma_1)$.

E_2 is holom. on $\mathbb{H}$, $E_2(z+1) = E_2(z)$.

However, $z^{-2}E_2(-1/z) = E_2(z) + \frac{12}{2\pi i z}$ (QM) ← called "quasi-modular".

The Dedekind-eta function

$\eta(z) := q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$ holomorphic, non-vanishing on $\mathbb{H}$.

(to check that, it's enough to check that $\sum q^n$ converge absolutely & uniformly on compacts).

$$\frac{d}{dz}\log(\eta(z)) = \frac{2\pi i}{24} + \sum_{n=1}^{\infty}\frac{-2\pi i n q^n}{1-q^n} = \frac{2\pi i}{24}\left(1 - 24\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}\right) =$$

$$= \frac{\pi i}{12}\left(1 - 24\sum_{n=1}^{\infty} n \sum_{m=1}^{\infty} q^{nm}\right) = \frac{\pi i}{12}E_2(z)$$

We have thus shown that $\frac{d}{dz}\log\eta(z) = \frac{\pi i}{12}E_2(z)$.

So $\frac{d}{dz}\log\left(\eta\left(\frac{-1}{z}\right)\right) \underset{\text{using (QM)}}{\overset{\uparrow}{=}} \frac{d}{dz}\log\left(\sqrt{\frac{z}{i}}\,\eta(z)\right)$

$\Rightarrow \eta\left(\frac{-1}{z}\right) = C\cdot\sqrt{\frac{z}{i}}\,\eta(z)$. Setting $z = i$, one gets $C = 1$. We've proved:

Theorem 9: $\eta\left(\frac{-1}{z}\right) = \sqrt{\frac{z}{i}}\,\eta(z)$.

Note: $\eta^{24}(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24} \leadsto \eta^{24}(z+1) = \eta^{24}(z)$.

Moreover, $\eta^{24}\left(\frac{-1}{z}\right) = z^{12}\eta^{24}(z)$

So, as $\eta^{24}(z) = q + \cdots$, $\eta^{24}(z) \in S_{12} = \mathbb{C}\Delta$, so $\eta^{24} = \Delta$.

So $\Delta = q\prod_{n\geq 1}(1-q^n)^{24}$.

Cor 6: $\Delta(z) = q \prod_{n=1}^{\infty} (1-q^n)^{24}$

Congruence Subgroups

Let $N \geq 1$ be an integer.

Def The principal congruence subgroup of level N is

$$\Gamma(N) := \left\{ \gamma \in SL_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\} \qquad \left(\text{write it as } \Gamma(N) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}\right)$$

Def Γ is a congruence subgroup of level N if $\Gamma(N) < \Gamma \leq SL_2(\mathbb{Z})$.

Examples:

- $\Gamma_1(N) = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\}$
- $\Gamma_0(N) = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}$.

We have $\underbrace{\Gamma(N) < \Gamma_1(N)}_{N} \underbrace{< \Gamma_0(N)}_{\phi(N)} \underbrace{< SL_2(\mathbb{Z})}_{N \prod_{p \mid N} (1+\frac{1}{p})}$ (see HW 1.2.?).

Example:

Spse f is weakly holomorphic modform on $SL_2(\mathbb{Z})$.

Set $g(z) := f(Nz)$.

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. So $\gamma' := \begin{pmatrix} a & bN \\ \frac{c}{N} & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

$$g(\gamma z) = f(N \cdot (\gamma z)) = f\left(\frac{Naz+Nb}{cz+d}\right) = f\left(\frac{a(Nz)+Nb}{\frac{c}{N}(Nz)+d}\right) = f(\gamma'(Nz)) = \left(\frac{c}{N}Nz+d\right)^k f(Nz)$$

$\Rightarrow g(\gamma z) = (cz+d)^k g(z)$. So g is invariant under $\Gamma_0(N)$.

Def: The weight-k operator ("slash", "stroke") is defined as:

$\gamma \in SL_2(\mathbb{Z})$, define the "automorphy factor" $j(\gamma, z) := cz+d$, and:

$[\gamma]_k$ acts as: $(f[\gamma]_k)(z) := (cz+d)^{-k} f(\gamma z) = j(\gamma, z)^{-k} f(\gamma z)$.

(Sometimes $f[\gamma]_k$ is written $f|_k \gamma$).

Note:

- $f[\gamma_1\gamma_2]_k = (f[\gamma_1]_k)[\gamma_2]_k$ (lemma 1.2.2 or 1st day).

Def f is weakly modular of weight k wrt Γ if it is meromorphic on $\mathbb{H}$,

$$f[\gamma]_k = f \quad \forall \gamma \in \Gamma.$$

- Fourier expansion at ∞.

$\Gamma(N) < \Gamma$, and note that $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma(N)$.

Let $h > 0$ be least with the property $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma$ (for width).

Also, note that $h \mid N$.

Now, let $q_h := e^{2\pi i z/h}$. The map $z \mapsto q_h$ is periodic with period h.

Then, define $g(q_h) := f(z)$. It will have a Laurent expansion:

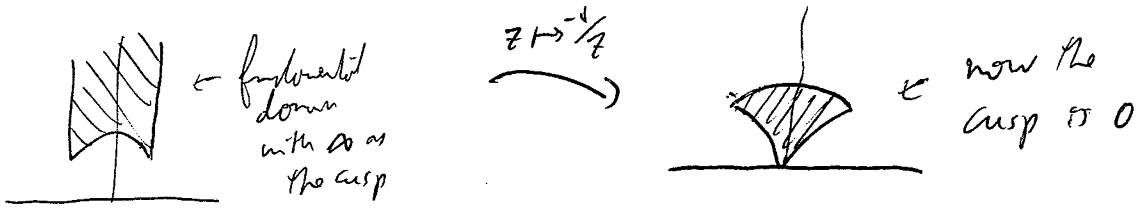
$$g(q_h) = \sum_{n=-\infty}^{+\infty} a(n)\, q_h^n$$

This is the expansion of f at ∞.

- Expansions at "cusps".

The cusps are $\{\infty\} \cup \mathbb{Q}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \infty = \frac{a}{c}.$$ So $SL_2(\mathbb{Z})$ acts transitively on the cusps.



But for instance, for $\Gamma(2)$, ∞ and 0 are not equivalent:

Let s be a cusp, not ∞. $s = \alpha\cdot\infty$ for some $\alpha \in SL_2(\mathbb{Z})$.

Then, the behavior of $f[\alpha]_k(z)$ as $z \to \infty$ is related to the behavior of $f(z)$ near s:

$$f[\alpha]_k(z) = \underset{\substack{\uparrow \\ \text{does not} \\ \text{change behavior.}}}{(cz+d)^{-k}} \, f(\underline{\alpha z}) \quad \leftarrow \text{when } z \sim \infty,\ \alpha z \sim s.$$

Assume f is weakly modular on the cong. sgp. Γ.

$f[\alpha]_k$ is invariant under $\alpha^{-1}\Gamma\alpha =: \Gamma'$

(because $f[\alpha]_k\left([\alpha^{-1}\gamma\alpha]_k\right] = \left(f[\gamma]_k\right)[\alpha]_k = f[\alpha]_k$).

Now $\Gamma(N) \triangleleft SL_2(\mathbb{Z})$ ($\Gamma(N)$ is the kernel of reduction mod N), so $\Gamma(N) < \Gamma'$ as well.

Hence, $f[\alpha]_k$ has a Fourier expansion, at least in powers of q_N:

$$f[\alpha]_k = \sum_{n=-\infty}^{+\infty} b(n)\, q_N^n \quad \leftarrow \text{"expansion of } f \text{ at } s\text{".}$$

We get now the definition of a modular form.

Let Γ be a cong. sgp, $k \in \mathbb{Z}$.

Def $f : \mathbb{H} \to \mathbb{C}$ is a <u>modular form</u> of weight k for Γ if:

1) f is holomorphic on $\mathbb{H}$.

2) $f[\gamma]_k = f \quad \forall \gamma \in \Gamma$.

3) $f[\alpha]_k$ is holomorphic at $\infty \quad \forall \alpha \in SL_2(\mathbb{Z})$.

(i.e. for all cusps $s \in \mathbb{P}^1(\mathbb{Q})$, the expansion of f at s ~~has~~ has no negative powers).

f is a <u>cusp form</u> if:

3') $f[\alpha]_k$ vanishes at $\infty \quad \forall \alpha \in SL_2(\mathbb{Z})$.

Prop 7: Suppose $f:\mathbb{H}\to\mathbb{C}$ satisfies (1) and (2). Then, if, $f(z)=\sum_{n\geq 0}^{\infty} a(n)\, q_N^n$ (i.e f is hol. at ∞)

Sps also $|a(n)| << n^r$ for some $r>0$ (i.e $\exists$ ct. C s.t $|a(n)| < Cn^r$ $\forall n$).

Then: f satisfies (3) (i.e. $f\in M_k(\Gamma)$).

(Pf in the book, as exercise)
or in handout

Now, suppose that $s_1\in\mathbb{Q}\cup\{\infty\}$, $s_1=\alpha_1\infty$, $\alpha_1\in SL_2(\mathbb{Z})$.

Then $f[\alpha_1]_k=\sum a(n)\, q_h^n$ for some $h|N$.

Q: What if s_2 is equivalent to s_1 under Γ?

Then $s_1=\gamma s_2$ for some $\gamma\in\Gamma$, $s_2=\alpha_2\infty$.

Prop 9: In this situation,

$$f[\alpha_2]_k=\sum b(n)\, q_h^n \quad \text{where} \quad b(n)=(\pm1)^k e^{2\pi i n j/h} a(n) \quad \text{for some } j\in\mathbb{Z}.$$

Cor: $a(n)=0 \iff b(n)=0$, so it's enough to check (3) for one representative from each of the equivalence classes of cusps.

Pf Have that $\alpha_1\infty=\gamma\alpha_2\infty$, so $\alpha_1^{-1}\gamma\alpha_2\infty=\infty \Rightarrow \alpha_1^{-1}\gamma\alpha_2=\pm\begin{pmatrix}1&j\\0&1\end{pmatrix}$ for some $j\in\mathbb{Z}$ (the only matrices that fix infinity).

$$\Rightarrow \alpha_2=(\pm I)(\gamma^{-1})\cdot(\alpha_1)\begin{pmatrix}1&j\\0&1\end{pmatrix}$$

So
$$f[\alpha_2]_k=\underbrace{f[\pm I]_k}_{(\pm1)^k}\underset{\uparrow\ \text{nothing!}}{[\gamma^{-1}]_k}[\alpha_1]_k\left[\begin{pmatrix}1&j\\0&1\end{pmatrix}\right]_k=(\pm1)^k\sum a(n)\, e^{\frac{2\pi i n z}{h}}\left[\begin{pmatrix}1&j\\0&1\end{pmatrix}\right]_k$$

$$=\sum(\pm1)^k a(n)\, e^{\frac{2\pi i n(z+j)}{h}}$$

//

§ 1.3 Complex Tori.

Def: A *lattice* Λ is $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ where ω_1, ω_2 are $\mathbb{R}$-linearly-indep.

We will always assume that $\omega_1/\omega_2 \in \mathbb{H}$ (otherwise, exchange them!).

Prop 9: $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, $\Lambda' = \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$. Then (we assume $\frac{\omega_1}{\omega_2} \in \mathbb{H}$ & $\frac{\omega_1'}{\omega_2'} \in \mathbb{H}$!!)

$$\Lambda = \Lambda' \iff \begin{pmatrix}\omega_1\\ \omega_2\end{pmatrix} = \gamma \begin{pmatrix}\omega_1'\\ \omega_2'\end{pmatrix} \quad \text{for some } \gamma \in SL_2(\mathbb{Z}).$$

Pf see handout.

Complex torus: $\mathbb{C}/\Lambda = \{z + \Lambda : z \in \mathbb{C}\}$.

Algebraically: an abelian group.

Analytically: a torus (a genus 1 Riemann surface). ✓ it's in the def of RS.

Lemma: Spse $f: X \to Y$ is a holomorphic map of compact connected Riemann Surfaces. Then f is either constant or surjective.

Pf X compact, ~~connected~~ $\Rightarrow f(X)$ is closed.

If f is not constant, then by the open mapping thm (complex analysis), then $f(X)$ is open (do it locally!). $\Rightarrow f(X) = Y$. //

We are interested in maps between tori.

Prop 11: Suppose $\varphi: \mathbb{C}/\Lambda \to \mathbb{C}/\Lambda'$ is holomorphic.

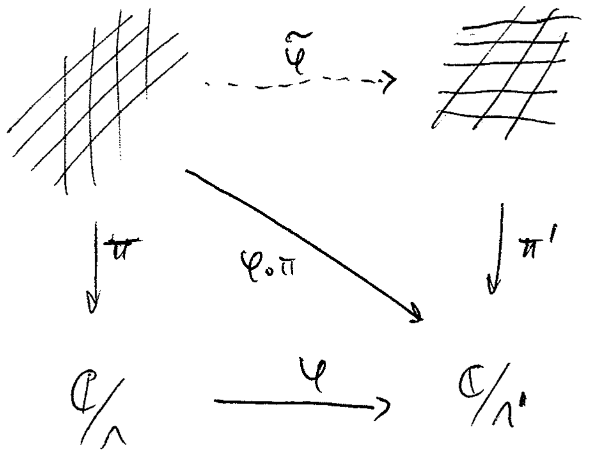
Then $\exists\, m, b \in \mathbb{C}$ s.t.:

1) $m\Lambda \subseteq \Lambda'$.

2) $\varphi(z+\Lambda) = mz + b + \Lambda'$

Moreover, φ is invertible $\iff m\Lambda = \Lambda'$.

Pf $\mathbb{C}$ is the universal covering space of $\mathbb{C}/\Lambda$ (and $\mathbb{C}/\Lambda'$).



From algebraic topology, such $\tilde{\varphi}$ exists because $\mathbb{C}$ is simply connected.
(So can lift $\varphi\circ\pi$ to $\tilde{\varphi}$).

Suppose now $\lambda\in\Lambda$, and set $f_\lambda(z) := \tilde{\varphi}(z+\lambda)-\tilde{\varphi}(z)$.

Then f_λ is continuous, with image in $\Lambda' \underset{\underset{\Lambda' \text{ discrete}}{\uparrow}}{\Longrightarrow} f_\lambda(z)$ is constant.

$\tilde{\varphi}'(z+\lambda)=\tilde{\varphi}'(z) \quad \forall \lambda\in\Lambda$.

$\tilde{\varphi}'(z)$ is holomorphic & doubly-periodic $\Rightarrow$ bounded $\overset{\text{Liouville}}{\Rightarrow}$ $\tilde{\varphi}'(z)$ = constant.

Hence $\tilde{\varphi}(z)$ is linear, $\tilde{\varphi}(z)=mz+b$.

<u>Corollary 12</u>: φ as above is a gp hom $\Leftrightarrow \varphi(0)=0 \Leftrightarrow b\in\Lambda'$.

<u>Rmk</u>: A holomorphic group isomorphism will then have to satisfy
$m\Lambda=\Lambda'$, $\varphi(z+\Lambda)=mz+\Lambda'$.

<u>Example</u>: $[N]:\mathbb{C}/\Lambda \to \mathbb{C}/\Lambda$ is a homomorphism. $(N\geq 1)$.
$z \longmapsto Nz+\Lambda$

The kernel of $[N]$ is the N-torsion points, $\mathbb{Z}/N\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z}$.

<u>Example</u>: if $\Lambda=\mathbb{Z}\omega_1\oplus\mathbb{Z}\omega_2$, $\tau:=\omega_1/\omega_2\in\mathbb{H}$, $\Lambda_\tau:=\mathbb{Z}\tau\oplus\mathbb{Z}$
Then $\mathbb{C}/\Lambda \simeq \mathbb{C}/\Lambda_\tau$

Lemma 13: $\mathbb{C}/\Lambda_\tau \simeq \mathbb{C}/\Lambda_{\tau'} \Leftrightarrow \tau = \gamma\tau'$ for some $\gamma \in SL_2(\mathbb{Z})$.

Pf/ Spz $\tau = \gamma\tau' = \dfrac{a\tau'+b}{c\tau'+d}$. Let $m := c\tau'+d$.

Then $m\Lambda_\tau = \mathbb{Z}(a\tau'+b) \oplus \mathbb{Z}(c\tau'+d) \overset{\text{(by prop 9)}}{=} \mathbb{Z}\tau' \oplus \mathbb{Z} = \Lambda_{\tau'}$

The other direction is basically the same. //

This is saying that $\{\text{iso. classes of tori}\} \xleftrightarrow{1:1} \{\tau \in SL_2(\mathbb{Z})\backslash\mathbb{H}\}$.

Goal: Associate $\mathbb{C}/\Lambda \leftrightarrow$ elliptic curve $E_\Lambda : Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda)$.

Hence Modular Forms $\leftrightarrow$ functions of lattices $\leftrightarrow$ functions of ell. curves.

Example: Lattice eisenstein series.

$$G_k(\Lambda) := \sum_{\omega\in\Lambda}{}' \frac{1}{\omega^k} \quad k > 2 \leftarrow \text{for convergence.}$$, and assume k even (otherwise, it's 0!).

Note: $G_k(\Lambda_\tau) = G_k(\tau)$ (usual Eisenstein series).

Transf. law: $G_k(m\Lambda) = m^{-k} G_k(\Lambda)$.

§ Meromorphic functions on $\mathbb{C}/\Lambda$ ($= \Lambda$-periodic mer. function on $\mathbb{H}$).

Let $\mathbb{C}(\Lambda)$ = field of meromorphic functions on $\mathbb{C}/\Lambda$.

Basic properties:

Prop 14: if $f \in \mathbb{C}(\Lambda)$, then:

a) $\displaystyle\sum_{z\in\mathbb{C}/\Lambda} \operatorname{res}_z f = 0$

b) $\displaystyle\sum_{z\in\mathbb{C}/\Lambda} \operatorname{ord}_z f = 0$

c) $\displaystyle\sum_{z\in\mathbb{C}/\Lambda} z\cdot\operatorname{ord}_z f \in \Lambda$

Pf/ D a fundamental parallelopiped which misses all zeros and poles.

Compute $\dfrac{1}{2\pi i}\displaystyle\int_{\partial D} f(z)\,dz$, $\dfrac{1}{2\pi i}\displaystyle\int_{\partial D} \frac{f'(z)}{f(z)}\,dz$, $\dfrac{1}{2\pi i}\displaystyle\int_{\partial D} \frac{zf'(z)}{f(z)}\,dz$. // (see handout)

Note: this Prop implies that # zeros = # poles =: order of f.

Also, pt (a) ⇒ order $f \geq 2$.

Weierstrass function: $\wp_\Lambda(z) := \frac{1}{z^2} + \sum'_{\omega\in\Lambda}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right)$

→ is even.

→ converges absolutely and uniformly on compact sets away from Λ.

→ periodic:

$\wp_\Lambda'(z) = -2\cdot\sum_{\omega\in\Lambda}\frac{1}{(z-\omega)^3}$ is periodic.

Set $f(z) := \wp(z+\omega_1) - \wp(z)$. Then $f'(z)=0$, so $f(z) = ct$.

Set now $z = -\frac{\omega_1}{2}$. Then $ct = \wp\left(\frac{+\omega_1}{2}\right) - \wp\left(-\frac{\omega_1}{2}\right) = 0$ ($\wp$ even) //

Hence, $\wp_\Lambda(z) \in \mathbb{C}(\Lambda)$. Indeed, $\mathbb{C}(\Lambda) = \mathbb{C}(\wp_\Lambda, \wp_\Lambda')$, but we are not proving it now.

Prop. 15: The Laurent expansion at $z=0$ of $\wp_\Lambda(z)$ is:

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{n\geq 2\\ n \text{ even}}} (n+1)\, G_{n+2}(\Lambda)\, z^n$$ converges until the closest lattice point.

Pf/ See book. Just rearrange. //

We can use this expansions to find alg. relations between $\wp_\Lambda, \wp_\Lambda'$:

$$\wp_\Lambda = \frac{1}{z^2} + 3\, G_4(\Lambda)\, z^2 + O(z^4).$$

$$\wp_\Lambda' = \frac{-2}{z^3} + 6\, G_4(\Lambda)\, z + O(z^3)$$

So $(\wp_\Lambda')^2 = \frac{4}{z^6} + O(z^{-2}) = 4(\wp_\Lambda)^3 + O(z^{-2})$

Working with more terms of the expansion, we finally get:

$$(\wp_\Lambda')^2 = 4(\wp_\Lambda)^3 - 60\, G_4(\Lambda)\, \wp_\Lambda - 140\, G_6(\Lambda) + F(z) \quad , \; F(z) = O(z^2).$$

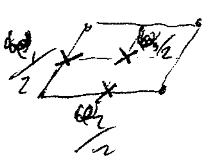
But $F(z) = O(z^2)$ is Λ-periodic $\Rightarrow$ $F(z) = \underset{\overset{\shortparallel}{0}}{\text{constant}}$ (Liouville).

<u>Prop 16</u>: Let $g_2(\Lambda) = 60\,G_4(\Lambda)$; $g_3(\Lambda) = 140\,G_6(\Lambda)$. Then:

a) $(\wp(z), \wp'(z))$ lies on the curve $E_\Lambda : Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda)$.

b) E_Λ has the form $Y^2 = 4(X-e_1)(X-e_2)(X-e_3)$ where:

$e_i = \wp\left(\frac{\omega_i}{2}\right)$ where $\omega_3 := \omega_1 + \omega_2$.



$\leftarrow$ the 2-torsion point!

Pf/ (a) is done.

(b): $\wp'$ is odd and periodic, so $\wp'\left(\frac{\omega_i}{2}\right) = \wp'\left(\frac{-\omega_i}{2}\right) = -\wp'\left(\frac{\omega_i}{2}\right) \Rightarrow \wp'\left(\frac{\omega_i}{2}\right) = 0$.

So $\wp$ takes the value e_i twice $\Rightarrow$ these are all the roots, as $\wp$ has order 2 $\Rightarrow$ <u>takes each value twice</u> $\Rightarrow$ does not take the value e_i at any other point.

$\uparrow$ Consider $f(z) := \wp(z) - c$

<u>Summary</u>:

$$\mathbb{C}/\Lambda \longrightarrow E_\Lambda : Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda)$$

$$z + \Lambda \longmapsto (\wp_\Lambda(z), \wp'_\Lambda(z))$$

This is a bijection:

- if $x \in \mathbb{C}$, $\wp$ hits x twice, as $\wp(\pm z + \Lambda) = x \Rightarrow Y = \pm\wp'(z+\Lambda)$

$\Rightarrow$ get two y-values unless $y = 0$ (i.e. $z = \frac{\omega_i}{2}$) in which case $\wp(z) = e_i$, and $\wp(z)$ hits e_i twice at z.

<u>Theorem 17</u> (Uniformization theorem): If $E : Y^2 = 4X^3 - g_2 X - g_3$ is an elliptic curve, then $\exists\,\Lambda$ s.t. $g_2(\Lambda) = g_2$, $g_3(\Lambda) = g_3$.

Pf/ Ommited.
Uses that $j(z)$ is surjective.

<u>Note</u>: 1) $E_{\Lambda_\tau} : Y^2 = 4X^3 - g_2(\tau)X - g_3(\tau)$ $\rightarrow$ has disc $= \frac{1}{16}\left(g_2(\tau)^3 - 27g_3(\tau)^2\right) \overset{\substack{\text{exercise}\\ \downarrow}}{=} \frac{(2\pi)^{12}}{16}\Delta(\tau)$

2) E_Λ inherits the group structure from $\mathbb{C}/\Lambda$.

Recall: Let $\Gamma = \Gamma(1) = SL_2(\mathbb{Z})$.

$$\underline{\mathbb{C}/\Lambda_\tau \simeq \mathbb{C}/\Lambda_{\tau'}} \Leftrightarrow \underline{m\Lambda_\tau = \Lambda_{\tau'}} \text{ (some } m) \Rightarrow \begin{pmatrix} m\tau \\ m \end{pmatrix} = \gamma \begin{pmatrix} \tau' \\ 1 \end{pmatrix} \text{ (some } \gamma \in \Gamma) \Rightarrow$$

$$\Rightarrow \underline{\tau} = \frac{m\tau}{m} = \gamma \underline{\tau'} \Leftrightarrow \underline{m = c\tau' + d} \qquad \left(\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right).$$

Prototype: $S = \{\text{elliptic curves}\}/\simeq$

- Every E isom. to $\mathbb{C}/\Lambda_\tau$ for some τ
- $\mathbb{C}/\Lambda_\tau \simeq \mathbb{C}/\Lambda_{\tau'} \Leftrightarrow \Gamma\tau = \Gamma\tau'$.

So there's a bijection: $S \longleftrightarrow \Gamma \backslash \mathcal{H}$

$$[\mathbb{C}/\Lambda_\tau] \longmapsto \Gamma\tau$$

$\Gamma\backslash\mathcal{H}$ is called the <u>moduli space</u> for isomorphism classes of elliptic curves.

<u>j-invariant</u>: define $j(E) := j(\tau)$ where $[E] = [E_\tau]$ $\quad (E_\tau = E_{\Lambda_\tau})$.

j-invariant is a weight-0 weakly-modular form. What about other weights?

Given f s.t. $f[\gamma]_k = f \quad \forall \gamma \in \Gamma(1)$, $\quad (*)$

define $F(\mathbb{C}/\Lambda_\tau) := f(\tau)$. It is well-defined:

if $\Lambda_\tau = \Lambda_{\tau'} \Leftrightarrow \tau = \tau' + b$ some b.

Suppose $m\Lambda_\tau = \Lambda_{\tau'}$. Then $\tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau'$, $m = c\tau' + d$.

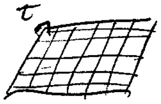
Then $F(\mathbb{C}/m\Lambda_\tau) = F(\mathbb{C}/\Lambda_{\tau'}) = f(\tau') = (c\tau'+d)^{-k} f(\tau) = F(\mathbb{C}/\Lambda_\tau) \cdot m^{-k}$.

So we get $\underline{F(\mathbb{C}/m\Lambda_\tau) = m^{-k} F(\mathbb{C}/\Lambda_\tau)}$, $\quad (**)$

We can reverse the argument, and we get $(*) \Leftrightarrow (**)$.

<u>Idea</u>: repeat this construction for Γ other congruence subgroups.

Repeat for $\Gamma_0(N)$, $\Gamma_1(N)$, $\Gamma(N)$

Recall: $E[N] = \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ ().

Enhanced ell. curve for $\Gamma_0(N)$: it is a pair (E, C) where E is an elliptic curve, and C is a cyclic sgp. of order $N \leq E[N]$.

Also, $(E, C) \sim (E', C') \Leftrightarrow \exists\, \varphi : E \xrightarrow{\sim} E'$ isomorphism such that $\varphi(C) = C'$.

Define $S_0(N) := \{(E,C)\}/\sim$.

Theorem 18:

a) $S_0(N) = \{[(\mathbb{C}/\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle)] : \tau \in \mathbb{H}\}$.

b) $(\mathbb{C}/\Lambda_\tau, \langle \frac{1}{N} + \Lambda_\tau \rangle) \sim (\mathbb{C}/\Lambda_{\tau'}, \langle \frac{1}{N} + \Lambda_{\tau'} \rangle)$ if, and only if,

$\Gamma_0(N)\tau = \Gamma_0(N)\tau'$.

(and so $S_0(N) \xrightarrow{1:1} \Gamma_0(N)\backslash\mathbb{H}$).
$(\mathbb{C}/\Lambda_\tau, \langle\frac{1}{N}+\Lambda_\tau\rangle) \mapsto \Gamma_0(N)\tau$.

Pf

(a) Choose $[(\mathbb{C}/\Lambda, C)] \in S_0(N)$.

Know that $\mathbb{C}/\Lambda \simeq \mathbb{C}/\Lambda_{\tau'}$ for some $\tau \in \mathbb{H}$. Then $\varphi(C)$ is cyclic of order n.

So $(\mathbb{C}/\Lambda, C) \sim (\mathbb{C}/\Lambda_{\tau'}, \langle \frac{c\tau'+d}{N} + \Lambda_{\tau'} \rangle)$. (for some $(c,d,N)=1$).

Claim: $\exists$ matrix $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z})$ s.t. $\begin{cases} c' \equiv c \ (N) \\ d' \equiv d \ (N) \end{cases}$

because $SL_2(\mathbb{Z}) \twoheadrightarrow SL_2(\mathbb{Z}/N\mathbb{Z})$ is surjective.

Set now $\tau = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \cdot \tau'$, $m = c'\tau' + d'$ and get $m\Lambda_\tau = \Lambda_{\tau'}$,

and $m\left(\frac{1}{N} + \Lambda_\tau\right) = \frac{c'\tau' + d'}{N} + \Lambda_{\tau'} = \frac{c\tau' + d}{N} + \Lambda_{\tau'}$. //

(cont. proof)

Remark: after finishing the proofs we will get a bijection:

$$S_0(N) \longleftrightarrow Y_0(N) = {}^{\mathbb{H}}/_{\Gamma_0(N)} \quad \text{(non compact modular curve)}$$

$$[\mathbb{C}/\Lambda_\tau, \langle \tfrac{1}{N}+\Lambda_\tau\rangle] \longmapsto \Gamma_0(N)\tau.$$

(b) Two classes are equal $[(\mathbb{C}/\Lambda_\tau, \langle\frac{1}{N}+\Lambda_\tau\rangle)] = [(\mathbb{C}/\Lambda_{\tau'}, \langle \frac{1}{N}+\Lambda_{\tau'}\rangle)] \Leftrightarrow$

$\Leftrightarrow \Big[\exists\, \gamma\in SL_2(\mathbb{Z}),\ \gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}$ s.t. $(c\tau'+d)\Lambda_\tau = \Lambda_{\tau'}$ and $\langle (c\tau'+d)(\frac{1}{N}+\Lambda_\tau)\rangle = \langle\frac{1}{N}+\Lambda_{\tau'}\rangle\Big]$

$\Leftrightarrow \exists\,\gamma$ s.t. $\langle \frac{c\tau'+d}{N}+\Lambda_{\tau'}\rangle = \langle\frac{1}{N}+\Lambda_{\tau'}\rangle \Leftrightarrow N\mid c$ (and $(d,N)=1$ is automatic, then)

$\Leftrightarrow \gamma\in\Gamma_0(N)$. //

Theorem 18':

a) $S_1(N) = \{[(\mathbb{C}/\Lambda_\tau, \frac{1}{N}+\Lambda_\tau)] : \tau\in\mathbb{H}\}$.

b) $[(\mathbb{C}/\Lambda_\tau, \frac{1}{N}+\Lambda_\tau)] = [(\mathbb{C}/\Lambda_{\tau'}, \frac{1}{N}+\Lambda_{\tau'})] \Leftrightarrow \Gamma_1(N)\cdot\tau = \Gamma_1(N)\cdot\tau'$

And so $\Gamma_1(N)$ "classifies" the classes of elliptic curves together with a N-torsion point (instead of with a group).

Pf Analogous to previous //.

Modular forms (in this context):

Def F is "weight-k homogenous" for $\Gamma_0(N)$ if $F(\mathbb{C}/m\Lambda, m\cdot C) = m^{-k}F(\mathbb{C}/\Lambda, C)$.

Define now $f(\tau) := F(\mathbb{C}/\Lambda_\tau, \langle\frac{1}{N}+\Lambda_\tau\rangle)$, and one can check that, for $\gamma\in\Gamma_0(N)$,

$f(\gamma\tau) = (c\tau+d)^k f(\tau)$.

The modular curve $Y_0(N) = {}_{\Gamma_0(N)}\backslash^{\mathbb{H}}$ is a "moduli space" for $S_0(N)$.

§2.1: Topology of Modular Curves.

1st to show: the action of $SL_2(\mathbb{Z})$ on $\mathbb{H}$ is "proper discontinuous":

Prop 2.1: Let $\tau_1, \tau_2 \in \mathbb{H}$. Then $\exists$ nbhds U_1, U_2 such that, for each $\gamma \in SL_2(\mathbb{Z})$, either:

(pf omitted) until the end

(1) $\gamma \tau_1 = \tau_2$; or (say that it's a proper disc. action)

(2) $\gamma U_1 \cap U_2 = \phi$.

Corollary 2.2: if Γ is a congruence subgroup, then $Y(\Gamma) = {}_{\Gamma}\backslash^{\mathbb{H}}$ is Hausdorff, (with the quotient topology).

Note: if $\pi : \mathbb{H} \to {}_{\Gamma}\backslash^{\mathbb{H}}$, then π is open:

$$U \subseteq \mathbb{H} \text{ open}, \quad \pi^{-1}(\pi(U)) = \bigcup_{\gamma \in \Gamma} \underbrace{\gamma U}_{\text{opens!}}$$

Pf of 2.2:

Pick $\pi(\tau_1) \neq \pi(\tau_2) \in Y(\Gamma)$. Pick U_1, U_2 as in the proposition 2.1.

Note that $\gamma \tau_1 \neq \tau_2$ for any $\gamma \in \Gamma$ (otherwise, $\pi(\tau_1) = \pi(\tau_2)$).

So $\gamma U_1 \cap U_2 = \phi \ \forall \gamma \in \Gamma$. So $\pi(U_1) \cap \pi(U_2) = \phi$.

As π is open, we are done. //

Key lemma for Prop 2.1: (Lemma 2.3):

Spse U_1, U_2 nbhds in $\mathbb{H}$, $S = \{\gamma \in SL_2(\mathbb{Z}) : \gamma U_1 \cap U_2 \neq \phi\}$. (assume compact closure) (i.e. bounded nbhds).

Then S is finite.

!!

↓

Pf

Group-theoretic description of $\mathbb{H}$: $SL_2(\mathbb{R})$ acts transitively on $\mathbb{H}$: if $\tau = x + iy \in \mathbb{H}$, then $s(\tau) = \begin{pmatrix} y^{1/2} & xy^{-1/2} \\ 0 & y^{-1/2} \end{pmatrix}$ is s.t. $s(\tau)(i) = \tau$.

$\mathrm{Stab}(i) = SO_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} : \theta \in [0, 2\pi] \right\}$. is compact in $SL_2(\mathbb{R})$.

So get a bijection

$$\mathbb{H} \longleftrightarrow SL_2(\mathbb{R}) / SO_2(\mathbb{R})$$
$$\tau \longmapsto s(\tau) SO_2(\mathbb{R})$$

(cont pf of lemma):

So $\mathbb{H}$ "=" $SL_2(\mathbb{R})/SO_2(\mathbb{R})$

<u>Note</u>: $s(\gamma\tau)$ sends i to $\gamma\tau$. Also $\gamma(s(\tau))$ sends i to $\gamma\tau$.

Hence $\gamma(s(\tau))\cdot SO_2(\mathbb{R}) = s(\gamma(\tau))\cdot SO_2(\mathbb{R})$.

Now, $$\gamma\tau_1 = \tau_2 \iff \underset{\overset{\shortparallel}{\gamma(s(\tau_1))\,SO_2(\mathbb{R})}}{s(\gamma\tau_1)\,SO_2(\mathbb{R})} = s(\tau_2)\,SO_2(\mathbb{R})$$

$\iff s(\tau_2)\,SO_2(\mathbb{R})\cdot s(\tau_1)^{-1} \ni \gamma$.

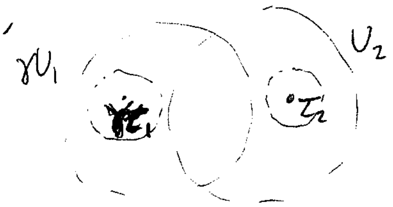
<u>Note</u>: $S \subseteq \{\gamma \in SL_2(\mathbb{Z}) : \gamma\overline{U}_1 \cap \overline{U}_2 \neq \emptyset\} = \overbrace{SL_2(\mathbb{Z})}^{\text{discrete}} \cap \overbrace{s(\overline{U}_2)\,SO_2(\mathbb{R})\,s(\overline{U}_1)^{-1}}^{\text{compact}}$

$\Rightarrow S \subseteq$ finite set. //

<u>Proof of Prop 2.1</u> (using this lemma)

Let U_1, U_2 be any nbhds. Let $\gamma \in S$. If $\gamma\tau_1 = \tau_2$, then ok.

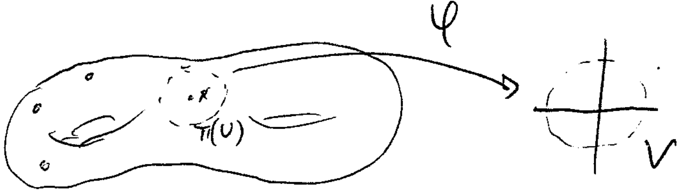
Otherwise,



Replace U_2 with V_2, and γU_1 with V_1, so replace U_1 by $\gamma^{-1}V_1$.

Do this for each $\gamma \in S$ (S is finite!). So done. //

<u>Goal</u>: $\pi : \mathbb{H} \to \Gamma\backslash\mathbb{H}$, $Y(\Gamma) = \Gamma\backslash\mathbb{H}$ modular curve. Want to give a structure of Riemann surface:



$\varphi : \pi(U) \to V$ homeo.

+ compatibility between the charts:

$\varphi_{12} : \varphi_1(\pi(U_1) \cap \pi(U_2)) \longrightarrow \varphi_2(\pi(U_1) \cap \pi(U_2))$ <u>holomorphic</u>.

First note: ${}_{\pm I\Gamma}\backslash^{\mathbb{H}} = {}_{\Gamma}\backslash^{\mathbb{H}}$. So WLOG we will assume that $-I \in \Gamma$.

$\tau \in \mathbb{H}$. • Isotropy group (stabilizer) is $\Gamma_\tau := \{\gamma \in \Gamma : \gamma\tau = \tau\}$.

• Period of τ: $h_\tau = |\Gamma_\tau|/2 \longleftarrow (\pm I \in \Gamma_\tau)$.

(Γ_τ is a finite cyclic group, so h_τ is well-defined).

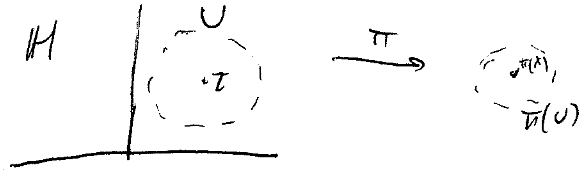
Def: τ is elliptic if $h_\tau > 1$

Easy case: $h_\tau = 1$.

Apply prop 2.1 with $\tau_1 = \tau_2 \Longrightarrow$ ~~either~~ $\exists$ nbhd $U \ni \tau$ st if $\gamma \neq \pm I$,

then $\gamma U \cap U \cancel{\neq} = \phi$.

So U has no pairs of Γ-equivalent points.



$\pi : U \longrightarrow \pi(U)$

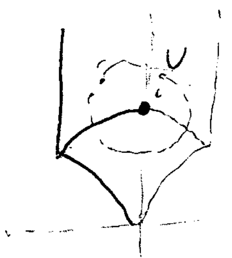
is a homeomorphism.

Then π^{-1} is the φ we are looking for.

What if $h_\tau > 1$?

Example: $\tau = i$, $\Gamma = SL_2(\mathbb{Z})$. So $\Gamma_\tau = \{\pm I, \pm\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\}$.

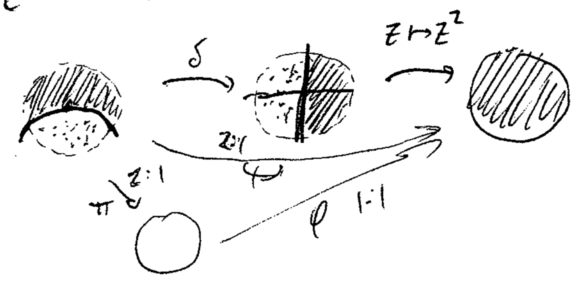
So $h_\tau = 2$.



Every nbhd U contains pairs of Γ-equiv points.

So π is 2 - 1

We will find σ s.t



<u>Lemma 2.4</u>: If $\tau \in \mathbb{H}$, $\exists\, U \ni \tau$ nbhd s.t. if $\gamma \in \Gamma$,

$$[\, \gamma(U) \cap U \neq \emptyset \Rightarrow \gamma \in \Gamma_\tau \,].$$

(Rewriting of Prop 2.1.)

Moreover, U has no elliptic point except possibly τ.

(cf $\gamma \neq \pm I$, $\gamma\tau = \tau$ has only two solutions at most: τ and $\bar{\tau}$).

<u>Defining δ</u> (for each τ, in some nbhd).

$\delta_\tau = \begin{pmatrix} 1 & -\tau \\ 1 & -\bar{\tau} \end{pmatrix}$ sends $\begin{matrix} \tau \mapsto 0 \\ \bar{\tau} \mapsto \infty \end{matrix}$

<u>Note</u>: $\left(\delta_\tau \Gamma \delta_\tau^{-1}\right)_0 \overset{\text{fixing } 0}{=} \delta_\tau \Gamma_\tau \delta_\tau^{-1}$ ← fixes 0!

Moreover, $\delta_\tau \Gamma_\tau \delta_\tau^{-1}$ fixes also ∞.

As $\delta_\tau \Gamma_\tau \delta_\tau^{-1}$ are linear fract. transformation, so they send lines + circles to lines + circles.

So $\delta_\tau \Gamma_\tau \delta_\tau^{-1}$ sends lines through 0 to lines through 0.

This group is cyclic of order $2h_\tau$.

So $\delta_\tau \Gamma_\tau \delta_\tau^{-1} / \pm\{I\} = \{$ rotations of $\frac{2\pi}{h_\tau}, \frac{4\pi}{h_\tau}, \ldots, 2\pi \}$.

If τ_1, τ_2 are s.t. $\pi(\tau_1) = \pi(\tau_2)$, we'd like that $\psi(\tau_1) = \psi(\tau_2)$.

$$\pi(\tau_1) = \pi(\tau_2) \Leftrightarrow \tau_1 \in \Gamma \tau_2 \Leftrightarrow \underset{\text{for some } \gamma \in \Gamma}{(\gamma U) \cap U \neq \emptyset} \overset{2.4}{\Leftrightarrow} \tau_1 \in \Gamma_\tau \tau_2 \Leftrightarrow \delta(\tau_1) \in \underbrace{\delta(\Gamma_\tau \tau_2)}_{(\delta \Gamma_\tau \delta^{-1})\, \delta \tau_2}$$

$$\Leftrightarrow \delta(\tau_1) = e^{2\pi i \frac{d}{h_\tau}} \cdot \delta(\tau_2) \quad \text{for some } d$$

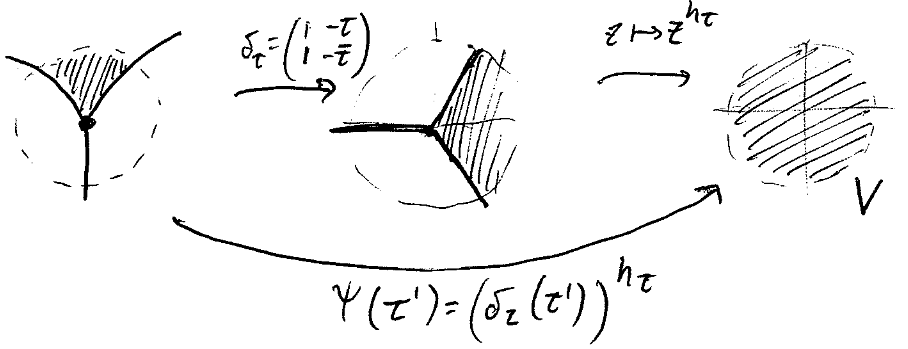
$$\Leftrightarrow \delta(\tau_1)^{h_\tau} = \delta(\tau_2)^{h_\tau}.$$

So we will define $\psi : U_\tau \longrightarrow V$, $\psi(\tau_1) = \delta(\tau_1)^{h_\tau}$.

And we will have $\boxed{\pi(\tau_1) = \pi(\tau_2) \Leftrightarrow \psi(\tau_1) = \psi(\tau_2).}$

* Problems: 1.5.2, 1.5.4, 2.2.2, 2.3.7.
↑only $\Gamma_1(N), \Gamma_0(N)$

Example: Now, with $h_\tau = 3$:



Now, because $\pi(\tau_1) = \pi(\tau_2) \Leftrightarrow \psi(\tau_1) = \psi(\tau_2)$.

$$\begin{tikzcd} U \arrow[r, "\psi"] \arrow[d, "\pi"'] & V \\ \pi(U) \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

Can define φ by $\varphi(\pi(\tau_1)) := \psi(\tau_1)$ (well-defined!)

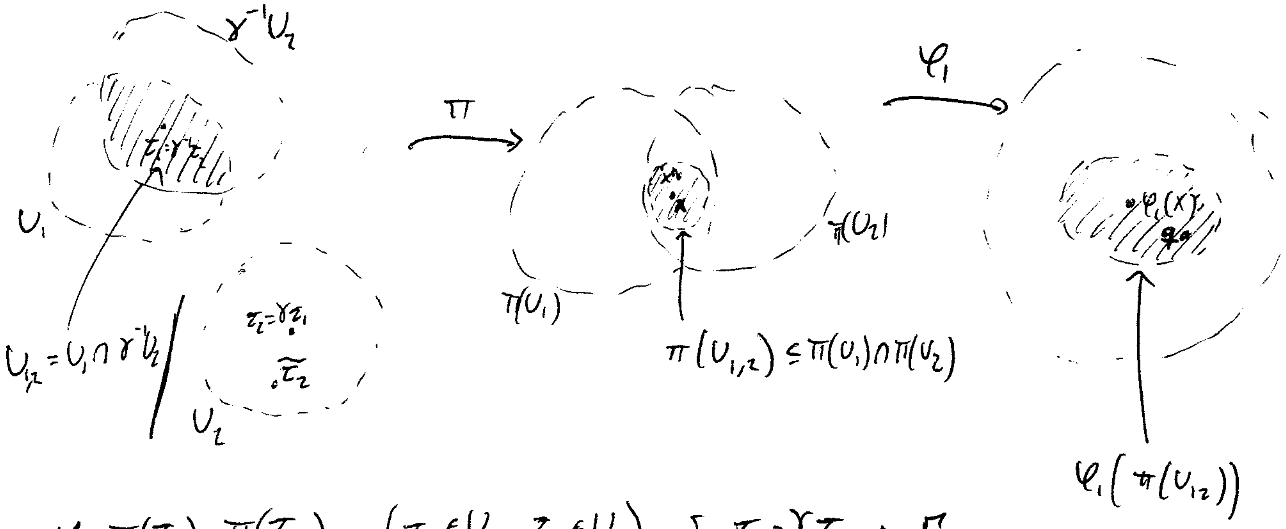
As everything is continuous + open, φ is 1-1 and surjective + cont + open $\Rightarrow$ homeo.

Note: This also works when $h_\tau = 1$.

We need to check now that the charts are coherent on intersections:

$$\begin{tikzcd} & V_{1,2} \subseteq \mathbb{C} \arrow[d, "\varphi_{2,1} := \varphi_2 \circ \varphi_1^{-1}"] \\ \pi(U_1) \cap \pi(U_2) \arrow[ur, "\varphi_1"] \arrow[dr, "\varphi_2"'] & \\ & V_{2,1} \subseteq \mathbb{C} \end{tikzcd}$$

transition map
↓
$\varphi_{2,1}$ is a bijection. We want it to be holomorphic.



$x = \pi(\tau_1) = \pi(\tau_2)$ $(\tau_1 \in U_1,\ \tau_2 \in U_2)$. So $\tau_2 = \gamma\tau_1$, $\gamma \in \Gamma$.

"<u>WLOG</u>": Assume $\varphi_1(x) = 0$. (computations are easier, the general case follows).
▼ $q \neq e^{2\pi i z}$!! it's just a variable!

Pf. $\varphi_1(x') = q$. Then $\varphi_{2,1}(q) = \varphi_2(x')$

<u>We compute $\varphi_1(x')$</u>:

Let τ' be st $\pi(\tau') = x'$ $(\tau' \in U_{1,2} \overset{\subseteq U_1}{})$.

So $\varphi_1(x') = \psi_1(\tau') = (\delta_1(\tau'))^{h_1}$. Hence $q = (\delta_1(\tau'))^{h_1}$.

Let $\tilde{\tau}_2 \in U_2$ be such that $\psi_2(\tilde{\tau}_2) = 0$ (ie $\varphi_2(\pi(\tilde{\tau}_2)) = 0$).

Let h_2 be the period of $\tilde{\tau}_2$.

<u>Now we compute $\varphi_2(x')$</u>.

$\tau' \in U_{1,2} \subseteq \gamma^{-1}U_2 \Rightarrow \gamma\tau' \in U_2$.

So $\varphi_2(x') = \psi_2(\gamma\tau') = (\delta_2(\gamma\tau'))^{h_2} = \left((\delta_2\gamma\delta_1^{-1})\overset{q^{1/h_1}}{\overset{\shortparallel}{\overbrace{(\delta_1\tau')}}}\right)^{h_2} \Rightarrow$

$\Rightarrow \varphi_{2,1}(q) = \varphi_2(x') = \left((\delta_2\gamma\delta_1^{-1})q^{1/h_1}\right)^{h_2}$

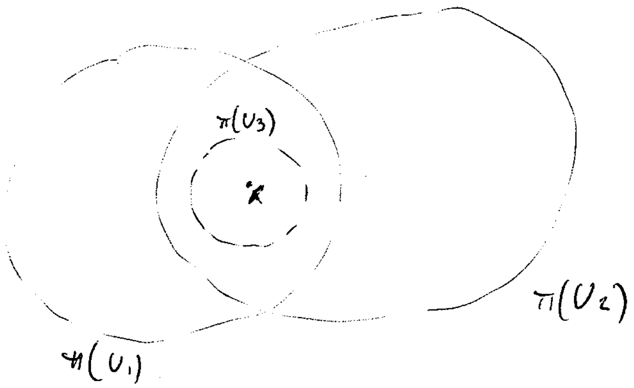
<u>Note</u>: if $h_1 = 1$, then φ_{21} is holomorphic!

What if $h_1 > 1$? Then U_2 has <u>exactly</u> 1 elliptic point, which has to be τ_2, and it has to be the one st. $\psi_2(\tau_2) = 0$ (ie. $\tilde{\tau}_2 = \tau_2$). In this case, as $\tau_2 = \gamma\tau_1$, $h_1 = h_2 \Rightarrow$ <u>ok!!</u>

Last thing to do: remove the assumption $\varphi_1(x)=0$.

We are done if $\varphi_1(x)=0$ or $\varphi_2(x)=0$ (inverse of hol. map is hol.).

So if $\varphi_1(x)\neq 0$, $\varphi_2(x)\neq 0$:



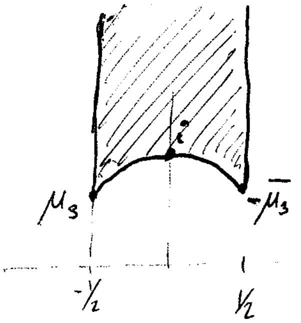
Make x the center of φ_3 i.e. $\varphi_3(x)=0$. (we've shrinked the domain of φ_3 s.t. it's inside the intersect.)

$$\begin{tikzcd}
\pi(U_3) \arrow[r, "\varphi_1"] & V_{1,3}=V_{1,2} \arrow[d, "\varphi_{3,1}\text{ hol}"] \\
\pi(U_1) \arrow[r, "\varphi_3"] & V_{3,1}=V_{3,2} \arrow[d, "\varphi_{23}\text{ hol}"'] \\
\pi(U_3) \arrow[r, "\varphi_2"] & V_{2,3} \\
& = V_{2,1}
\end{tikzcd}$$

$\Rightarrow$ $\varphi_{23}\circ\varphi_{31}$ is holomorphic

So $\varphi_{23}\circ\varphi_{31} : V_{1,2} \to V_{2,1}$ is hol.

• Elliptic Points



$\mu_3 = e^{2\pi i/3}$

$D = \{\tau\in H : \frac{-1}{2} \leq \mathrm{Re}(\tau) \leq \frac{1}{2},\ |\tau|\geq 1\{$ is a fundamental domain for the action of $SL_2(\mathbb{Z})$, which is what the following says:

Prop: a) The map $\pi : D \to SL_2(\mathbb{Z})\backslash H$ is a surjection.

b) If $\pi(\tau_1)=\pi(\tau_2)$, $\tau_1,\tau_2\in D$, then either

1) $\tau_2 = \tau_1 \pm 1$

2) $|\tau_1|=1$, $\tau_2 = -1/\tau_1$.

Pf See Book, or Koblitz or Serre.

· Elliptic points for $SL_2(\mathbb{Z})$.

Suppose $\gamma\tau=\tau$, $\gamma=\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{Z})$. (quadratic formula) $+ (\tau\in\mathbb{H})$

This is iff $c\tau^2+(d-a)\tau-b=0 \overset{\downarrow}{\iff} |a+d|<2 \Rightarrow$

$\Rightarrow |\operatorname{tr}\gamma|<2$ and recall $\det\gamma=1$.

So the characteristic polynomial is one of $x^2\pm1$, $x^2\pm x+1$.

Hence either $\gamma^4=1$ or $\gamma^6=1 \Rightarrow \gamma$ has order $1,2,3,4,6$.

If γ has order 1 or 2, then $\gamma=\pm I$.

<u>Prop 2.6</u>:

a) If γ has order 4, then γ is conjugate to $\begin{pmatrix}0&-1\\1&0\end{pmatrix}^{\pm1}$ in $SL_2(\mathbb{Z})$.

b) " —— " —— 3 " ———— " —— " $\begin{pmatrix}0&1\\-1&-1\end{pmatrix}^{\pm1}$ — " —

c) " —— " 6 " ———— " ——— " $\begin{pmatrix}0&-1\\1&1\end{pmatrix}^{\pm1}$ — " ——

Pf Book //

<u>Note</u>: $\begin{pmatrix}0&-1\\1&0\end{pmatrix}$ fixes i. (only)

$\begin{pmatrix}0&-1\\1&1\end{pmatrix}=-I\cdot\begin{pmatrix}0&1\\-1&-1\end{pmatrix}$ fixes $\mu_3\left(=\frac{-1+\sqrt{-3}}{2}\right)$ (only).

So suppose now $\tau\in\mathbb{H}$ is fixed by a matrix γ with order 4.

Then $\gamma=\delta\begin{pmatrix}0&-1\\1&0\end{pmatrix}^{\pm1}\cdot\delta^{-1}$ for some $\delta\in SL_2(\mathbb{Z})$. So $\gamma\tau=\tau\iff\delta\begin{pmatrix}0&-1\\1&0\end{pmatrix}^{\pm1}\delta^{-1}\tau=\tau$

$\iff\begin{pmatrix}0&-1\\1&0\end{pmatrix}^{\pm1}(\delta^{-1}\tau)=\delta^{-1}\tau \Rightarrow \delta^{-1}\tau=i \Rightarrow \tau=\delta i$.

In other words, $SL_2(\mathbb{Z})\tau=SL_2(\mathbb{Z})i$.

For order 3 or 6, it will be a translate of μ_3.

Corollary 2.7: Let $\pi : \mathbb{H} \longrightarrow Y(1) = \mathbb{H}/SL_2(\mathbb{Z}) = \mathbb{H}/\Gamma(1)$.

a) if τ is elliptic for $SL_2(\mathbb{Z})$, then either $\tau \in SL_2(\mathbb{Z})\cdot i$ or $\tau \in SL_2(\mathbb{Z})\mu_3$.

b) $\pi(i)$ and $\pi(\mu_3)$ are the only elliptic points in $Y(1)$.

c) $SL_2(\mathbb{Z})_i = \langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle$ (stabilizer) (order 4).

$SL_2(\mathbb{Z})_{\mu_3} = \langle \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \rangle$ " (order 6)

d) $\tau \in \mathbb{H}$ elliptic $\Rightarrow SL_2(\mathbb{Z})_\tau$ is conjugate to either $SL_2(\mathbb{Z})_i$ or $SL_2(\mathbb{Z})_\tau$.

Suppose now that Γ is a congruence subgroup.

τ elliptic for $\Gamma \Rightarrow \tau$ elliptic for $SL_2(\mathbb{Z})$.

Hence $\Gamma_\tau = \Gamma \cap SL_2(\mathbb{Z})_\tau \Rightarrow \Gamma_\tau$ is finite cyclic, and of order 4 or 6 (still assuming that $\pm I \in \Gamma$!).

Write $SL_2(\mathbb{Z}) = \bigcup_{j=1}^{d} \Gamma\gamma_j$, coset decomposition.

Then if τ is elliptic for Γ, then either $\tau \in SL_2(\mathbb{Z})\cdot i$ or $SL_2(\mathbb{Z})\cdot\mu_3$.

$\Rightarrow$ $\tau \in \Gamma(\gamma_j i)$ (some j) or $\tau \in \Gamma(\gamma_j \mu_3)$ (some j). $\leftarrow$ finite # of possibilities!

Corollary 2.8: $Y(\Gamma)$ has finitely many elliptic points.

Example: $\Gamma = \Gamma_1(N)$, $N > 3$. $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$ $\swarrow \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N$ suppose γ fixes τ.

So $|a+d| < 2$, and $a+d \equiv 2 \bmod N \underset{N>3}{\Rightarrow}$ contradiction. So there are no elliptic points in $\Gamma_1(N)(N>3)$. //

(Same for $\Gamma = \Gamma(N)$).

$\Gamma_0(3)$ Example

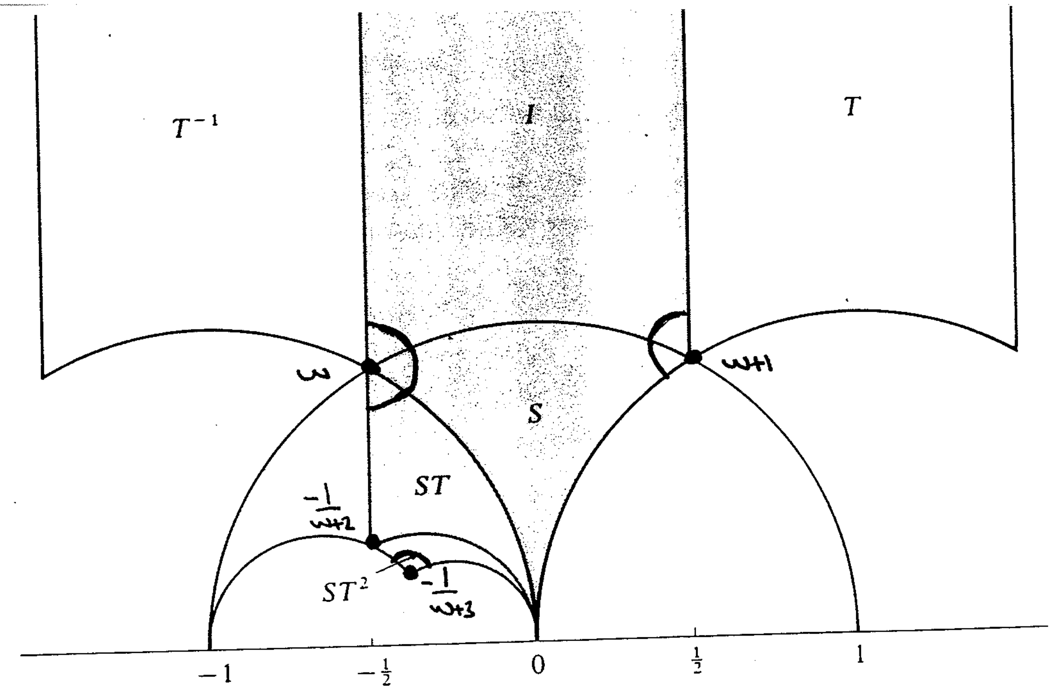


Figure 4.1 Fundamental region for $\Gamma_0(3)$

$S=\begin{pmatrix}0&-1\\1&0\end{pmatrix}$

$T=\begin{pmatrix}1&1\\0&1\end{pmatrix}$

$\omega=e^{2\pi i/3}$
$=\frac{-1+\sqrt{-3}}{2}$

- Points which are $SL_2(\mathbb{Z})$-equivalent to ω:

  $\omega,\ \omega+1,\ \frac{-1}{\omega+2},\ \frac{-1}{\omega+3}$

- ω is $\Gamma_0(3)$ equivalent to $\omega+1=\begin{pmatrix}1&1\\0&1\end{pmatrix}\omega$

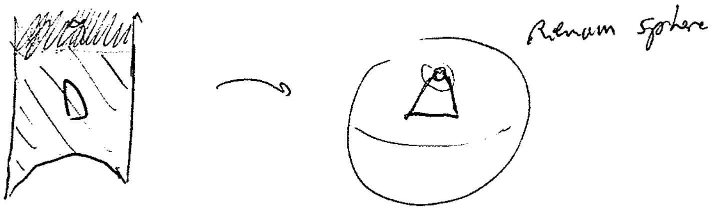
  and to $\frac{-1}{\omega+3}=\begin{pmatrix}-1&-1\\3&2\end{pmatrix}\omega$

  So these 3 points are identified in $X_0(3)$, and so $\pi(\omega)\in X_0(3)$ is not elliptic.
  (The semicircles drawn come together to form a "whole" neighborhood of $\pi(\omega)$)

- $\frac{-1}{\omega+2}$ is stabilized by $\begin{pmatrix}-2&-1\\3&1\end{pmatrix}\in\Gamma_0(3)$

  So its isotropy group in $\Gamma_0(3)$ has order 6.
  So $\pi\left(\frac{-1}{\omega+2}\right)\in X_0(3)$ is elliptic, with period 3

  (Note that only 2 of the 6 semicircles needed for a complete neighborhood are there)



$D^* := D \cup \{\infty\}$ is compact (are $\Gamma = SL_2(\mathbb{Z})$.).

<u>Cusps</u>: are $\mathbb{Q} \cup \{\infty\} \subseteq \mathbb{C}^*$. We've shown that $SL_2(\mathbb{Z})$ acts transitively on them.

If Γ is a congruence subgroup, then Γ acts on $\mathbb{Q} \cup \{\infty\}$ (maybe not trans.).

<u>Cusps of Γ</u>: they are the orbits $\Gamma \cdot s \subseteq \mathbb{Q} \cup \{\infty\}$ under this action.

(so $SL_2(\mathbb{Z})$ has only one cusp).

Can write $SL_2(\mathbb{Z}) = \bigcup_{j=1}^{d} \Gamma \gamma_j$ (coset decomposition).

If s is a cusp, then $s \in SL_2(\mathbb{Z}) \cdot \infty = \bigcup_{j=1}^{d} \Gamma(\gamma_j \infty)$ $\Rightarrow$ cusps are represented by finitely many elts. of $\mathbb{Q} \cup \{\infty\}$: $\{\gamma_1 \infty, \gamma_2 \infty, \ldots, \gamma_d \infty\}$.

(these need not be n distinct orbits! can have less cusps than d!).

<u>Example</u>: $[SL_2(\mathbb{Z}) : \Gamma_0(p)] = p+1$ but there are only two cusps: $0, \infty$.

<u>Compactification of $Y(\Gamma)$</u>

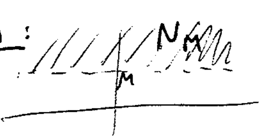
Let $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ $(= \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}))$. Let Γ a congruence subgroup.

Define $X(\Gamma) := {}_{\Gamma}\backslash^{\mathbb{H}^*}$, $\pi : \mathbb{H}^* \longrightarrow X(\Gamma)$.

We will give $X(\Gamma)$ the quotient topology, so we need to give a topology for $\mathbb{H}^*$.

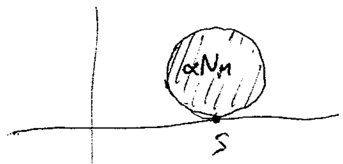
<u>Topology for $\mathbb{H}^*$</u>:

<u>At ∞</u>:



define $N_M := \{\tau \in \mathbb{H} : \operatorname{Im} \tau > M\}$. These form a basis of neighborhoods at ∞ (definition).

<u>At $s = \alpha \infty$</u>: The neighborhood basis is $\alpha \cdot N_M$. Know that α takes lines to circle/line.



$\leftarrow \alpha N_M$ is a circle, tangent to $\mathbb{R}$ at s.

Note: if $s' \in \mathbb{Q}$, $s' \neq s$, then all $s \notin \alpha N_M$ for any M.

Proposition 2.9: $X(\Gamma)$ is compact and connected and Hausdorff

Pf.
- **Compact**: $D^* = D \cup \{\infty\}$ is compact. Note that $\mathbb{H}^* = SL_2(\mathbb{Z}) \cdot D^* =$

$$= \left(\bigcup_{j=1}^{d} \Gamma \gamma_j\right) D^* \Rightarrow X(\Gamma) = \pi(\mathbb{H}^*) = \bigcup_{j=1}^{d} \pi(\gamma_j D^*) \Rightarrow$$

$\Rightarrow X(\Gamma)$ is a finite union of compact sets (as π continuous and $\gamma_j D^*$ compact)

- **Connected**: Enough to show that $\mathbb{H}^*$ is connected:
  if $H^* = U_1 \sqcup U_2$, U_i open, then since $\mathbb{H}$ is connected,
  we get one of them $\supseteq \mathbb{H}$, say $\mathbb{H} \subseteq U_1$.
  So $U_2 \subseteq \mathbb{Q} \cup \{\infty\}$. $\Rightarrow U_2 = \emptyset \Rightarrow$!! //

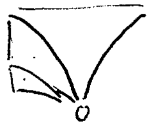
- **Hausdorff**: exercise. //

Fact: if $M > 1$, then N_M has no elliptic points.

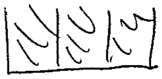
Hence, if $\tau_1, \tau_2 \in N_M$ have $\pi(\tau_1) = \pi(\tau_2)$, then $\tau_1 = \tau_2 + m$ for some $m \in \mathbb{Z}$.

Example:

$\Gamma_0(3)$.



$\leftarrow$ 3 triangles meet at 0 $\xrightarrow{\delta = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}}$ $\delta 0 = \infty$



3 strips $\xrightarrow{q \mapsto e^{2\pi i \tau/3}}$

This is what we will do.

General Case:

Let s be a cusp. In principle, ∞ thly many triangles meet at s. But how many of them are inequivalent?

Q: when $\pi(\tau_1)=\pi(\tau_2)$? Let δ s.t. $\delta s=\infty$

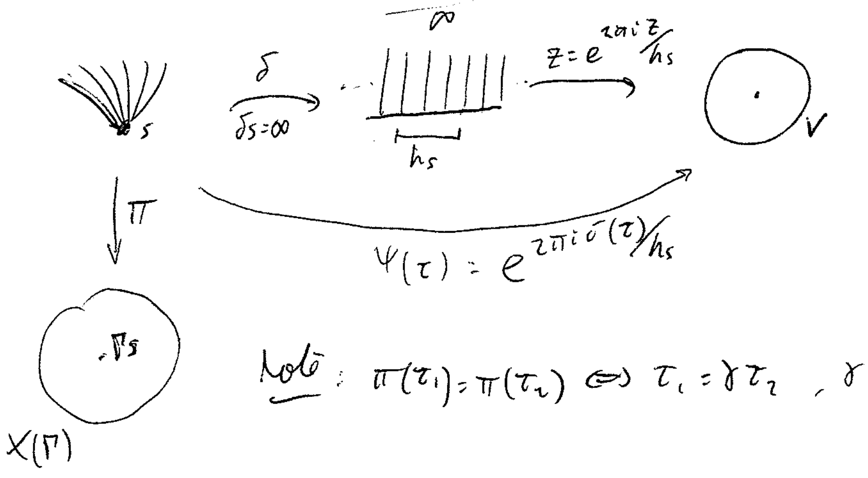
$\Gamma\tau_1=\Gamma\tau_2 \Leftrightarrow (\delta\Gamma\delta^{-1})(\delta\tau_1)=(\delta\Gamma\delta^{-1})\delta\tau_2 \Leftrightarrow (\delta\gamma\delta^{-1})\,\delta\tau_1=\delta\tau_2$ for some $\gamma\in\Gamma$. $\underset{\text{prev. fact}}{\Rightarrow}$ $\delta\gamma\delta^{-1}$ is a translation $=\pm\begin{pmatrix}1&m\\0&1\end{pmatrix}$ some m.

i.e. $\delta\gamma\delta^{-1}\in SL_2(\mathbb{Z})_\infty$ (stabilizer of ∞)

Consider now $(\delta\Gamma\delta^{-1})\cap SL_2(\mathbb{Z})_\infty$. It has the form $\pm\langle\begin{pmatrix}1&h\\0&1\end{pmatrix}\rangle$ for a unique $h>0$. (as $SL_2(\mathbb{Z})_\infty=\pm\langle\begin{pmatrix}1&1\\0&1\end{pmatrix}\rangle$).

Define then $h_s := h$, called the width of the cusp s.

One can check: h_s depends only on Γs (orbit of s).
(i.e. $h_{\gamma s}=h_s$ $\forall\gamma\in\Gamma$).



Note: $\pi(\tau_1)=\pi(\tau_2)\Leftrightarrow\tau_1=\gamma\tau_2$, $\gamma\in\Gamma \Leftrightarrow \delta\tau_1=(\delta\gamma\delta^{-1})\delta\tau_2$

As there are no elliptic points over $\mathrm{Im}(z)=1$, then $\delta\gamma\delta^{-1}\in\delta\Gamma\delta^{-1}\cap SL_2(\mathbb{Z})_\infty \Rightarrow$

$\Rightarrow \delta\gamma\delta^{-1}=\pm\begin{pmatrix}1&h_s\\0&1\end{pmatrix}^m$ some m $\Leftrightarrow \delta\tau_1=\delta\tau_2+mh_s \Leftrightarrow \psi(\tau_1)=\psi(\tau_2)$.

So we have:

$$\begin{tikzcd} U \arrow[r, "\psi"] \arrow[d] & V \\ \pi(U) \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

Define $\varphi(\pi(\tau)) := \psi(\tau)$, and check that it's a homeomorphism with holomorphic transition maps.

Ch 3.1. The Genus.

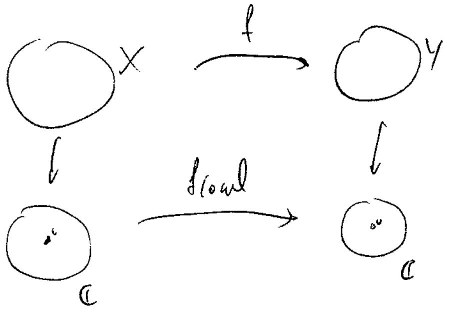
$X(\Gamma) = \Gamma\backslash\mathcal{H}^*$ has genus g

If one triangulates it with v vertices, e edges, f faces, then $v - e + f = 2 - 2g$.

Consider the map

$$X(\Gamma) \longrightarrow X(\overset{SL_2(\mathbb{Z})}{\overset{\shortparallel}{\Gamma(1)}}).$$
$$\Gamma\tau \longmapsto SL_2(\mathbb{Z})\tau$$

For $f: X \to Y$ holomorphic nonconstant between compact Riemann surface ($\Rightarrow f$ surjective), then:



$$f_{local} = a_k z^k + \cdots = z^k(a_k + a_{k+1}z + \cdot)$$
$$= \psi(z)^k$$

So can assume $f_{local}(z) = z^k$

Define $e_x := k$ (Ramification index at x).

Say that x is ramified if $e_x > 1$. (only finitely-many num. points are ramified).

Lemma 3.1: Given f as above, $\exists d$ s.t.:

(skip pf). $\displaystyle\sum_{x \in f^{-1}(y)} e_x = d \quad \forall y \in Y.$ (note: $f^{-1}(y)$ is a finite set (discrete + everything compact)).

Def d is called the degree of f..

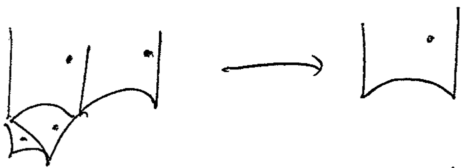
By taking a triangulation on Y that includes all ramified points, then looking at f^{-1}(triangulation) one gets:

Riemann-Hurwitz Formula: Let $f: X \to Y$ be nonconstant holomorphic map of degree d.

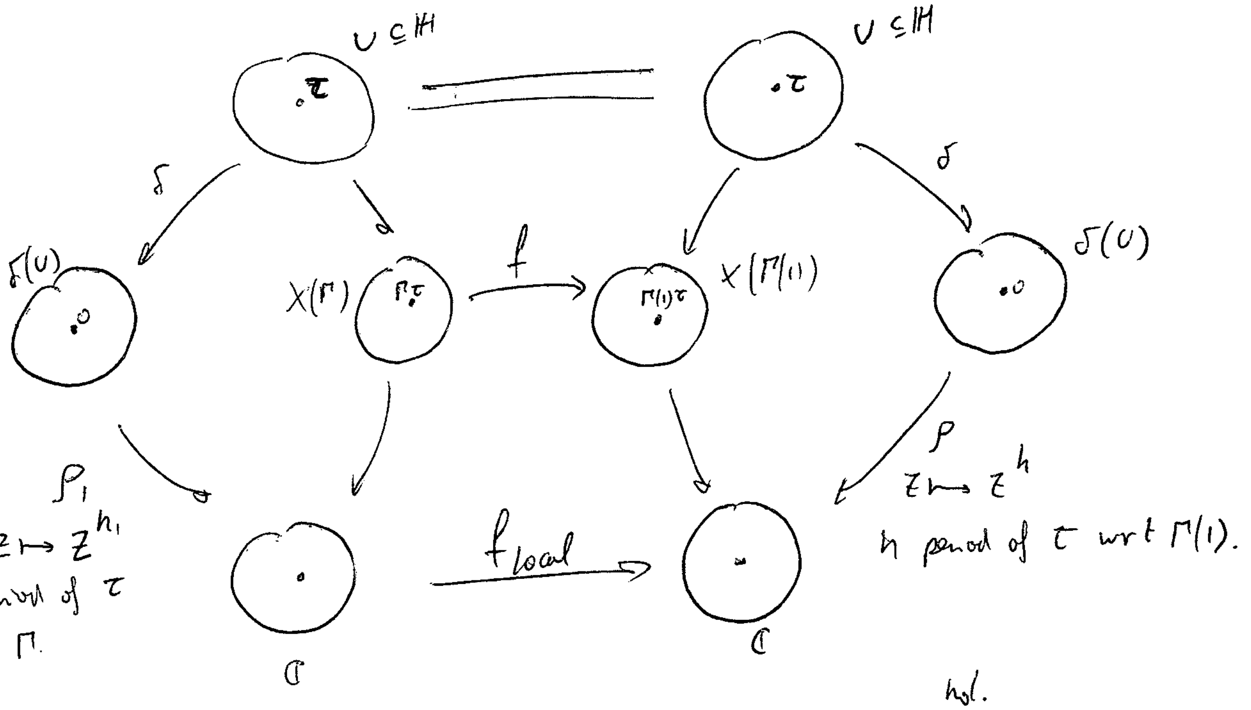
$$2g_X - 2 = d \cdot (2g_Y - 2) + \sum_{x \in X} (e_x - 1)$$

Let Γ be any congruence subgroup, and let $X = X(\Gamma)$, $Y = X(\Gamma(1))$.

Let $f: X \to Y$, $\Gamma\tau \mapsto \Gamma(1)\tau$.



$\deg f = [\Gamma(1) : \Gamma]$.



f_{local} takes the form $z^{h_1} \mapsto z^h$, i.e. $z \mapsto {}^{h}/_{h_1} \overset{\text{hol.}}{\Rightarrow} h_1 | h$.

Note also that $h = 1, 2, 3$.

Cases:

a) $h = 1 \Rightarrow h_1 = 1 \Rightarrow f$ unramified at $\Gamma\tau$ $\quad$ ($h = 1 \Leftrightarrow \tau$ not elliptic in $SL_2(\mathbb{Z})$).

b) $h = 2, 3 \Rightarrow \begin{cases} h_1 = 1 \Rightarrow f \text{ ramified at } \Gamma\tau, \text{ with ram. index } h. \\ h_1 = h \Rightarrow f \text{ unramified at } \Gamma\tau. \end{cases}$

Recap: $\tau \in \mathbb{H}$, $x = \pi(\tau) \in X(\Gamma)$.

We saw:

$$e_x = \begin{cases} 1 & \text{if } \tau \text{ not elliptic for } SL_2(\mathbb{Z}) \text{ or } \tau \text{ elliptic for } \Gamma(1) \text{ and } \Gamma. \\ h & \text{if } \tau \text{ is elliptic of order } h \text{ for } \Gamma(1) \text{ but not for } \Gamma. \end{cases}$$

Now we compute: Let $y_h \in X(\Gamma(1))$ elliptic of order h $(h=2,3)$.

~~Df~~: Call ε_h := # points of order h and ε_∞ := # cusps, of Γ.

Then we know $d = \sum_{x \in f^{-1}(y_h)} e_x = \sum_{x \text{ ell.}} 1 + \sum_{x \text{ not ell.}} h = \varepsilon_h + h(\#f^{-1}(y_h) - \varepsilon_h)$.

Then
$$\boxed{\sum_{x \in f^{-1}(y_h)} (e_x - 1)} = \sum_{x \in f^{-1}(y_h)} e_x - \#f^{-1}(y_h) = \cancel{\frac{h-1}{h}(\#f^{-1}(y_h) - \varepsilon_h)}\ (h-1)(\#f^{-1}(y_h) - \varepsilon_h)$$

(use $d = \varepsilon_h + h(\dots)$) $= \boxed{\frac{h-1}{h}(d - \varepsilon_h)}$.

Also,
$$\boxed{\sum_{x \in f^{-1}(y_\infty)} (e_x - 1) = d - \varepsilon_\infty}$$

From this, we get:

Thm 3.2: the genus g of $X(\Gamma)$ is:

$$g = 1 + \frac{[\Gamma(1) : \Gamma]}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2}.$$

All the quantities in RHS $(\varepsilon_2, \varepsilon_3, \varepsilon_\infty)$ can be easily computed (see section 3.7, 3.8 in the book).

e.g.
$$\varepsilon_2(\Gamma_0(N)) = \begin{cases} 0 & \text{if } 4 \mid N \\ \prod_{p \mid N} \left(1 + \left(\frac{-1}{p}\right)\right) & \text{if } 4 \nmid N. \end{cases}$$

§3.2. Automorphic Forms

Automorphic Forms of wt K $\longleftrightarrow$ meromorphic modular forms of wt K.

So $f \in A_K(\Gamma) \Leftrightarrow$ 1) f meromorphic on $\mathbb{H}$.

2) $f[\gamma]_k = f \quad \forall \gamma \in \Gamma$.

3) $f[\alpha]_k$ meromorphic at ∞ $\forall \alpha \in SL_2(\mathbb{Z})$.

$\updownarrow$ differentials on $X(\Gamma)$

$\Omega^{\otimes k/2}(X(\Gamma))$

Recall: $f[\gamma]_k(z) := j(\gamma, z)^{-k} f(\gamma z) = (cz+d)^{-k} f(\gamma z)$.

Examples:

1) $A_0(SL_2(\mathbb{Z})) = \mathbb{C}(j(z))$, $\quad j(z) = \dfrac{E_4^3(z)}{\Delta(z)} = q^{-1} + 744 + \cdots$

(see the proof in the notes from Koblitz or in the book).

2) $j(\gamma z) = j(z)$ $\forall \gamma$. So $j'(\gamma z) \cdot \dfrac{d\gamma z}{dz} = j'(z) \Rightarrow j'(\gamma z)(cz+d)^{-2} = j'(z)$

so $j'(z)$ is in $A_2(SL_2(\mathbb{Z}))$.

In fact, $j'(z)$ is then in $A_2(\Gamma)$ $\forall \Gamma \subseteq SL_2(\mathbb{Z})$.

(it's not true in general that $f \in A_K(\Gamma) \Rightarrow f' \in A_{K+2}(\Gamma)$) $\swarrow$ only for $K=0$!

3) So $j'(z)^n \in A_{2n}(\Gamma)$ $\forall n \in \mathbb{Z}$, so in particular they are nontrivial spaces.

3) If $f, g \in A_K(\Gamma)$, $f \neq 0$, then $\dfrac{g}{f} \in A_0(\Gamma) \Rightarrow A_K(\Gamma)$ is a 1-dimensional $A_0(\Gamma)$ vectorspace: $A_K(\Gamma) = A_0(\Gamma) \cdot f$ (for any nonzero $f \in A_K(\Gamma)$).

If $f \in A_K(\Gamma)$, then $f(\gamma z) = (cz+d)^k f(z)$. So it doesn't define a function on $X(\Gamma)$ (unless $f=0$ or $k=0$).

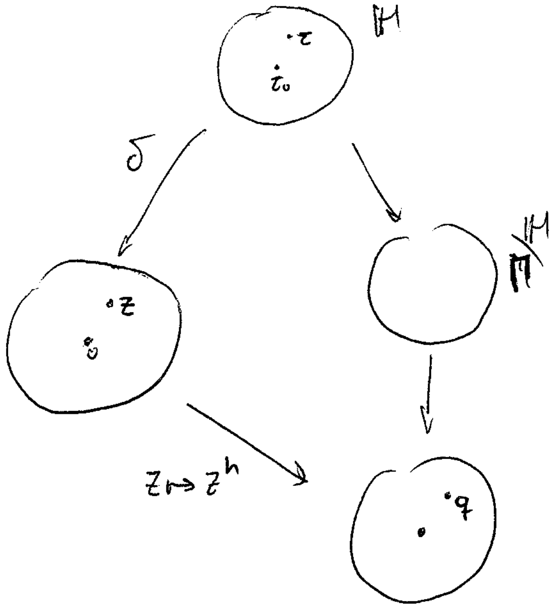
However, $(cz+d)^k \neq 0, \infty$. So the order of vanishing is well-defined.

So if $\tau_0 \in \mathbb{H}$, $f(\tau) = a_{n_0}(\tau-\tau_0)^{n_0} + \cdots$

and define $\nu_{\tau_0}(f) := n_0$ (well-defined).

So: $f \in A_k(\Gamma) \Rightarrow \nu_{\tau_0}(f) = \nu_{\gamma\tau_0}(f) \quad \forall \gamma \in \Gamma$.

We want ~~to~~ define $\nu_{\pi(\tau_0)}(f)$, where $\pi : \mathbb{H} \longrightarrow {}_{\Gamma}\backslash\mathbb{H}$.



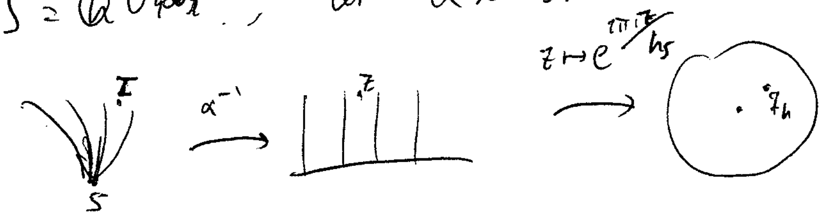
$$\sigma(\tau) = z = (\tau-\tau_0)\overbrace{\sigma_1(\tau)}^{\text{non } 0,\ \text{non } \infty}$$

$$\text{So} \quad q = z^h = (\tau-\tau_0)^h \underbrace{(\sigma_1(\tau))^h}_{\text{hol. non } 0}$$

Def: $\nu_{\pi(\tau_0)}(f) := \dfrac{\nu_{\tau_0}(f)}{h}$.

!! We no longer assume $-I \in \Gamma$. !!

$s = \mathbb{Q} \cup \{\infty\}$, let $\alpha\infty = s$.



Local variable: $q_h = e^{\frac{2\pi i z}{h_s}}$, $z = \alpha^{-1}\tau$

h_s is defined by: $\pm I(\alpha^{-1}\Gamma\alpha)_\infty = \pm I \cdot \left\langle \begin{pmatrix} 1 & h_s \\ 0 & 1 \end{pmatrix} \right\rangle \quad h_s > 0$.

Given $f \in A_k(\Gamma)$, can represent it locally by $g(q)$, which ~~is~~ not necessarily analytic (as f is not a function on ${}_{\Gamma}\backslash\mathbb{H}$!).

Have 3 possibilities:

1) $(\alpha^{-1}\Gamma\alpha)_\infty = \pm I \cdot \langle \begin{pmatrix} 1 & h_s \\ 0 & 1 \end{pmatrix} \rangle$

2) $(\alpha^{-1}\Gamma\alpha)_\infty = \langle \begin{pmatrix} 1 & h_s \\ 0 & 1 \end{pmatrix} \rangle$

3) $(\alpha^{-1}\Gamma\alpha)_\infty = \langle -\begin{pmatrix} 1 & h_s \\ 0 & 1 \end{pmatrix} \rangle$.

Now, let $f \in A_k(\Gamma)$. Then $g(z) = f[\alpha]_k$ is invariant under $\alpha^{-1}\Gamma\alpha$.

Case (1),(2):

Have $g(z+h_s) \overset{\begin{pmatrix} 1 & h_s \\ 0 & 1 \end{pmatrix} \in (\alpha^{-1}\Gamma\alpha)_\infty}{\overset{\downarrow}{=}} g(z) \Rightarrow g(z)$ has a Fourier exp $= \sum_{n \geq n_0} a(n) q_{h_s}^n$.

So can define $V_{\pi(s)}(f) := n_0$.

Case (3)

a) k even:

$f[-I]_k = f \Rightarrow g(z+h_s) = g(z)$ and we have no problem: $V_{\pi(s)}(f) := n_0$.

b) k odd:

$f[-I]_k = -f$. So $g(z+h_s) = -g(z) \Rightarrow g(z+2h_s) = g(z)$.

Hence $g(z) = \sum_{n \geq n_0} a(n) q_{2h_s}^n$, and q_{2h_s} is the square-root of the local variable.

In this case, define $V_{\pi(s)}(f) := \frac{n_0}{2}$.

Rk: $g(z)$ is an odd function $\Rightarrow a(2k) = 0 \ \forall k$.

In particular, $V_{\pi(s)}(f)$ is never an integer.

Def: Say s is regular (for Γ, k) if case 1, 2, 3a.

s is irregular (for Γ, k) if case 3b.

Example: $s = \frac{1}{2}$ is irregular for $\Gamma_1(4)$ when k is odd.

Good news: $s=\frac{1}{2}$, $\Gamma_1(4)$, k odd is the only irregular cusp for $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$!!!

Meromorphic differentials.

Idea: $f(\tau) \in A_{2n}(\Gamma)$. Then $f(\gamma\tau)(d(\gamma\tau))^n = f(\tau)(d\tau)^n \cdot$ (formally).

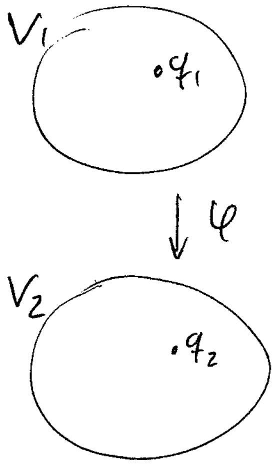
So $\omega = f(\tau)(d\tau)^n$ should be defined on $X(\Gamma)$.

ω will be called a differential of degree n.

For $V \subseteq \mathbb{C}$ an open, $\Omega^{\otimes n}(V) := \{ f(q)(dq)^n : f \text{ meromorphic on } V \}$.

which is a $\mathbb{C}$-vectorspace.

Now, make the chain rule work:



$$\omega_1 = f(\varphi(q_1))(\varphi'(q_1))^n (dq_1)^n = \varphi^* \omega_2 \in \Omega^{\otimes n}(V_1)$$

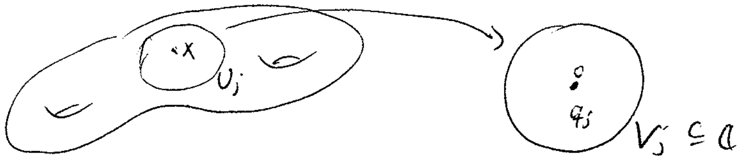
$\uparrow$ ← change of vars: $dq_2 = \varphi'(q_1)\,dq_1$

$\Uparrow$ pullback of ω_2.

$q_2 = \varphi(q_1)$. $\omega_2 = f(q_2)(dq_2)^n$

The pullback is contravariant: $(\varphi \circ \psi)^* = \psi^* \circ \varphi^*$.

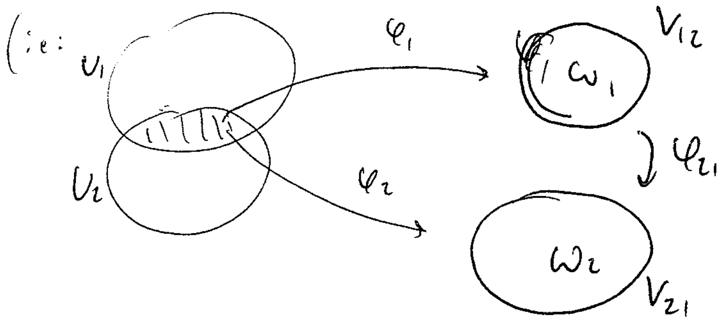
Let $X (= X(\Gamma))$ a cpct Riemann surface.



we have $\omega_j = f_j(q_j)(dq_j)^n$.

Def: An element $\omega \in \Omega^{\otimes n}(X)$ is a collection $\omega = (\omega_j)_j$ (one for each chart) which are compatible w.r.t. coordinate change.

(ie:



Require: $\boxed{\varphi_{21}^*(\omega_2)=\omega_1}$)

Now, if $X = X(\Gamma)$ is our modular curve; given $\omega \in \Omega^{\otimes n}(X)$,

$$\begin{tikzcd}
\mathbb{H} \arrow[d, "\pi"'] & \pi^*\omega = f(\tau)(d\tau)^n \in \Omega^{\otimes n}(\mathbb{H}). \\
X & \omega \arrow[u, mapsto]
\end{tikzcd}$$

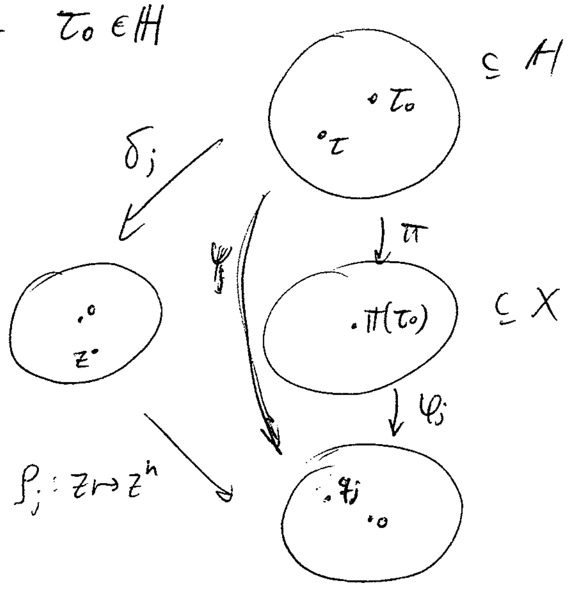
Note: $\gamma \in \Gamma \Rightarrow \gamma^* \circ \pi^* = (\pi \circ \gamma)^* = \pi^* \Rightarrow f(\gamma\tau)(d\gamma\tau)^n = f(\tau)(d\tau)^n.$

$\Rightarrow f(\tau) \in A_{2n}(\Gamma)$

↑ after checking meromorphicity (specially at cusps).

Conversely, suppose $f(\tau) \in A_{2n}(\Gamma)$. Want to produce $\omega \in \Omega^{\otimes}(X)$. (ie. a pack of ω_j's).

Spz $\tau_0 \in \mathbb{H}$



Use ψ_j to define

$$\omega_j = f(q_j)(dq_j)^n$$

(s.t. it pulls-back to $f(\tau)(d\tau)^n$)

Can check that ω_j so defined are compatible, so get $\omega \in \Omega^{\otimes n}(X)$.

·Problems to look at: 3.2.5, 3.4.3, 3.5.5

Thm 3.3: $\Omega^{\otimes n}(X(\Gamma)) \simeq A_{2n}(\Gamma)$ as $\mathbb{C}$-vectorspaces, under isomorphisms:

$$\omega \longmapsto f(\tau),$$

(where $\pi^*(\omega) = f(\tau)(d\tau)^n \in \Omega^{\otimes n}(\mathbb{H})$)

Abuse notation: $\omega = f(\tau)(d\tau)^n$

~~Pf~~ Done!

§3.4, 3.5. Riemann-Roch and Dimension formulas.

Write $X = X(\Gamma)$ the modular curve (works for any curve).

Def: The divisor group is $\mathrm{Div}(X) := \left\{ \sum_{x \in X} n_x \cdot x,\ n_x \in \mathbb{Z} \right\}$ free $\mathbb{Z}$module gen. by X.

If $D = \sum n_x \cdot x$, $D' = \sum n_x' \cdot x$, then $D \geqslant D'$ if $n_x \geqslant n_x'$ $\forall x \in X$.

Can define $\deg(D) = \sum n_x$.

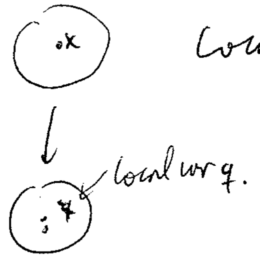
Functions: Let $f \overset{\neq 0}{\in} \mathbb{C}(X)$ ($\mathbb{C}(X)$ = field of meromorphic functions on X).

Define $\mathrm{div}(f) := \sum_{x \in X} v_x(f) \cdot x$.

Note: $\deg(\mathrm{div}(f)) = \sum v_x(f) = \#\text{zeros} - \#\text{poles} = d - d = 0$.

If we call $\mathrm{Div}^0(X) := \{ D \in \mathrm{Div}(X) : \deg D = 0 \}$ ← sgp of $\mathrm{Div}(X)$, then $\mathrm{div}(f) \in \mathrm{Div}^0(X)$.

Differentials: Let $\omega \in \Omega^{\otimes n}(X)$. $(\omega \neq 0)$.



Locally, $\omega_x = f_x(q)(dq)^n$ near $q=0$. Define $v_x(\omega) := v_0(f_x) \in \mathbb{Z}$.

So define $\mathrm{div}(\omega) = \sum_{x \in X} v_x(\omega) \cdot x$

<u>Def</u>: A <u>canonical divisor</u> is a divisor of the form $\mathrm{div}(\lambda)$, where $\lambda \in \Omega^{\otimes 1}(X)$.

<u>Lemma 3.4</u>:

1) If $\mathrm{div}(\lambda)$ is <u>canonical</u>, then $\deg(\mathrm{div}(\lambda)) = 2g-2$.

2) If $\omega \in \Omega^{\otimes n}(X)$, then $\deg(\mathrm{div}(\omega)) = n\cdot(2g-2) = 2n(g-1)$.

Pf (1) Later, using R-R. But actually can be done without, and is used to prove RR!!

(Pf)(2) <u>Crucial fact</u>: if $\omega \in \Omega^{\otimes n}(X)$, $\omega \neq 0$, then $\Omega^{\otimes n}(X) = \omega\cdot\mathbb{C}(X)$.

(as for $f \in A_{2n}(\Gamma)$, $f \neq 0$, then $A_{2n}(\Gamma) = \mathbb{C}(X(\Gamma))\cdot f$).

(Or just consider $\omega_1 \in \Omega^{\otimes n}(X)$, then check that $\frac{\omega_1}{\omega} \in \mathbb{C}(X)$.)

So then, if $\overset{\neq 0}{\lambda} \in \Omega^1(X)$, then $\omega = f_0\cdot\lambda^n$, $f_0 \in \mathbb{C}(X)$.

Then $\mathrm{div}(\omega) = \mathrm{div}(f_0) + n\cdot\mathrm{div}(\lambda) \Rightarrow \deg(\mathrm{div}\,\omega) = n\cdot\deg(\mathrm{div}\,\lambda) = n(2g-2)$ //

<u>Def</u> For D a divisor,

$$L(D) = \{f \in \mathbb{C}(X) : \mathrm{div}(f) + D \geq 0\} \cup \{0\}, \quad \ell(D) := \dim_{\mathbb{C}} L(D). \quad (\text{a priori}, \infty).$$

<u>Thm 3.5</u> (Riemann-Roch): X of genus g, $\mathrm{div}(\lambda)$ canonical, $D \in \mathrm{Div}(X)$. <u>Then</u>:

$$\ell(D) = \deg(D) - g + 1 + \ell(\mathrm{div}(\lambda) - D).$$

<u>Note 1</u>: $\overset{D=0}{L(0)} = \mathbb{C} \Rightarrow \ell(0) = 1 \Rightarrow 1 = -g + 1 + \ell(\mathrm{div}(\lambda)) \Rightarrow \boxed{\ell(\mathrm{div}\,\lambda) = g.}$

<u>$D = \mathrm{div}(\lambda)$</u> $\Rightarrow \ell(\mathrm{div}(\lambda)) = \deg(\mathrm{div}(\lambda)) - g + 1 + 1 \Rightarrow \boxed{\deg(\mathrm{div}\,\lambda) = 2g-2}.$

<u>Note 2</u>: Let $f \in L(D)$, $f \neq 0$. Then $\mathrm{div} f + D \geq 0 \Rightarrow \deg(\overset{0}{\mathrm{div} f}) + \deg D \geq 0 \Rightarrow \deg(D) \geq 0$

So if $\deg(D) < 0$, then $L(D) = \{0\}$.

<u>Corollary 3.6</u>: if $\deg D > \deg(\mathrm{div}\,\lambda) = 2g-2$, then $\boxed{\ell(D) = \deg D - g + 1.}$

We need to relate $M_k(\Gamma)$ to $L(D)$, to get dimension formulas for $M_k(\Gamma)$.

Take $f \in A_k(\Gamma)$, for <u>even k</u>.

Define $\mathrm{div}(f) := \sum_{x \in X} v_x(f)\cdot x \in \mathrm{Div}_{\mathbb{Q}}(X) = \mathrm{Div}(X) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Now $M_k(\Gamma) = \{ f \in A_k(\Gamma) : \mathrm{div}(f) \geq 0 \}$.

If we choose $\overset{0}{*}f \in A_k(\Gamma)$, then $A_k(\Gamma) = \mathbb{C}(X)\cdot f$.

So then $M_k(\Gamma) = \{ f_0 \cdot f : f_0 \in \mathbb{C}(X),\ \mathrm{div}(f_0 \cdot f) \geq 0 \} \overset{\text{as } \mathbb{C}\text{-vectorspace}}{\simeq} \{ f_0 \in \mathbb{C}(X) : \mathrm{div}(f_0) + \mathrm{div}(f) \geq 0 \}$

And $\{ f_0 \in \mathbb{C}(X) : \mathrm{div}(f_0) + \mathrm{div}(f) \geq 0 \} = L(\mathrm{div}(f)) = L(\lfloor \mathrm{div}(f) \rfloor)$

(where $\lfloor \sum n_x \cdot x \rfloor := \sum \lfloor n_x \rfloor \cdot x$).

<u>Conclusion</u>: $\dim_{\mathbb{C}}(M_k(\Gamma)) = \ell(\lfloor \mathrm{div}(f) \rfloor)$.

<u>Plan</u>: $\omega = f(\tau)(d\tau)^{k/2} \in \Omega^{\otimes k/2}(X)$.

<u>Know</u>: $\deg(\mathrm{div}(\omega)) = k(g-1)$. How div f relates to div ω?

① $x = \pi(\tau_0)$, $\tau_0 \in \mathbb{H}$, <u>period h</u>.

The local variable is $q = (\tau - \tau_0)^h \cdot \overset{\text{hol, nonzero}}{\overset{\downarrow}{\lambda(\tau)}}$

Locally at x: $\omega = \omega_x = \underbrace{f_x(q)\cdot\left(\frac{d\tau}{dq}\right)^{k/2}}(dq)^{k/2}$ ↖ order at 0?

$$\frac{dq}{d\tau} = h(\tau - \tau_0)^{h-1}\lambda(\tau) + (\tau - \tau_0)^h \lambda'(\tau).$$

$v_0\left(\frac{dq}{d\tau}\right) = \frac{h-1}{h}$, as $(\tau - \tau_0)^{h-1} \doteq q^{\frac{h-1}{h}}$

Hence $\boxed{v_x(\omega) = v_x(f) - \frac{k}{2}\cdot\frac{h-1}{h}}$

(II) ~~$X = \pi(s)$~~ $x = \pi(s)$, s a cusp.

Then the local variable is $q = e^{2\pi i \tau/h}$

$\frac{dq}{d\tau} = \frac{2\pi i}{h} q$, $v_0\left(\frac{d\tau}{dq}\right) = -1$.

So $v_x(\omega) = v_x(f) - \frac{k}{2}$ at cusps.

So now let $x_{2,i}$, $x_{3,i}$ be the elliptic points (of order 2 and 3), let $x_{\infty,i}$ be the cusps. Let $\varepsilon_2, \varepsilon_3, \varepsilon_\infty$ be the # of each.

Then $\boxed{\mathrm{div}(f) = \mathrm{div}(\omega) + \sum \frac{k}{4} x_{2,i} + \sum \frac{k}{3} x_{3,i} + \frac{k}{2}}$

Check: $\deg(\mathrm{div}(f)) \geq 2g-2$ (see book).

By R.R. (easy version) says: $\ell(\lfloor \mathrm{div} f \rfloor) = \deg \lfloor \mathrm{div} f \rfloor - g + 1$.

no floor, as k is even!

$\deg \lfloor \mathrm{div} f \rfloor = \deg(\mathrm{div}\, \omega) + \lfloor \frac{k}{4} \rfloor \varepsilon_2 + \lfloor \frac{k}{3} \rfloor \varepsilon_3 + \frac{k}{2} \varepsilon_\infty$

Hence $\ell(\lfloor \mathrm{div} f \rfloor) = \underbrace{\deg(\mathrm{div}\, \omega)}_{k(g-1)} + \lfloor \frac{k}{4} \rfloor \varepsilon_2 + \lfloor \frac{k}{3} \rfloor \varepsilon_3 + \frac{k}{2} \varepsilon_\infty$, we've just proven:

Theorem 3.7: if $k \geq 2$ is even, then

$$\dim_{\mathbb{C}}(M_k(\Gamma)) = (k-1)(g-1) + \lfloor \tfrac{k}{4} \rfloor \varepsilon_2 + \lfloor \tfrac{k}{3} \rfloor \varepsilon_3 + \tfrac{k}{2} \varepsilon_\infty$$

Note: $S_k(\Gamma) \doteq L(\lfloor \mathrm{div} f - \sum x_{\infty,i} \rfloor)$

So for $k \geq 4$ even, $\dim(S_k(\Gamma)) = \dim(M_k(\Gamma)) - \varepsilon_\infty$

"Motivating" example: $S_2(\Gamma)$.

Let $f \in S_2(\Gamma)$. so $\mathrm{div}(f) \geq \sum x_{\infty,i}$

$\updownarrow$

$\omega = f(\tau)\, d\tau \in \Omega^1(X) \Rightarrow \mathrm{div}(f) = \mathrm{div}(\omega) + \sum \frac{1}{2} x_{2,i} + \sum \frac{2}{3} x_{3,i} + \sum x_{\infty,i} \geq \sum x_{\infty,i}$

Always integer coeffs

$\Leftrightarrow \mathrm{div}(\omega) \geq 0$. $\{\omega \in \Omega^1(X) : \mathrm{div}(\omega) \geq 0\}$ = hol diff on $X = \Omega^1_{hol}(X)$.

(cont example): so $S_2(\Gamma) \overset{\sim}{\hookrightarrow} \Omega^1_{hol}(X)$.

Also, from $\mathrm{div}(f) = \mathrm{div}(\omega) + \sum \frac{1}{2} x_{2,i} + \sum \frac{2}{3} x_{3,i} \geq 0 \Rightarrow$ f vanishes at all elliptic points

Note also that $\dim S_2(\Gamma) = \ell\left(\lfloor \mathrm{div} f - \sum x_{\infty,i} \rfloor\right) = \ell(\mathrm{div}\,\omega) = g$, since $\mathrm{div}\,\omega$ is canonical.

§ Eta Function:

$$\eta(z) := q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1-q^n) \qquad q = e^{2\pi i z}$$

(so $\Delta(z) = \eta^{24}(z) \in S_{12}(SL_2(\mathbb{Z}))$)

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

Then $\eta\left(\frac{az+b}{cz+d}\right) = \varepsilon_{a,b,c,d}\,(cz+d)^{\frac{1}{2}}\,\eta(z)$. where ε_{abcd} is a 24th root of 1.

Dedekind sum: $S(h,k) := \sum_{r=1}^{k-1} \frac{r}{k}\left(\frac{hr}{k} - \left\lfloor \frac{hr}{k} \right\rfloor - \frac{1}{2}\right)$

(See Apostol's book. There's Dedekind's reciprocity...)

Theorem 4.1 (Dedekind): if $c > 0$, then

$$\varepsilon_{abcd} = \exp\left(\pi i\left(\frac{a+d}{12c} + S(-d,c)\right)\cdot(-i)^{1/2}\right)$$

Facts from chapter 3:

1) Γ cong. subg:

$$g = 1 + \frac{[SL_2(\mathbb{Z}):\Gamma]}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2}$$

2) $f \in A_k(\Gamma)$, then $\deg(\mathrm{div} f) = k(g-1) + \frac{k}{4}\varepsilon_2 + \frac{k}{3}\varepsilon_3 + \frac{k}{2}\varepsilon_\infty$

So: $\deg(\mathrm{div} f) = \frac{k}{12}[SL_2(\mathbb{Z}):\Gamma]$

Thm 3.9: If $f \in M_k(\Gamma)$, $f \not\equiv 0$, then f has exactly $\frac{k}{12}[SL_2(\mathbb{Z}):\Gamma]$ zeros.

Corollary: If $f \in M_k(\Gamma)$ has more than $\frac{k}{12}[SL_2(\mathbb{Z}):\Gamma]$ zeros, then $f \equiv 0$.

Recall: $\eta(z) = q^{1/24}\prod_{n=1}^{\infty}(1-q^n)$

The so-called Dedekind reciprocity laws allow us to build modular forms.

Eta-quotient:

$$f(z) = \eta(\delta_1 z)^{r_1}\,\eta(\delta_2(z))^{r_2}\cdots\eta(\delta_d z)^{r_d}, \quad r_i \in \mathbb{Z}, \quad \underline{\delta_i \in \mathbb{N}}$$

we can write it as $f(z) = \prod_{\delta | N} \eta(\delta z)^{r_\delta}$

Example: $f(z) = \dfrac{\eta^{\ell}(\ell z)}{\eta(z)}$, ℓ prime, $\ell \geq 5$.

Thm 4.2 (Gordon - Hugles - Newman).

Let $f(z) = \prod_{\delta|N}\eta(\delta z)^{r_\delta}$.

Suppose also:

$$\left.\begin{array}{l} 1)\ k := \dfrac{1}{2}\displaystyle\sum_{\delta|N} r_\delta \in \mathbb{Z}. \\[2ex] 2)\ \displaystyle\sum_{\delta|N} r_\delta\cdot\delta \equiv 0 \pmod{24} \\[2ex] 3)\ N\cdot\displaystyle\sum_{\delta|N}\frac{r_\delta}{\delta} \equiv 0 \pmod{24} \end{array}\right\} \xRightarrow{\text{Then}} \begin{array}{l} \forall\gamma = \begin{pmatrix}a&b\\c&d\end{pmatrix}\in\Gamma_0(N), \text{ we have:} \\[2ex] f[\gamma]_k = \chi(d)\cdot f \\[2ex] \text{where } \underset{\uparrow}{\chi(d)} = \left(\dfrac{(-1)^k\cdot s}{d}\right), \quad s := \prod \delta^{r_\delta}. \end{array}$$

quadratic dirichlet char. (extends Kronecker)

Rk: if $\gamma\in\Gamma_1(N)$ ($\Rightarrow d\equiv 1 \pmod N$) then $f[\gamma]_k = f$.

Def: Spz χ is a Dirichlet character mod N.

Then $A_k(\Gamma_0(N),\chi) := \{f\in A_k(\Gamma_1(N)) : f[\gamma]_k = \chi(d)\cdot f \ \ \forall \overset{\begin{pmatrix}a&b\\c&d\end{pmatrix}}{\overset{\|}{\gamma}} \in\Gamma_0(N)\}$

$M_k(\Gamma_0(N),\chi) := A_k(\Gamma_0(N),\chi)\cap M_k(\Gamma_1(N))$.

Note: $f\in M_k(\Gamma_0(N),\chi) \Rightarrow f^N\in M_{kN}(\Gamma_0(N))$

$f\in A_k(\Gamma_0(N),\chi)\Rightarrow f^N\in A_{kN}(\Gamma_0(N))$

Example: $\ell \geq 5$ prime, let $\chi(d) := \left(\frac{(-1)^{\frac{\ell-1}{2}}\ell}{d}\right) \overset{Q.R.}{=} \left(\frac{d}{\ell}\right)$

Define $f(z) := \frac{\eta^{\ell}(\ell z)}{\eta(z)}$. Then $\left\{\begin{array}{l} k = \frac{\ell-1}{2} \in \mathbb{Z}. \\ \sum \delta r_\delta = \ell^2 - 1 \equiv 0 \pmod{24}. \\ \sum \frac{r_\delta}{\delta} = \frac{\ell}{\ell} - \frac{1}{1} = 0 \quad \Rightarrow N = \ell \text{ works for the thm.} \end{array}\right.$

Conclude: $f(z) = \frac{\eta^{\ell}(\ell z)}{\eta(z)} \in A_{\frac{\ell-1}{2}}\left(\Gamma_0(\ell), \left(\frac{\cdot}{\ell}\right)\right)$.

Check: $\frac{\eta^{\ell}(z)}{\eta(\ell z)} \in A_{\frac{\ell-1}{2}}\left(\Gamma_0(\ell), \left(\frac{\cdot}{\ell}\right)\right)$, also.

Cusp conditions:

If $f(z) = \prod_{\delta | N} \eta(\delta z)^{r_\delta}$, then $f^{24}(z) = \prod \Delta(\delta z)^{r_\delta}$

If we know how to compute $\Delta(\delta z)\left[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right]_{12}$ $\forall \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, then we'll be able to check the vanishing of $f(z)$ at cusps.

Note: if $\gamma \in GL_2^+(\mathbb{Q})$, then $\frac{d(\gamma\tau)}{d\tau} = (\det \gamma) \cdot (cz + d)^{-2}$

Def: For $\gamma \in GL_2^+(\mathbb{Q})$, $f[\gamma]_k := \left(\frac{d(\gamma\tau)}{d\tau}\right)^{k/2} f(\gamma\tau) = (\det\gamma)^{k/2}(cz + d)^{-k} f(\gamma\tau)$

By the chain rule: $f[\gamma_1\gamma_2]_k = (f[\gamma_1]_k)[\gamma_2]_k$

Observe that, using this definition, $\Delta(\delta z) = \delta^{-6}\Delta\left[\left(\begin{smallmatrix} \delta & 0 \\ 0 & 1 \end{smallmatrix}\right)\right]_{12}(z)$.

Hence $\Delta(\delta z)\left[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right]_{12} = \delta^{-6}\Delta\left[\left(\begin{smallmatrix} \delta & 0 \\ 0 & 1 \end{smallmatrix}\right)\right]_{12}\left[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right]_{12}$

Can check: $\exists B \in \mathbb{Z}, \gamma \in SL_2(\mathbb{Z})$ s.t. $\begin{pmatrix} \delta & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \gamma \cdot \begin{pmatrix} \overset{\substack{\text{gcd} \\ \downarrow}}{(\delta, c)} & B \\ 0 & \frac{\delta}{(\delta,c)} \end{pmatrix}$

With that, $\Delta(\delta z)\left[\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\right] = \delta^{-6}\Delta[\gamma]\left[\begin{pmatrix} (\delta,c) & B \\ 0 & \frac{\delta}{(\delta,c)} \end{pmatrix}\right] = \delta^{-6}\Delta\left[\begin{pmatrix} (\delta,c) & B \\ 0 & \frac{\delta}{(\delta,c)} \end{pmatrix}\right]$

As we are only looking for the order of vanishing, we get $(\text{constant}) \cdot q^{\frac{(\delta,c)^2}{\delta}} + (\text{higher order terms})$

$\left(\text{get actually} \quad \delta^{-6} e^{2\pi i \left(\frac{(\delta,c)z + \beta}{\frac{\delta}{(\delta,c)}} \right)} = (ct) \cdot e^{2\pi i \frac{(\delta,c)^2}{\delta} \cdot z} \right)$.

Conclusion: $f(\tau) \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]_k = (\text{constant}) \cdot q^{w} + \dots$

(Thm 4.3) where $$\boxed{w = \frac{1}{24} \cdot \sum_{\delta \mid N} \frac{(\delta,c)^2 \cdot r_\delta}{\delta}}$$

Remark: 1) w only depends on (c,N), not on the matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ itself.

Hence, it's enough to check it for $c \mid N$.

2) f holomorphic at cusps $\Leftrightarrow \sum \frac{(\delta,c)^2}{\delta} r_d \geq 0 \quad \forall c \mid N$.

vanishes at cusps $\Leftrightarrow \sum \frac{(\delta,c)^2}{\delta} r_d > 0 \quad \forall c \mid N$.

Example:

$\ell \geq 5$ prime. $f(z) = \frac{\eta^\ell(\ell z)}{\eta(\ell z)}$; $g(z) = \frac{\eta^\ell(z)}{\eta(\ell z)}$ $\quad f, g \in A_{\frac{\ell-1}{2}}\left(\Gamma_0(\ell), \left(\frac{\cdot}{\ell}\right)\right)$. ↙checked last day.

Cusp conditions for f:

- $\underline{c=1}$: $c=1 \sim \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ forces ∞ to 1. $\Rightarrow$ cusp $s=1 \equiv$ cusp $s=0$.
- $\underline{c=\ell}$ $c=\ell \sim \begin{pmatrix} 1 & 0 \\ \ell & 1 \end{pmatrix}$ corresponds to $s = \frac{1}{\ell} \equiv$ cusp $s = \infty$.

(recall that $\Gamma_0(\ell)$ has two cusps, represented by 0 and ∞).

~~For f and~~ For $c=\ell \rightarrow$ get $w = \frac{1}{24}\left(\frac{(\ell,\ell)^2}{\ell} \cdot \ell - \frac{1}{1} \cdot 1 \right) = \frac{\ell^2-1}{24}$

For $c=1 \rightarrow$ get $w = \frac{1}{24}\left(\frac{1^2}{\ell} \cdot \ell - \frac{1}{1} \cdot 1 \right) = 0$

Note: Total number of zeros is $\frac{k}{12}[SL_2(\mathbb{Z}) : \Gamma_0(\ell)] = \frac{\ell-1}{24} \cdot (\ell+1) = \frac{\ell^2-1}{24}$, so ✓!!

Cusp for g: at ∞: $w=0$; at 0: $w = \frac{\ell^2-1}{24\ell}$ (recall here that the local coord. is $q^{\frac{1}{\ell}}$).

Note: $\dfrac{\eta^\ell(z)}{\eta(\ell z)} = \dfrac{\prod(1-q^n)^\ell}{\prod(1-q^{\ell n})} \equiv 1 \mod \ell$
$\uparrow$ as $(1-q^n)^\ell \equiv 1-q^{\ell n} \mod \ell$

Note: $p(n)$:= # partitions of n. (eg $4 = 3+1 = 2+2 = 2+1+1 = 1+1+1+1$). So $p(4)=5$.

Euler: $\prod \dfrac{1}{1-q^n} = \sum p(n) q^n$

So if we set $\delta_\ell := \dfrac{\ell^2-1}{24} \in \mathbb{Z}$, then $f(z) = q^{\delta_\ell} \dfrac{\prod(1-q^{\ell n})^\ell}{\prod(1-q^n)} = \cancel{\prod(1-q^{\ell n})^\ell \sum p(n)}$

$= \prod(1-q^{\ell n})^\ell \cdot \sum p(n)\, q^{n+\delta_\ell}$
$\leftarrow$ interesting for additive #theorists.

Modular forms with character (§4.3, §5.2)

Dirichlet character mod N is a gp hom. $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$.

Extend it to $\mathbb{Z}/N\mathbb{Z}$ and to $\mathbb{Z}$ via $\chi(d) := 0$ if $(d,N) \neq 1$.

χ is totally multiplicative.

We have a map $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$, with kernel $= \Gamma_1(N)$.
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \bmod N$

Hence $\Gamma_0(N)/\Gamma_1(N) \simeq (\mathbb{Z}/N\mathbb{Z})^\times$. via $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\Gamma_1(N) \mapsto \bar{d}$.

Define thus $\langle d \rangle : M_k(\Gamma_1(N)) \longrightarrow M_k(\Gamma_1(N))$
$f \longmapsto f\left[\begin{smallmatrix} a & b \\ c & \delta \end{smallmatrix}\right]_k$ where $\begin{pmatrix} a & b \\ c & \delta \end{pmatrix} \in \Gamma_0(N)$, $\delta \equiv d \pmod N$.

Which is well defined because $\dfrac{\Gamma_0(N)}{\Gamma_1(N)} \simeq (\mathbb{Z}/N\mathbb{Z})^\times$.

Note:
1) $\langle d \rangle \in Gl(M_k(\Gamma_1(N)))$ (linear invertible maps).
2) $\langle d \rangle f = \chi(d) \cdot f \iff f \in M_k(\Gamma_0(N), \chi)$.

25

<u>Theorem 5.1</u>: $M_K(\Gamma_1(N)) = \bigoplus_{\chi \bmod N} M_K(\Gamma_0(N), \chi)$ (and the same for S_k).

<u>Pf 1</u>: Prove it directly, using orthogonality of characters. (Koblitz, or exercise in book).

<u>Pf 2</u>: Use basic representation theory..

Have a rep'n of $\rho : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathrm{Gl}(M_K(\Gamma_1(N))) \overset{\text{choose a basis}}{\underset{d}{\simeq}} Gl_n(\mathbb{C})$ (some $\underset{\dim M_k(\Gamma_1(N))}{\overset{\shortparallel}{n}}$)

$$d \longmapsto \langle d \rangle$$

<u>Fact</u>: $(\mathbb{Z}/N\mathbb{Z})^\times$ abelian $\Rightarrow$ ρ decomposes as a sum of irred-representations, which are 1-dimensional, i.e. can pick a basis so that the corresponding matrix is diagonal $= \begin{pmatrix} \chi_1(d) & & 0 \\ & \ddots & \\ 0 & & \chi_n(d) \end{pmatrix} \text{"="} \langle d \rangle$.

Then $\langle d \rangle$ acts as $\chi_i(d)$ on the i^{th} component.

Just collect the χ's. to form $M_K(\Gamma_0(N), \chi)$, //

<u>Goal</u>: Find a canonical basis for $M_K(\Gamma_1(N))$.

If Γ is any congruence subgroup,

<u>Def</u>: The <u>Eisenstein space</u> is $E_K(\Gamma) := M_K(\Gamma) / S_k(\Gamma)$.

$(\dim E_K = \dim M_K - \dim S_K \underset{\substack{\uparrow \\ \text{use dimension} \\ \text{formulas}}}{=} \#$ of <u>regular</u> <u>cusps</u> of Γ).

<u>Note</u>: Every holomorphic form vanishes at <u>irregular</u> cusps.

<u>Idea</u>: There will be 1 Eisenstein series for each of the regular cusps s of Γ, say E^s which vanishes at all other cusps $s' \neq s$, and doesn't vanish at s.

<u>Prototype</u>. $SL_2(\mathbb{Z})$. Recall that $G_K(\tau) = \sum'_{(c,d)\in\mathbb{Z}^2} \frac{1}{(c\tau+d)^k} = \sum_{n=1}^{\infty} \sum_{(c,d)=n} \frac{1}{(c\tau+d)^k} = \zeta(k) \sum_{(c,d)=1} \frac{1}{(c\tau+d)^k}$

Also, $E_K(\tau) = \frac{1}{2\zeta(k)} G_k(\tau) = \frac{1}{2} \sum_{(c,d)=1} \frac{1}{(c\tau+d)^k}$

We want an intrinsic definition of it:

View (c,d) as the bottom row of a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

Note: γ, γ_1 have the same bottom row $\Leftrightarrow \gamma\gamma_1^{-1} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, some $n \in \mathbb{Z}$.

$\Leftrightarrow P^+\gamma = P^+\gamma_1$ where $P^+ = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z} \right\}$

Recalling that $j(\gamma,\tau) = c\tau + d$, one get:

$$E_k(\tau) = \frac{1}{2} \sum_{\gamma \in P^+ \backslash SL_2(\mathbb{Z})} j(\gamma,\tau)^{-k}$$

As $j(\gamma\gamma_1, \tau) = j(\gamma, \gamma_1\tau) \cdot j(\gamma_1, \tau)$ (Chap. I), then:

With this setting, the transformation law is "obvious":

$\gamma\gamma_1$ runs over all cosets of P^+ as γ does.

$$E_k[\gamma_1]_k(\tau) = \frac{1}{2} j(\gamma_1,\tau)^{-k} \sum_{\gamma \in P^+ \backslash SL_2(\mathbb{Z})} j(\gamma, \gamma_1\tau)^{-k} = \frac{1}{2} \sum_{\gamma \in P^+ \backslash SL_2(\mathbb{Z})} j(\gamma\gamma_1, \tau)^{-k} \overset{\downarrow}{=} E_k(\tau)$$

• Generalize to $\Gamma(N)$, first $k \geq 3$.

Notation: Fix $\bar{v} \in (\mathbb{Z}/N\mathbb{Z})^2$ of order N. (i.e. $\bar{v} = (\bar{c}_v, \bar{d}_v)$, $\gcd(c_v, d_v, N) = 1$).

($\bar{\ }$ denotes reduction mod N).

Fix $\delta_v = \begin{pmatrix} a_v & b_v \\ c_v & d_v \end{pmatrix} \in SL_2(\mathbb{Z})$ with $(\bar{c}_v, \bar{d}_v) = \bar{v}$.

$$\varepsilon_N := \begin{cases} \frac{1}{2} & \text{if } N = 1, 2 \\ 1 & \text{otherwise} \end{cases}$$

Def: $E_k^{\bar{v}}(\tau) := \varepsilon_N \sum_{\substack{(c,d) \equiv v \bmod N \\ (c,d) = 1}} (c\tau + d)^{-k}$ ($= E_k$ when $N = 1$).

Intrinsic def: Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then $\gamma \cdot \delta_v^{-1} = \begin{pmatrix} ad_v - bc_v & a_v b - b_v a \\ cd_v - dc_v & a_v d - b_v c \end{pmatrix}$

Claim: $\gamma\delta_v^{-1} \in \Gamma(N) \Leftrightarrow (c,d) \equiv (c_v, d_v) (\equiv v)$ (mod N)

As $\Gamma(N) \triangleleft SL_2(\mathbb{Z})$, $\gamma\delta_v^{-1} \in \Gamma(N) \Leftrightarrow \gamma \in \delta_v \Gamma(N)$.

Also, $\gamma, \gamma_1 \in \Gamma(N)\delta_v$ will have the same bottom row $\Leftrightarrow \gamma\gamma_1^{-1} \in P^+ \cap \Gamma(N)$

So we get the definition:

$$E_k^{\bar v}(\tau) := \varepsilon_N \sum j(\gamma,\tau)^{-k}$$ where the sum runs through $\gamma \in P^+\cap\Gamma(N) \backslash \Gamma(N)\delta_v$

Transformation law: $\gamma_1 \in SL_2(\mathbb{Z})$:

$$E_k^{\bar v}[\gamma_1]_k(\tau) = \varepsilon_N\, j(\gamma_1,\tau)^{-k} \sum j(\gamma,\gamma_1\tau)^{-k} = \varepsilon_N \sum j(\gamma\gamma_1,\tau)^{-k} =$$

Now γ runs through $(P^+\cap\Gamma(N))\backslash\Gamma(N)\delta_v = P^+\cap\Gamma(N)\backslash\delta_v\Gamma(N)$, so the sum is equal to:

$$\varepsilon_N \sum_{\gamma\in(P^+\cap\Gamma(N))\backslash\delta_v\Gamma(N)\gamma_1 = (P^+\cap\Gamma(N))\backslash\Gamma(N)\delta_v\gamma_1} j(\gamma,\tau)^{-k} = E_k^{\overline{v\cdot\gamma_1}}(\tau)$$

~~Then δ_v and $\delta_v\gamma_1$ have the same bottom row,~~ .

As a consequence:

Prop 5.3: $E_k^{\bar v} \in M_k(\Gamma(N))$.

Pf/
- holomorphic (it's a subseries of a series that defines a holomorphic function).
- Transforms under $\Gamma(N)$ by Lemma 5.2.
- We'll compute its Fourier expansion, and we'll find that the coefficients have polynomial growth $\Rightarrow$ holomorphic at the cusps (by Book prop 1.2.4).

//

Define the non-reduced series:

$$G_k^{\bar v}(\tau) := \sum_{(c,d)\equiv\bar v\ (\mathrm{mod}\ N)} (c\tau+d)^{-k}$$

We will compute the Fourier expansion of $G_k^{\bar v}$ and relate them to $E_k^{\bar v}$.

Prop 5.4: Let $\mu(n)$ be the Möbius function.

1) $$G_k^{\bar{v}} = \frac{1}{\varepsilon_N} \sum_{\substack{n \bmod N \\ (n,N)=1}} \left(\left(\sum_{\substack{m \equiv n\,(N) \\ m>0}} \frac{1}{m^k} \right) \cdot E_k^{\overline{n^{-1}v}} \right).$$

2) $$E_k^{\bar{v}} = \varepsilon_N \sum_{\substack{n \bmod N \\ (n,N)=1}} \left(\left(\sum_{\substack{m \equiv n(N) \\ m>0}} \frac{\mu(m)}{m^k} \right) \cdot G_k^{\overline{n^{-1}v}} \right).$$

Pf/ (1): just compute.

(2): we'll do it, to illustrate:

Fact, $$\sum_{m \mid e} \mu(m) = \begin{cases} 1 & e=1 \\ 0 & e>1 \end{cases}$$

$$E_k^{\bar{v}} = \varepsilon_N \cdot \sum_{(c,d)\equiv v} \left(\sum_{m \mid (c,d)} \mu(m) \right) \cdot (c\tau+d)^{-k}$$

Note: $m \mid (c,d) \Rightarrow (m,N)=1$. So

$$E_k^{\bar{v}} \overset{\text{exchange order of sums}}{=} \varepsilon_N \sum_{\substack{m=1 \\ (m,N)=1}}^{\infty} \mu(m) \cdot \left(\sum_{(cm,dm)\equiv v} (cm\tau+dm)^{-k} \right) = \varepsilon_N \sum_{\substack{n \bmod N \\ (n,N)=1}} \sum_{\substack{m \equiv n\,(N) \\ m>0}} \frac{\mu(m)}{m^k} \sum_{(c,d)\equiv m^{-1}v} (c\tau+d)^{-k}$$

//

Computing the Fourier expansion of $G_k^{\bar{v}}$:

Key Fact: $$\sum_{d \in \mathbb{Z}} \frac{1}{(\tau+d)^k} = C_k \cdot \sum_{m=1}^{\infty} m^{k-1} q^m, \quad C_k = \frac{(-2\pi i)^k}{(k-1)!}, \quad \tau \in \mathbb{H}$$

(this is 1.2 in book)

Constant term of expansion: let $\tau \to \infty$. If $\overline{c_v} \neq 0$, then the constant term is 0.

If $\overline{c_v} = \bar{0}$, then get a contribution: $$\sum_{d \equiv d_v (N)} d^{-k}.$$

Write now:

$$G_k^{\bar{v}}(\tau) = \sum_{c \equiv c_v} \sum_{d} \frac{1}{(c\tau + d_v + dN)^k} = \frac{1}{N^k} \sum_{c \equiv c_v} \sum_{d} \frac{1}{\left(\frac{c\tau + d_v}{N} + d\right)^k} =$$

If $c > 0$, then $\frac{c\tau + d_v}{N} \in \mathbb{H}$, so can use the formula, with a contribution:

$$\frac{C_k}{N^k} \sum_{\substack{c \equiv c_v \\ c > 0}} \sum_{m=1}^{\infty} m^{k-1} e^{2\pi i \left(\frac{c\tau + d_v}{N}\right) \cdot m}$$

Let $\zeta_N := e^{2\pi i/N}$. Then $= \frac{C_k}{N^k} \sum_{m=1}^{\infty} m^{k-1} \sum_{\substack{c \equiv c_v \\ c > 0}} \zeta_N^{d_v m} \cdot q_N^{cm}$

Let $n := c \cdot m$. Get $\frac{C_k}{N^k} \sum_{n=1}^{\infty} \left(\sum_{\substack{m \mid n \\ \frac{n}{m} \equiv c_v \\ m > 0}} m^{k-1} \zeta_N^{d_v m} \right) q_N^n$

The case $c < 0$ is similar. We get finally:

Define $\sigma_{k-1}^{\bar{v}}(n) := \sum_{\substack{m \mid n \\ n/m \equiv c_v (N)}} \overset{\text{sign of } m}{\mathrm{sgn}(m)} m^{k-1} \zeta_N^{d_v m}$ and $\zeta^{\bar{d_v}}(k) := \sum_{d \equiv d_v \bmod N} d^{-k}$

$! \to m \in \mathbb{Z}$

Also, $\delta(\bar{c_v}) = \begin{cases} 1 & \text{if } \bar{c_v} \equiv \bar{0} \\ 0 & \text{else.} \end{cases}$

Theorem 5.5:

$$G_k^{\bar{v}}(\tau) = \delta(\bar{c_v}) \zeta^{\bar{d_v}}(k) + \frac{C_k}{N^k} \sum_{n=1}^{\infty} \sigma_{k-1}^{\bar{v}}(n) q_N^n$$

To build Eisenstein series on a congruence sgp $\Gamma \supseteq \Gamma(N)$, we do it as:

$E_{k,\Gamma}^{\bar{v}} := \sum E_k^{\bar{v}}[\gamma_j]_k$ where the sum is over all $\gamma_j \in \Gamma(N) \backslash \Gamma$

One needs to check that it is well-defined (doesn't depend on coset representatives). Also, that it's invariant under $[\gamma]_k$, $\gamma\in\Gamma$, which just permutes the coset representatives.

- How to build series in $M_k(\Gamma_0(N),\chi)$:

Note: if $\gamma=\begin{pmatrix}a_\gamma & b_\gamma\\ c_\gamma & d_\gamma\end{pmatrix}\in\Gamma_0(N)$ and $d\in(\mathbb{Z}/N\mathbb{Z})^\times$, then $\overline{(0,d)\gamma}=\overline{(0,dd_\gamma)}$

So if γ is fixed, dd_γ runs through $(\mathbb{Z}/N\mathbb{Z})^\times$ with d.

Then $$\sum_{d\in(\mathbb{Z}/N\mathbb{Z})^\times} G_k^{\overline{(0,d)}} \in M_k(\Gamma_0(N)).$$

Given a character, then $$\sum_{d\in(\mathbb{Z}/N\mathbb{Z})^\times} \overline{\chi}(d)\, G_k^{\overline{(0,d)}} \in M_k(\Gamma_0(N),\chi):$$

Pf

If $\gamma\in\Gamma_0(N)$, then $$\sum_{d\in(\mathbb{Z}/N\mathbb{Z})^\times} \overline{\chi}(d)\, G_k^{\overline{(0,d)}}[\gamma]_k = \sum_d \overline{\chi}(d)\, G_k^{\overline{(0,dd_\gamma)}} =$$

$$= \chi(d_\gamma)\sum_d \overline{\chi}(dd_\gamma)\, G_k^{\overline{(0,dd_\gamma)}} = \chi(d_\gamma)\cdot\sum_d \overline{\chi}(d)\, G_k^{\overline{(0,d)}} \quad //$$

Notes on Characters

- Trivial character mod N': $\chi_{N'}^{triv}(d) := \begin{cases} 1 & \text{if } (d,N')=1 \\ 0 & \text{if } (d,N')>1 \end{cases}$

- if χ is a char mod N and $N\mid N'$, then $\chi\cdot\chi_{N'}^{triv}$ is a character mod N':

$$\chi\,\chi_{N'}^{triv} = \begin{cases} \chi(d) & \text{if } (d,N')=1 \\ 0 & \text{if } (d,N')\neq 1 \end{cases}$$

Def: if χ is defined mod N', the conductor of χ is the smallest $N\mid N'$ such that $\chi=\chi'\cdot\chi_{N'}^{triv}$, χ' char mod N.

- χ is primitive if its conductor is N'.

Example: χ mod 12:

$1 \to 1$
$5 \to -1$
$7 \to 1$
$11 \to -1$

is not primitive, as χ' mod 3 : $1 \mapsto 1$, $2 \mapsto -1$

and $\chi = \chi' \cdot \chi_{12}^{triv}$.

Def: χ mod N. Define its Gauss sum as: $g(\chi) := \sum_{d=0}^{N-1} \chi(d) \zeta_N^d$

Eisenstein series on $M_k(\Gamma_0(N), \chi)$:

Fix N, k. Take characters ψ mod u, φ mod v, φ primitive, $N = u \cdot v$.

Also assume that $(\psi\varphi)(-1) = (-1)^k$.

Define:
$$G_k^{\psi,\varphi}(\tau) := \sum_{c=0}^{u-1} \sum_{d=0}^{v-1} \sum_{e=0}^{u-1} \psi(c)\, \overline{\varphi}(d)\, G_k^{\overline{(cv,\, d+ev)}}(\tau).$$

One can check that $G^{\psi,\varphi}(\tau) \in M_k(\Gamma_0(N), \psi\cdot\varphi)$ (formal calculation).

Also, one can compute its Fourier expansion:

Let $L(s,\chi) := \sum_{n=1}^{\infty} \chi(n) n^{-s}$ $\quad Re(s) > 1$ (L-series)

$$\sigma_{k-1}^{\psi,\varphi}(n) := \sum_{\substack{m \mid n \\ m > 0}} \psi(n/m)\, \varphi(m)\, m^{k-1}$$

$$\delta(\psi) := \begin{cases} 1 & \text{if } \psi \text{ is the trivial char. mod } 1. \\ 0 & \text{else.} \end{cases}$$

Then:

Theorem 5.6; Let $k \geq 3$. $G_k^{\psi,\varphi}(\tau) = \dfrac{C_k\, g(\overline{\varphi})}{v^k} E_k^{\psi,\varphi}(\tau)$

where $E_k^{\psi,\varphi}(\tau) = \delta(\psi) L(1-k, \varphi) + 2 \sum_{n=1}^{\infty} \sigma_{k-1}^{\psi,\varphi}(n)\, q^n$.

Note: $L(1-k,\varphi)$ is defined via its functional equation. Actually one can compute it via the generalized Bernoulli numbers. (see book, or Ireland-Rosen)

To compute the Bernoulli number, let χ be mod N.

$$\sum_{a=1}^{N-1} \frac{\chi(a)\, t\, e^{at}}{e^{Nt}-1} \overset{\text{Taylor}}{=} \sum_{k=0}^{\infty} B_{k,\chi} \cdot \frac{t^k}{k!}$$

Fact: If $k \geq 1$, $L(1-k,\chi) = \frac{-B_{k,\chi}}{k}$.

Define now $E_k^{\psi,\varphi,d}(\tau) := E_k^{\psi,\varphi}(d\tau)$ for $d \in \mathbb{Z}_{>0}$.

And $A_{N,k} := \{ (\psi,\varphi,d) : \psi$ primitive mod u, φ primitive mod v, $u \cdot v \cdot d = N$, $(\psi\varphi)(-1) = (-1)^k \}$

Theorem 5.7: A basis for $E_k(\Gamma_1(N))$ is $\{ E_k^{\psi,\varphi,d} : (\psi,\varphi,d) \in A_{N,k} \}$.

Moreover, a basis for $E_k(\Gamma_1(N),\chi)$ is $\{ E_k^{\psi,\varphi,d} : (\psi,\varphi,d) \in A_{N,k}$ and $\psi \cdot \varphi = \chi \}$

Example: $M_3(\Gamma_0(7),\chi)$, where $\chi(d) = \left(\frac{d}{7}\right)$ (Legendre symbol).

Let χ_0 = triv. char mod 1. $(\chi_0(d)=1)$

Only two Eisenstein series: ~~$E_3(\chi,\chi_0)$, $E_3(\chi_0,\chi)$~~

~~$E_3($~~ E_3^{χ,χ_0} and $E_3^{\chi_0,\chi}$

Exercise: compute each expansion to order 3, and write each of these in term of

$$\frac{-\eta^7(z)}{\eta(7z)} = 1 - 7q + 14q^2 + \cdots$$

$$\eta^3(7z) \cdot \eta^3(z) = q - 3q^2 + -$$

$$\frac{\eta^7(7z)}{\eta(z)} = q^2 + \cdots$$

↑ hand in

(due Monday 30th)

Hint: $\frac{t}{e^{7t}-1} = \frac{1}{7} - \frac{1}{2}t + \frac{7}{12}t^2 + O(t^4)$

no t^3-term.

Recall: we computed Sturm bound for $M_{\frac{\ell-1}{2}}(\Gamma_0(\ell),\chi)$: $\frac{\ell}{2} \cdot \frac{\ell-1}{2} \cdot [SL_2(\mathbb{Z}):\Gamma_0(\ell)]$
$= \frac{\ell^2-1}{24}$.

Goal: Find a canonical basis for $S_k(\Gamma_1(N))$.

Linear Algebra: V fin. dim. inner-product space over $\mathbb{C}$, $T: V \to V$ linear.

The adjoint T^* is defined by $\langle Tv, w\rangle = \langle v, T^* w\rangle$.

T Hermitian $\Leftrightarrow$ $T = T^*$

Normal $\Leftrightarrow$ $TT^* = T^*T$

Thm 6.1 "Spectral Theorem": if $\{T_i\}_{i \in I}$ is a family of commuting normal operators on a fin. dim. vectorspace V, then V has a basis of simultaneous eigenvectors of all T_i.

So we need to put an inner product on S_k, and find the T_i's.

Hecke Operators

General way ~~to~~ define operators: Double Cosets.

Γ_1, Γ_2 congruence sgps, $\alpha \in GL_2^+(\mathbb{Q})$.

Def: $\Gamma_1 \alpha \Gamma_2 = \{\gamma_1 \cdot \alpha \cdot \gamma_2 : \gamma_i \in \Gamma_i\}$.

Note that $\Gamma_1 \circlearrowright \Gamma_1\alpha\Gamma_2$, $\Gamma_1\alpha\Gamma_2 \circlearrowleft \Gamma_2$. (multiplication).

Can decompose into orbits: $\Gamma_1\alpha\Gamma_2 = \overset{\text{finite?}}{\dot\bigcup} \Gamma_1 \beta_j$ (disjoint union of orbits).

Goal: given $f \in M_k(\Gamma_1)$, define $f[\Gamma_1\alpha\Gamma_2]_k = \sum f[\beta_j]_k$

and will get a modular form in $M_k(\Gamma_2)$! ↖ finite?

Lemma 6.2: a) If Γ is a congruence sgp, $\alpha \in GL_2^+(\mathbb{Q})$, ~~then $\alpha^{-1}\Gamma\alpha$ is a cong. sgp.~~

Then $\alpha^{-1}\Gamma\alpha \cap SL_2(\mathbb{Z})$ is a congruence subgroup.

b) Any two congruence subgroups Γ_1, Γ_2 are commensurable.

(i.e. $[\Gamma_1 : \Gamma_1 \cap \Gamma_2] < \infty$, $[\Gamma_2 : \Gamma_1 \cap \Gamma_2] < \infty$).

Pf (a) book, 5.1.1. (b) $\exists\, d$ s.t. $\Gamma(d) \subseteq \Gamma_1 \cap \Gamma_2$. Then $[\Gamma_1 : \Gamma_1 \cap \Gamma_2] \leq [SL_2(\mathbb{Z}) : \Gamma(d)]$ //

We want to identify: $\underset{\uparrow \text{orbits}}{\Gamma_1\backslash^{\Gamma_1\alpha\Gamma_2}} \longleftrightarrow \underset{\uparrow \text{cosets}}{\Gamma_3\backslash^{\Gamma_2}}$ (what's Γ_3 ?).

Map $\Gamma_2 \longrightarrow \Gamma_1\backslash^{\Gamma_1\alpha\Gamma_2}$ (clearly surjective).

$$\gamma_2 \longmapsto \Gamma_1\alpha\gamma_2 \left(= \Gamma_1\cdot(I\cdot\alpha\cdot\gamma_2)\right).$$

Q: When γ_2, γ_2' get mapped to the same orbit?

$\Gamma_1\alpha\gamma_2 = \Gamma_1\alpha\gamma_2' \iff \gamma_2'\gamma_2^{-1} \in \alpha^{-1}\Gamma_1\alpha \iff \gamma_2, \gamma_2'$ are in the same coset of $(\alpha^{-1}\Gamma_1\alpha)\cap\Gamma_2$

Let $\Gamma_3 := (\alpha^{-1}\Gamma_1\alpha)\cap\Gamma_2$. So we've proved:

Prop 6.3: There's a bijection $\Gamma_3\backslash^{\Gamma_2} \longleftrightarrow \Gamma_1\backslash^{\Gamma_1\alpha\Gamma_2}$.

$$\Gamma_3\gamma_2 \longmapsto \Gamma_1\alpha\gamma_2$$

(i.e if $\Gamma_2 = \bigcup \Gamma_3\gamma_j$ is a coset decomposition of $\Gamma_3\backslash^{\Gamma_2}$, then $\underset{\text{(orbit decomp)}}{\Gamma_1\alpha\Gamma_2 = \bigcup \Gamma_1\alpha\gamma_j}$).

In particular, the number of orbits of $\Gamma_1 \curvearrowright \Gamma_1\alpha\Gamma_2$ is finite.

Suppose $f \in M_k(\Gamma)$. $\Gamma_1\alpha\Gamma_2 = \bigcup \Gamma_1\beta_j$ an orbit decomposition.

Define now $f[\Gamma_1\alpha\Gamma_2]_k := \sum f[\beta_j]_k$

Note: Indep. of choice of β_j, as f is k-inv. under Γ_1!

Note: if $\Gamma_2 = \bigcup(\underbrace{\alpha^{-1}\Gamma_1 a \cap \Gamma_2}_{\Gamma_3})\gamma_j$, then can take $\{\beta_j\} = \{\alpha\cdot\gamma_j\}$ (by 6.3).

So if $\gamma_2 \in \Gamma_2$, then $\{\gamma_j\gamma_2\}$ is a complete set of rep's for $\Gamma_3\backslash^{\Gamma_2}$ (if $\{\gamma_j\}$ was!)

Hence, $\{\alpha\gamma_j\gamma_2\}$ is a set of rep's for $\Gamma_1\backslash^{\Gamma_1\alpha\Gamma_2}$.

This implies that $f[\Gamma_1\alpha\Gamma_2]_k$ ~~$\in M_k(\Gamma_2$~~ is k-invariant for Γ_2.

Proposition 6.4: $[\Gamma_1 \alpha \Gamma_2]_k$ maps $M_k(\Gamma_1)$ to $M_k(\Gamma_2)$ and $S_k(\Gamma_1)$ to $S_k(\Gamma_2)$.

Pf. • Transf. law is done.

• Holom. on $\mathbb{H}$ is done as $f[\beta_j] \in Hol(\mathbb{H})$ for any $\beta_j \in GL_2^+(\mathbb{Q})$.

• Cusp conditions: will be done in Prop 6.5. //

Example:

1) $\Gamma_2 \subset \Gamma_1$, $\alpha = I$. Then $\Gamma_1 \alpha \Gamma_2 = \Gamma_1 \Gamma_2 = \Gamma_1$. Then $\Gamma_1 = \Gamma_1 \cdot I$ is a orbit decomp.

So $f[\Gamma_1 \alpha \Gamma_2]_k = f[I]_k = f$ (so $f \in M_k(\Gamma_1) \Rightarrow f \in M_k(\Gamma_2)$).

2) $\Gamma_2 = \alpha^{-1} \Gamma_1 \alpha$. Then $\Gamma_1 \alpha \Gamma_2 = \Gamma_1 \alpha \alpha^{-1} \Gamma_1 \alpha = \Gamma_1 \alpha$ ← only one ~~coset~~ orbit.

So $f[\Gamma_1 \alpha \Gamma_2]_k = f[\alpha]_k$. So $f \in M_k(\Gamma_1) \Rightarrow f[\alpha]_k \in M_k(\alpha^{-1}\Gamma_1 \alpha)$.

Prop 6.5: Spz $\forall \gamma \in SL_2(\mathbb{Z})$, $f[\gamma]_k$ has the form $\sum_{n \geq n_0} a(n) q_N^n$.

Then if $\alpha \in GL_2^+(\mathbb{Q})$, $\forall \gamma \in SL_2(\mathbb{Z})$ have $(f[\alpha]_k)[\gamma]_k = \sum_{n \geq a \cdot n_0} b(n) q_{Nd}^n$

where a, d depend on α ($\overset{\neq 0}{a}, \overset{\neq 0}{d} \in \mathbb{N}$).

(So cusp forms are preserved). (i.e. preserves the statements: "f hol. at cusps" "f vanishes at cusps").

Pf (Sketch):

if $a > 0$, compute $f\left[\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right]_k = a^{2(k-1)} \cdot a^{-k} \cdot f$.

So WLOG we can assume that α has integer entries.

Find $\gamma_0 \in SL_2(\mathbb{Z})$ st $\gamma_0^{-1} \cdot \alpha$ is upper-triangular, $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$, $\overset{\neq 0}{a}, \overset{\neq 0}{d} \in \mathbb{N}$ (exercise in body).

Then $f[\alpha]_k = (f[\gamma_0]_k) \cdot \left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]_k = \left(\sum_{n \geq n_0} a(n) e^{2\pi i n \frac{z}{N}} \right) \left[\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right]_k =$

$$= (*) \cdot \sum_{n \geq n_0} a(n) e^{\frac{2\pi i n (az+b)}{dN}} = (*) \, q_{Nd}^{a n_0} + \cdots$$

//

Let p be a prime.

Def: $T_p : M_k(\Gamma_1(N)) \longrightarrow M_k(\Gamma_1(N))$ is defined by $T_p f := f\left[\Gamma_1(N)\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma_1(N)\right]_k$ is (the) Hecke operator at p.

Note: If $\gamma \in \Gamma_1(N)\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma_1(N)$ then:

1) $\det \gamma = p$

2) $\gamma \equiv \begin{pmatrix}1&*\\0&p\end{pmatrix} \bmod N$.

(see chap III in book)

Fact: $\Gamma_1(N)\begin{pmatrix}1&0\\0&p\end{pmatrix}\Gamma_1(N) = \left\{\gamma \in M_2(\mathbb{Z}) \text{ s.t } \det\gamma = p,\ \gamma \equiv \begin{pmatrix}1&*\\0&p\end{pmatrix} \bmod N\right\}$

We want an explicit description of $\Gamma_3 \backslash \Gamma_1(N)$ where $\Gamma_3 = \begin{pmatrix}1&0\\0&p\end{pmatrix}^{-1}\Gamma_1(N)\begin{pmatrix}1&0\\0&p\end{pmatrix} \cap \Gamma_1(N)$

Note: if $\begin{pmatrix}a&b\\c&d\end{pmatrix} \in \Gamma_1(N)$, then $\begin{pmatrix}1&0\\0&p\end{pmatrix}^{-1}\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&0\\0&p\end{pmatrix} = \begin{pmatrix}a&bp\\c/p&d\end{pmatrix}$ is in $\Gamma_1(N)$

iff $\frac{c}{p} \equiv 0 \pmod N \Leftrightarrow \begin{pmatrix}a&bp\\c/p&d\end{pmatrix} \in \Gamma_1(N) \cap \Gamma^0(p)$

where $\Gamma^0(p) = \left\{\begin{pmatrix}*&0\\ *&*\end{pmatrix} \bmod p\right\}$.

Conclusion: $\Gamma_3 = \Gamma_1(N) \cap \Gamma^0(p)$.

We are thus looking for $(\Gamma_1(N)\cap\Gamma^0(p))\backslash\Gamma_1(N)$: ~~try~~ $\gamma_j := \begin{pmatrix}1&j\\0&1\end{pmatrix}$, ~~$j\in\mathbb{Z}$~~ $0 \leq j \leq p-1$.

These are all distinct mod $\Gamma_1(N)\cap\Gamma^0(p)$. Is this a complete set?

Take $\begin{pmatrix}a&b\\c&d\end{pmatrix} \in \Gamma_1(N)$, then $\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1&-j\\0&1\end{pmatrix} = \begin{pmatrix}a&-aj+b\\c&-cj+d\end{pmatrix}$

So if $p \nmid a$, then can make RHS $\in \Gamma^0(p)$ for some j.

Note: if $p \mid N$, then $p \nmid a$ for any $\begin{pmatrix}a&b\\c&d\end{pmatrix} \in \Gamma_1(N)$, so we've got a complete set of reps.

If $p \nmid N$, just need to look at $\begin{pmatrix}a&b\\c&d\end{pmatrix}$, $p \mid a$. Choose $\gamma_\infty = \begin{pmatrix}mp&n\\N&1\end{pmatrix} \in \Gamma_1(N)$. Then,

$\begin{pmatrix}a&b\\c&d\end{pmatrix}\gamma_\infty^{-1} = \begin{pmatrix}*&-na+bmp\\ *&*\end{pmatrix}$. As $p \mid -na+bmp$, then $\begin{pmatrix}a&b\\c&d\end{pmatrix} \equiv \gamma_\infty \bmod \Gamma^0(p)$

Hence $\{\gamma_j\} \cup \{\gamma_\infty\}$ is a complete set of reps.

To get the orbit reps, just multiply by the fixed elt. $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$,

and get: $\left\{ \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} : 0 \leq j \leq p-1 \right\} \underset{\overset{\uparrow}{\text{if } p \nmid N}}{\cup} \left\{ \begin{pmatrix} mp & n \\ Np & p \end{pmatrix} = \begin{pmatrix} m & n \\ N & p \end{pmatrix} \cdot \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right\}$.

<u>Prop 6.6</u>: If $f \in M_k(\Gamma_1(N))$, then:

$$T_p f = \begin{cases} \sum_{j=0}^{p-1} f\left[\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right]_k & \text{if } p \mid N \\ \sum_{j=0}^{p-1} f\left[\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right]_k + f\left[\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right]_k \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]_k & \text{if } p \nmid N. \end{cases}$$

Pf/ Just done! //

Let now $f = \sum a_n q^n$, and define $U_p f := \sum a_{np} q^n \overset{\substack{\text{abuse of notation} \\ \downarrow}}{=} \sum a_n q^{n/p}$. $q^{\frac{n}{p}} = 0$ if $p \nmid n$

<u>Lemma 6.7</u>: if $f = \sum a_n q^n$, then $U_p f = \frac{1}{p} \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) = \sum_{j=0}^{p-1} f\left[\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right]_k$

Pf/ Use the fact that $\sum_{j=0}^{p-1} \zeta_p^{nj} = \begin{cases} p & \text{if } p \mid n \\ 0 & \text{if } p \nmid n \end{cases}$

Now compute: $\sum_{j=0}^{p-1} f\left[\begin{smallmatrix} 1 & j \\ 0 & p \end{smallmatrix}\right]_k = p^{k-1} p^{-k} \sum_j f\left(\frac{z+j}{p}\right)$

As ~~f~~ is periodic, this is $\frac{1}{p} \sum_j \sum_n a_n e^{2\pi i n\left(\frac{z+j}{p}\right)} = \sum_n a_n e^{\frac{2\pi i n z}{p}} \cdot \frac{1}{p} \sum_j \zeta_p^{nj}$ //

<u>Rk 6.8</u>: if $p \mid N$ then U_p maps $M_k(\Gamma_1(N))$ to itself.
if $p \nmid N$ then U_p maps $M_k(\Gamma_1(N))$ to $M_k(\Gamma_1(Np))$.

<u>Def</u>: $V_p(f(z)) = f(pz)$.

<u>Notes</u>:
1) $f\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]_k = p^{k-1} V_p(f)$

2) $f\left[\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right]_k = \langle p \rangle f$

<u>Cor 6.9</u>: $T_p f = \begin{cases} U_p f & \text{if } p \mid N \\ U_p f + p^{k-1} V_p(\langle p \rangle f) & \text{if } p \nmid N. \end{cases}$

Cor 6.10: If $f \in M_k(\Gamma_0(N), \chi)$, then $T_p f = U_p f + \chi(p) p^{k-1} (V_p f)$ $\forall p$.

Rk: can see $M_k(\Gamma_0(N)) = M_k(\Gamma_0(N), \chi_N^{\text{triv}})$.

"everything commutes":

Thm 6.11: Let p, q primes, $e, d \in (\mathbb{Z}/N\mathbb{Z})^\times$. Then:

a) $\langle d \rangle T_p = T_p \langle d \rangle$

b) $\langle d \rangle \langle e \rangle = \langle e \rangle \langle d \rangle$

c) $T_p T_q = T_q T_p$

Pf Assume (a) and prove (b) and (c).

(a) $\Rightarrow$ that T_p preserves each $M_k(\Gamma_0(N), \chi)$:

if $f \in M_k(\Gamma_0(N), \chi)$, then $\langle d \rangle (T_p f) = T_p(\langle d \rangle f) = T_p(\chi(d) \cdot f) = \chi(d) T_p f$

So one can check (b), (c) for $f \in M_k(\Gamma_0(N), \chi)$

(as $M_k(\Gamma_1(N)) = \bigoplus M_k(\Gamma_0(N), \chi)$).

Then (b) is obvious: $\langle d \rangle \langle e \rangle f = \chi(d)\chi(e) f = \chi(e)\chi(d) f = \langle e \rangle \langle d \rangle f$.

Also, if $f = \sum a_n q^n \in M_k(\Gamma_0(N), \chi)$, then:

$$T_p f = \sum \left(a_{pn}(f) + \chi(p) p^{k-1} a_{n/p}(f) \right) q^n \qquad (a_{n/p} = 0 \text{ if } p \nmid n).$$

So
$$a_n(T_p(T_q f)) = a_{pn}(T_q f) + \chi(p) p^{k-1} a_{n/p}(T_q f) =$$
$$= a_{pqn}(f) + \chi(q) q^{k-1} a_{pn/q}(f) + \chi(p) p^{k-1} \left(a_{nq/p}(f) + \chi(q) q^{k-1} a_{n/pq}(f) \right)$$

and this is symmetric in p and q, so ✓.

For (a), write $\langle d \rangle$ as a double coset: take $\gamma \equiv \begin{pmatrix} * & * \\ 0 & d \end{pmatrix}$ mod N

$(\gamma \in \Gamma_0(N))$. Then $\Gamma_1(N) \gamma \Gamma_1(N) \overset{\Gamma_1 \trianglelefteq \Gamma_0}{=} \Gamma_1(N) \cdot \gamma$. So $\langle d \rangle f = f[\gamma]_k = f[\Gamma_1(N) \gamma \Gamma_1(N)]_k$

(cont pf). Put $\Gamma_1 = \Gamma_1(N)$, and want that $\langle d\rangle^{-1} T_p \langle d\rangle = T_p$

Write now $\Gamma_1 \alpha \Gamma_1 = \dot{\bigcup_j} \Gamma_1 \beta_j$ (orbits)

Need to show that $\Gamma_1 \alpha \Gamma_1 = \dot{\bigcup_j} \Gamma_1 (\gamma \beta_j \gamma^{-1})$ (orbits)

(and so $T_p f = \sum f[\beta_j] = \sum f[\gamma\beta_j\gamma^{-1}] = \sum f[\gamma][\beta_j][\gamma] = \langle d\rangle^{-1} T_p \langle d\rangle f$).

Note then that $\bigcup_j \Gamma_1(\gamma\beta_j\gamma^{-1}) = \gamma\left(\bigcup_j \Gamma_1\beta_j\right)\gamma^{-1} = \gamma(\Gamma_1\alpha\Gamma_1)\gamma^{-1} = \Gamma_1(\gamma\alpha\gamma^{-1})\Gamma_1$

Check (exercise) that $\Gamma_1 \alpha \Gamma_1 = \Gamma_1(\gamma\alpha\gamma^{-1})\Gamma_1$.

<u>Example</u>: $E_k(z) = 1 - \frac{2k}{B_k}\sum_{n\geq 1}^{\infty} \sigma_{k-1}(n) q^n \in M_k(\Gamma_1(1))$; $k \geq 4$, $\sigma_{k-1}(n) = \sum_{d|n} d^{k-1}$

Then the Fourier exp of $T_p E_k$ is:

(as $a_n(T_p f) = a_{np}(f) + \chi(p) p^{k-1} a_{n/p}(f)$).

$a_0(T_p E_k) = a_0(E_k) + p^{k-1} a_0(E_k) = 1 + p^{k-1} = \sigma_{k-1}(p)$

if $n \geq 1$,

$$a_n(T_p E_k) = -\frac{2k}{B_k}\left(\sigma_{k-1}(np) + p^{k-1}\underbrace{\sigma_{k-1}\left(\tfrac{n}{p}\right)}_{\overset{\shortparallel}{0 \text{ if } p\nmid n}}\right)$$

<u>Fact</u>: $\sigma_{k-1}(np) + p^{k-1}\sigma_{k-1}\left(\frac{n}{p}\right) = \sigma_{k-1}(p)\sigma_{k-1}(n) \quad \forall n \geq 1.$

Pf if $p \nmid n$, as σ_{k-1} is multiplicative it is obvious.

if $p | n$, write $n = p^e \cdot n'$, $p \nmid n'$, ...

So $a_n(T_p E_k) = \frac{-2k}{B_k}\sigma_{k-1}(p)\sigma_{k-1}(n) = \sigma_{k-1}(p) a_n(E_k)$.

<u>Hence</u>: $T_p E_k = \sigma_{k-1}(p) \cdot E_k$.

We say that E_k is an <u>eigenform</u> of <u>all</u> T_p, with eigenvalue $\overset{1+p^{k-1}}{\overset{\shortparallel}{\sigma_{k-1}(p)}}$.

<u>Note</u>: if $f = 1 + \sum_{n\geq 1} a_n q^n \in M_k(SL_2(\mathbb{Z}))$ is an Eigenform of T_p, then the Eigenvalue <u>is</u> $\sigma_{k-1}(p)$.

By a similar argument, one can compute that if $(\psi, \varphi, t) \in A_{N,k}$, then

$E_k^{\psi,\varphi,t} \in M_k(\Gamma_0(N), \psi\varphi)$ is an eigenform of T_p for $p \nmid N$,

with eigenvalue $\psi(p) + \varphi(p)p^{k-1}$. (exercise in book)

- Application:

$p(n)$:= partition function.

Then $\sum_{n=0}^{\infty} p(n) q^n = \prod_{n=1}^{\infty} \frac{1}{1-q^n}$.

As $\Delta(z) = q \cdot \prod (1-q^n)^{24} = \frac{q \prod (1-q^n)^{25}}{1-q^n} = \prod(1-q^n)^{25} \cdot \sum_{n=0}^{\infty} p(n) q^{n+1}$

Thm (Ramanujan): $p(5n+4) \equiv 0 \bmod 5 \ \forall n$.

Pf work mod 5: $\Delta(z) \equiv \prod (1-q^{25n}) \sum p(n-1) q^n \pmod 5$.

Facts:

1) $\Delta | T_5 \ (= T_5(\Delta)) = \Delta | (U_5 + 5^{11} V_5) \equiv \Delta | U_5 \pmod 5$.

2) $\left(\left(\sum a_n q^{pn}\right)\left(\sum b_n q^n\right)\right) | U_p = \left(\sum a_n q^n\right)\left(\sum b_n q^{n/p}\right) = \left(\sum a_n q^n\right) \cdot \left(\left(\sum b_n q^n\right) | U_p\right)$

Combining this, $\Delta | T_5 \equiv \Delta | U_5 \equiv \prod (1-q^{5n}) \cdot \left(\sum p(n-1) q^n\right) | U_5 =$

$\equiv \prod (1-q^{5n}) \sum p(5n-1) q^n \pmod 5$.

So $p(5n+4) \equiv 0 \bmod 5$ ~~ta~~ $\forall n \iff \Delta | T_5 \equiv 0 \pmod 5$.

$\Delta \in S_{12}(\Gamma_0(1)) \leftarrow$ 1-dim'l space.

$\Delta = q + \dots = \sum_{n=1}^{\infty} a_n q^n$.

So $\Delta | T_5 = \sum (a_{5n} + 5^{11} a_{n/5}) q^n = a_5 \cdot q + \dots$

So $\Delta | T_5 = a_5 \cdot \Delta$. But $a_5 \equiv p(4) \pmod 5 \equiv 0 \pmod 5$. Or also $a_5 = \overset{\substack{\equiv 0 \bmod 5\,! \\ \downarrow}}{4830}$

Exercise: Prove that $p(7n+5) \equiv 0 \mod 7$, $p(11n+6) \equiv 0 \mod 11$.

$\Delta(z)$: Ramanujan's observations:

$$\Delta(n) = \sum_{n=1}^{\infty} a_n q^n \quad , \quad (a_n = \tau(n))$$

$$\left.\begin{array}{l} 1)\ a_{nm} = a_n a_m \text{ if } (n,m)=1. \\ 2)\ a_{p^r} = a_p \cdot a_{p^{r-1}} - p^{11} \cdot a_{p^{r-2}} \text{ if } r \geq 2. \end{array}\right\} \text{Hecke Theory}$$

3) $|a_p| \leq 2 \cdot p^{11/2}$ $\forall p$. ← Ramanujan's conjecture.

Ramanujan's Conjecture was proven by Deligne in 1971: | prove a_p is ~ Frobenius action on some alg. variety

| Prove Weil conjectures.

(1) Says that $\displaystyle\sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p \sum_{r=0}^{\infty} \frac{a_{p^r}}{p^{rs}}$

(2) Says that $\displaystyle\sum_{r=0}^{\infty} \frac{a_{p^r}}{p^{rs}} \left(1 - a_p p^{-s} + p^{11-2s}\right) = 1$

So get an L-series $\displaystyle L(\Delta, s) = \sum a_n n^{-s} \overset{\text{equivalent to (1)\&(2).}}{=} \prod_p \frac{1}{1 - a_p p^{-s} + p^{11-2s}}$

- Definition of T_n on $M_k(\Gamma_1(N))$ $\forall n$.

Def: $\displaystyle\sum_{n=1}^{\infty} T_n n^{-s} = \prod_p \frac{1}{1 - T_p p^{-s} + \langle p \rangle p^{k-1-2s}}$ where $\langle p \rangle = 0$ if $p \mid N$

This def. is equivalent to:

1) $T_{nm} = T_n \cdot T_m$ if $(n,m)=1$.

2) $T_{p^r} = T_p \cdot T_{p^{r-1}} - p^{k-1} \langle p \rangle T_{p^{r-2}}$ if $r \geq 2$

Note: Each T_n is a polynomial in the T_p, and all T_n's commute.

- How T_n acts on a Fourier expansion:

write $f = \sum_{m=0}^{\infty} a_m(f)\, q^m \in M_k(\Gamma_1(N))$.

Then $T_n(f) = \sum a_m(T_n f)\, q^m$.

Prop 6.12: $$a_m(T_n f) = \sum_{d|(m,n)} d^{k-1} a_{\frac{mn}{d^2}}(\langle d\rangle f).$$

If $f \in M_k(\Gamma_0(N), \chi)$, then
$$a_m(T_n f) = \sum_{d|(m,n)} \chi(d)\, d^{k-1} a_{\frac{mn}{d^2}}(f).$$

Pf/ Computation //

Petersson inner product on $S_k(\Gamma)$.

Short version: hyperbolic measure $d\mu(\tau) = \frac{dx\,dy}{y^2}$.

$f, g \in S_k(\Gamma)$, then $$\langle f, g\rangle_\Gamma := \frac{1}{\mathrm{vol}(\Gamma)} \int_{X(\Gamma)} f(\tau)\, \overline{g(\tau)}\, \mathrm{Im}(\tau)^k\, d\mu(\tau)$$

If it's well defined, then:

- $\langle f+h, g\rangle = \langle f, g\rangle + \langle h, g\rangle$
- $\langle g, f\rangle = \overline{\langle f, g\rangle}$
- $\langle cf, g\rangle = c\langle f, g\rangle$
- $\langle f, f\rangle > 0$ if $f \neq 0$.

- Surface integrals:

$V \subseteq \mathbb{C}$, a 2-form on V is $f(z,\bar{z})\, dz \wedge d\bar{z}$

$$dz \wedge d\bar{z} = (dx + i\,dy) \wedge (dx - i\,dy) = -2i\, dx \wedge dy$$

Then $$\int_V f(z,\bar{z})\, dz \wedge d\bar{z} = \iint -2i\big(f(x+iy, x-iy)\big)\, \overbrace{dx \wedge dy}^{\text{write it } dxdy}$$

Let now $\alpha \in GL_2^+(\mathbb{R})$, and consider the change $z \mapsto \alpha z$.

Then $\mathrm{Im}(\alpha z) = \dfrac{\det \alpha}{|cz+d|^2}\, \mathrm{Im}(z)$.

Also, $d(\alpha z) = \dfrac{\det(\alpha)}{(cz+d)^2}\, dz$, and $\overline{d(\alpha z)} = \dfrac{\det(\alpha)}{(\overline{cz+d})^2}\, d\bar{z}$.

So $dz \wedge d\bar{z} \longrightarrow \dfrac{(\det \alpha)^2}{|cz+d|^4}\, dz \wedge d\bar{z} = \left(\dfrac{\mathrm{Im}(\alpha z)}{\mathrm{Im}(z)}\right)^2 dz \wedge d\bar{z}$

So $\dfrac{dz \wedge d\bar{z}}{\mathrm{Im}\, z}$ is invariant under $z \mapsto \alpha z$.

Define: $$d\mu(z) := \frac{dx \wedge dy}{y^2} = -\frac{1}{2i}\, \frac{dz \wedge d\bar{z}}{(\mathrm{Im}\, z)^2}$$

Let D^* be a fundamental domain for $SL_2(\mathbb{Z})$.

We can define the volume of $SL_2(\mathbb{Z})$:

$$\mathrm{Vol}(SL_2(\mathbb{Z})) := \int_{D^*} d\mu(z) \overset{\text{exercise}}{=} \frac{\pi}{3}$$

This implies that, if φ is bounded, $\int_{D^*} \varphi(z)\, d\mu(z)$ converges.

Integral over $X(\Gamma)$:

Let D be a fund. domain for Γ, $D = \bigcup_j \alpha_j D^*$ (disjoint if ignoring boundary)

(the α_j are coset rep's for $\pm I \cdot \Gamma \backslash SL_2(\mathbb{Z})$).

Now if $\varphi(\tau)$ is Γ-invariant, then:

$$\int_{X(\Gamma)} \varphi(\tau)\,d\mu(\tau) := \int_{\bigcup_j \alpha_j D^*} \varphi(\tau)\,d\mu(\tau) = \sum_j \int_{\alpha_j D^*} \varphi(\tau)\,d\mu(\tau) = \sum_j \int_{D^*} \varphi(\alpha_j \tau)\,d\mu(\tau)$$

From the last equality, we see that the definition does not depend on the choice of coset reps.

Also,

$$\mathrm{Vol}(\Gamma) := \int_{X(\Gamma)} 1 \cdot d\mu(\tau) = [SL_2(\mathbb{Z}) : \pm I\Gamma] \cdot \mathrm{vol}(SL_2(\mathbb{Z})) = \frac{\pi}{3}[SL_2(\mathbb{Z}) : \pm I\Gamma].$$

Let $f, g \in S_k(\Gamma)$. Set $\varphi(\tau) := f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^k$.

<u>If $\gamma \in \Gamma$</u>: $\varphi(\gamma\cdot\tau) = f[\gamma]_k\, j(\gamma,\tau)^{-k} \cdot \overline{g[\gamma]_k\, j(\gamma,\tau)^{-k}} \cdot j(\gamma,\tau)^{2k} \cdot \mathrm{Im}(\tau)^k = \varphi(\tau)$

<u>If $\alpha \in SL_2(\mathbb{Z})$</u>: $\varphi(\alpha\cdot\tau) = f[\alpha]_k \cdot \overline{g[\alpha]_k} \cdot \mathrm{Im}(\tau)^k \underset{\substack{\wedge \\ f,g \text{ are cusp forms}}}{=} (* q_h + \cdots)\overline{(* q_h + \cdots)}\, y^k =$

$$= O(||q_h|^2 y^k) \longrightarrow 0 \text{ as } y \to \infty \quad \left(\text{as } q_h = e^{\frac{2\pi i(x+iy)}{h}}\right).$$

<u>Conclusion</u>: φ is Γ-invariant and $\varphi(\alpha\tau)$ is bounded on D^* $\forall \alpha \in SL_2(\mathbb{Z})$.

So $\langle f, g\rangle_\Gamma := \dfrac{1}{\mathrm{vol}(\Gamma)} \displaystyle\int_{X(\Gamma)} f(\tau)\overline{g(\tau)}\,\mathrm{Im}(\tau)^k\,d\mu(\tau)$ is <u>well-defined</u>.

<u>Note</u>: we only needed that one of the forms was in S_k. So the product of a modular form with a cusp form is defined.

<u>Note</u>: we divide by $\mathrm{vol}(\Gamma)$ so that if $\Gamma \subseteq \Gamma'$, $\langle f, g\rangle_\Gamma = \langle f, g\rangle_{\Gamma'}$.

Adjoint to an operator T:

T^* is defined by $\langle Tf, g\rangle = \langle f, T^* g\rangle$. (fin. dim vectorspaces!)

Goal: Thm 6.13: On $S_k(\Gamma_1(N))$ we have:

$$\left.\begin{array}{l}\langle p\rangle^* = \langle p\rangle^{-1} = \langle p^{-1}\rangle \\ T_p^* = \langle p\rangle^{-1} T_p\end{array}\right\} \text{ if } p \nmid N.$$

Corollary: The T_n with $(n,N)=1$ are normal: $T_n^* T_n = T_n T_n^*$. (and so are $\langle n\rangle$).

Spectral Theorem (for one normal operator):

If $(n,N)=1$, then $S_k(\Gamma_1(N))$ has an orthogonal bases of eigenforms for T_n (resp $\langle n\rangle$).

Thm 6.14: $S_k(\Gamma_1(N))$ has an orthogonal basis of $\overset{\text{simultaneous}}{\vee}$ eigenforms for all T_n, $\langle n\rangle$, with $(n,N)=1$.

Pf (sketch): List the operators $\Psi_1, \Psi_2, \dots$. Call $S := S_k(\Gamma_1(N))$

The spectral theorem allows to decompose $S = V_1 \oplus \cdots \oplus V_t$ where V_i are eigenspaces of Ψ_1; and each V_i has a orthogonal basis.

Ψ_2 ~~respect~~ preserves each V_i (because they commute), so spe. thm $\Rightarrow$ $V_i = W_1^{(i)} \oplus \cdots \oplus W_r^{(i)}$, where $W_r^{(i)}$ are are eigenspaces of Ψ_2, each with an orthogonal basis.

This process continues until it stops, because S is finite dimensional.

Eventually, $S = Y_1 \oplus \cdots \oplus Y_s$, Y_i eigenspaces for all Ψ_j. //

On $SL_2(\mathbb{Z})$: Note that $S_k(SL_2(\mathbb{Z})) = S_k(\Gamma_1(1))$ is has a basis of eigenforms $\forall T_n$. Normalize the eigenforms so that they are $f = q + \sum_{n\geq 2} a(n) q^n$

So $T_n f = a_n f$ $\forall n$.

Then a "package" of eigenvalues $\{\lambda_n\}_{n\geq 1}$ corresponds to a <u>unique</u> eigenform f.
We say that they have "multiplicity one", i.e that if $S = Y_1 \oplus \cdots \oplus Y_s$,
then $\dim Y_i = 1 \, (\forall i)$.

<u>General case $S_k(\Gamma_1(N))$:</u>

We've seen that we have a basis of eigenforms for T_n, $\langle n \rangle$ for $(n,N)=1$.

<u>Q:</u> 1) Basis of e-forms $\forall T_n$, $\langle n \rangle$?
2) Multiplicity one ?

<u>Recall</u>: $V_d f(\tau) := f(d\tau) = d^{1-k} f\left[\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right]_k$, $V_d : M_k(\Gamma_1(M)) \longrightarrow M_k(\Gamma_1(M\cdot d))$ (ex 1.2.11)

<u>Check</u>: $V_d U_t = U_t V_d$ if $(t,d)=1$. So $V_d T_n = T_n V_d$ if $(n,d)=1$.

<u>Example</u>: $\Delta(z)$, $\Delta(2z) \in S_{12}(\Gamma_1(2))$.

If $\Delta = \sum \tau(n) q^n$, then $T_p \Delta = \tau(p) \Delta \quad \forall p$.
(Here T_2 means T_2 on $S_{12}(SL_2(\mathbb{Z}))$)
By the previous remarks, $T_p(\Delta(2z)) = \tau(p)\Delta(2z) \quad \forall p \neq 2$.
So $\Delta(z)$, $\Delta(2z)$ have the same "package" of eigenvalues: $\{\tau(n)\}_{(n,2)=1}$
Hence there's no multiplicity one !

<u>However</u>: on $S_{12}(\Gamma_1(2))$, have T_p for $p \neq 2$ and U_2 (= T_2 as on $S_{12}(\Gamma_1(2))$)

Then note that
$$\begin{cases} \Delta(2z) | U_2 = \Delta(z) \\ \Delta(z) | U_2 = \Delta | T_2 - 2^{11} \Delta | V_2 = -24\Delta - 2^{11}\Delta(2z) \end{cases}$$

So the matrix of U_2 is:

$$\begin{pmatrix} -24 & 1 \\ -2^{11} & 0 \end{pmatrix}$$ which is diagonalizable.

Eigenvectors: $f_\pm = \left(\frac{-3}{512} \pm \frac{\sqrt{137}}{512}\right)\Delta + \Delta(2z) \Rightarrow$ can find a basis of eigenform for <u>all</u> T_n !

Another example: There may not be a basis of eigenforms for all T_p.

Take $f \in S_2(\Gamma_1(N))$ be an eigenform for $\begin{cases} T_q & q \nmid N \\ U_q & q \mid N \end{cases}$

Take $p \nmid N$, and let $S = \text{Span}\left(f(\tau), f(p\tau), f(p^2\tau), f(p^3\tau) \right)$ (4-dim'l)

Also, $S \subseteq S_2(\Gamma_1(Np^3))$

S is stable under T_q, $\binom{q \nmid N}{q \neq p}$ (as T_q and V_p commute).

Also, S is stable under U_q, $q \mid N$ (as they also commute with V_p).

Show (exercise): 1) S is stable under U_p.

(Turn in Friday 17th) 2) Compute the matrix of U_p and show that it's *not* diagonalizable,

(ez with linear algebra) So there's no basis of eigenforms for U_p.

Exercise 2: Use that $S_{24}(SL_2(\mathbb{Z}))$ is 2-dimensional, with a basis $f_1 = \Delta^2$, $f_2 = \Delta E_6^2$.

Compute a basis $\{g_1, g_2\}$ of eigenforms of *all* T_p, in terms of f_1 and f_2.

Hint: only need one T_p! and use a computer.

Newforms (Atkin-Lehner-Li):

If $M \mid N$, there are many ways to embed $S_k(\Gamma_1(M)) \hookrightarrow S_k(\Gamma_1(N))$.

In particular, can map $f \longmapsto V_d f$ for any d s.t. $dM \mid N$.

Def: $S_k(\Gamma_1(N))^{old} := \text{Span}\left\{ S_k(\Gamma_1(M)) | V_d \ : \ \substack{dM \mid N \\ M \neq N} \right\}$

$S_k(\Gamma_1(N))^{new} := \left(S_k(\Gamma_1(N))^{old} \right)^{\perp}$ under Petersson inner product.

Theorem 6.15:

a) S_k^{old}, S_k^{new} are stable under T_n, $\langle n \rangle$ $\forall n$.

b) S_k^{new} has a basis of eigenforms for all T_n, $\langle n \rangle$ ($\forall n$). (Take them $\overset{\text{leading coeff is } q.}{\text{normalized}}$).

These are called newforms.

↓

Thm 6.15 (restated)

a) S_k^{old}, S_k^{new} are stable under T_n, $\langle n \rangle$ $\forall n$.

b) S_k^{new} has a basis of normalized eigenforms for T_n, $\langle n \rangle$ $\forall n$. These are called <u>newforms</u> (only the eigenforms!).

c) f a newform $\Rightarrow f \in S_k(\Gamma_0(N), \chi)$ for some χ. If $f = \sum_{n \geq 1}^{\infty} a_n q^n$, then $T_n f = a_n f \cdot (\forall n)$.

d) If $\{\lambda_n\}_{(n,N)=1}$ is a "package" of eigenvalues for T_n with $(n,N)=1$, then $\exists !$ newform $f \in S_k(\Gamma_1(N))^{new}$ for some $M | N$ s.t $T_n f = \lambda_n f$ $\forall (n,N)=1$. One says that "multiplicity one" holds in the new subspace.

Pf omitted //

Write $S_k(\Gamma_1(N)) = V_1 \oplus \cdots \oplus V_t$ where V_i are common eigenspaces for T_n, $\langle n \rangle$ (for $(n,N)=1$).

Then every $f \in V_1$ has the same "package" $\{\lambda_n\}_{(n,N)=1}$. So by (6.15)(d), every $f \in V_1$ comes from a single newform, say $f_1 \in S_k(\Gamma_1(M_1))^{new}$ for some $M_1 | N$. And so $V_1 = \bigoplus_{dM_1 | N} \mathbb{C}(f_1 | V_d)$

Conclusion:

Thm 6.16: $S_k(\Gamma_1(N)) = \bigoplus_{M|N} \bigoplus_{dM|N} \left(S_k(\Gamma_1(M))^{new} | V_d \right)$ ← works also if we replace all 1 for 0.

Note on L-series

$f \in M_k(\Gamma_0(N), \chi)$, $f = \sum a_n q^n$. Its L-series is $L(f,s) = \sum a_n n^{-s}$ ($\mathrm{Re}\, s > k$)
($\mathrm{Re}\, s > \frac{k}{2}+1$) if f is a cusp form

Theorem 6.17: TFAE for $f = \sum a_n q^n \in S_k(\Gamma_0(N), \chi)$.

1) f is a normalized eigenform of <u>all</u> T_n.

2) $a_1 = 1$, $a_{mn} = a_m a_n$ if $(m,n)=1$, and $a_{p^r} = a_{p^{r-1}} a_p - \chi(p) p^{k-1} a_{p^{r-2}}$ if $r \geq 2$.

3) $L(f,s) = \sum a_n n^{-s} = \prod_p \left(1 - a_p p^{-s} + \chi(p) p^{k-1-2s}\right)^{-1}$.

• Galois Representations

The absolute Galois group $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = \varprojlim_{\substack{F/\mathbb{Q} \text{ finite} \\ \text{Galois ext.}}} \mathrm{Gal}(F/\mathbb{Q})$

So $\sigma \in G_{\mathbb{Q}}$ can be thought of $\sigma = \{\sigma_F\}_{F/\mathbb{Q} \text{ finite Galois}}$ such that, if

$$\begin{tikzcd} K \arrow[dr, dash] & & \\ & F \arrow[dr, dash] & \\ & & \mathbb{Q} \end{tikzcd}$$

, then $\sigma_K|_F = \sigma_F$.

Make it a topological group (Krull topology): a neighborhood basis of the identity is $\{\mathrm{Gal}(\overline{\mathbb{Q}}/K)\}$ K ranges over finite extension of $\mathbb{Q}$.

Note: $\mathrm{Gal}(\overline{\mathbb{Q}}/K) = \ker(G_{\mathbb{Q}} \to \mathrm{Gal}(K/\mathbb{Q}))$ are exactly the normal subgroups of finite index.

Theorem 7.1: $G_{\mathbb{Q}}$ is compact and Hausdorff.

Thm 7.2: (Fundamental Thm of Galois Theory):

There's a bijection:

$$\{\text{Extensions } K/\mathbb{Q}\} \longleftrightarrow \{\text{closed subgroups of } G_{\mathbb{Q}}\}.$$
$$K \longmapsto \mathrm{Gal}(\overline{\mathbb{Q}}/K).$$

Also, $K/\mathbb{Q}$ is finite $\iff \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is open.

Frobenius elements:

$\mathfrak{P} \subseteq \overline{\mathbb{Z}}$ prime ideal over p. (think $\mathfrak{P} \leftrightarrow \{\mathfrak{P}_F\}_{F/\mathbb{Q} \text{ finite}}$ st $\mathfrak{P}_K \cap F = \mathfrak{P}_F$).

Reduction map: $\overline{\mathbb{Z}} \longrightarrow \overline{\mathbb{Z}}/\mathfrak{P} = \overline{\mathbb{F}_p}$

Decomposition group: $D_{\mathfrak{P}} = \{\sigma \in G_{\mathbb{Q}} : \mathfrak{P}^{\sigma} = \mathfrak{P}\}$

Inertia group: $I_{\mathfrak{P}} = \{\sigma \in G_{\mathbb{Q}} : x^{\sigma} \equiv x \bmod \mathfrak{P} \ \forall x\}$.

we have that $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \langle \sigma_p \rangle$, $\sigma_p(\alpha)=\alpha^p$ (infinite cyclic).

We have a map/exact sequence:

$$\begin{tikzcd}
1 \arrow[r] & I_{\mathfrak{p}} \arrow[r] & D_{\mathfrak{p}} \arrow[r] & \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) \arrow[r] & 1 \\
& & \sigma \arrow[r, mapsto] & \left[\alpha+\mathfrak{p}) \mapsto \alpha^{\sigma}+\mathfrak{p}\right] &
\end{tikzcd}$$

Def: $\mathrm{Frob}_{\mathfrak{p}}$ is any preimage of σ_p. (defined up to inertia).

Note: if $\mathfrak{p}'$ is another prime over $\mathfrak{p}$, then $\mathfrak{p}' = \mathfrak{p}^{\sigma}$ for some σ,

and $D_{\mathfrak{p}'} = \sigma^{-1} D_{\mathfrak{p}} \sigma$. so $\mathrm{Frob}_{\mathfrak{p}'} = \sigma^{-1} \mathrm{Frob}_{\mathfrak{p}} \cdot \sigma$

Def: $\mathrm{Frob}_p := \mathrm{Frob}_{\mathfrak{p}}$ for some $\mathfrak{p}$ over p.

Thm 7.3: (Chebotarev density):

1) If $F/\mathbb{Q}$ is Galois and $\sigma \in \mathrm{Gal}(F/\mathbb{Q})$, then $\sigma = \mathrm{Frob}_p$ for infinitely many p.

ez $\Updownarrow$

2) Let S be a ~~finite~~ set of primes $\mathfrak{p}$ of $\mathbb{Z}$.

For all $\mathfrak{p} \notin S$, choose $\mathrm{Frob}_{\mathfrak{p}} \in G_{\mathbb{Q}}$. The set $\{\mathrm{Frob}_{\mathfrak{p}}\}_{\mathfrak{p}\notin S}$ is dense in $G_{\mathbb{Q}}$.

Pf (omit) //

Let now K be a #field, $\mathcal{O}_K$ its ring of integers.

Let ℓ be a prime of $\mathbb{Q}$, $\ell \mathcal{O}_K = \prod_{\lambda | \ell} \lambda^{e_\lambda}$ λ prime of $\mathcal{O}_K$.

Let K_λ be the completion of K at λ.

Then $\{$all such $K_\lambda\} \longleftrightarrow \{$finite extensions L of $\mathbb{Q}_\ell\}$.

↓

Def: A d-dimensional ℓ-adic Galois representation is a continuous homomorphism $\rho : G_\mathbb{Q} \longrightarrow GL_d(L)$. for L a finite ext. of $\mathbb{Q}_\ell$ (with the ℓ-adic topology on $\mathbb{Q}_\ell$, and L the vectorspace top over $\mathbb{Q}_\ell$).

Note: If $\rho : G_\mathbb{Q} \to GL_d(\mathbb{C})$ is continuous, then the image is finite, so it's not very useful.

Pf The topologies at each side are "very incompatible".

As $G_\mathbb{Q}$ is compact, $\mathrm{im}(\rho)$ is compact, sgp of $GL_d(\mathbb{C})$ containing the identity.

(example: for $d=1$, only get roots of unity $\Rightarrow$ finite). Can do the same for any d. //

We would like to evaluate $\rho(\mathrm{Frob}_p)$. This is only defined if $I_\mathfrak{p} \subseteq \mathrm{Ker}\,\rho$.

Def: ρ is unramified at p if $I_\mathfrak{p} \subseteq \mathrm{Ker}\,\rho$ (as $I_\mathfrak{p} \triangleleft \mathrm{Ker}\,\rho$, thus if $I_\mathfrak{p} \subseteq \mathrm{Ker}\,\rho$, then $I_{\mathfrak{p}'} \subseteq \mathrm{Ker}\,\rho$ too, if $\mathfrak{p}'|p$)

Example: $d=1$, χ a Dirichlet character mod N.

$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow K_\lambda$ for some λ (take $K = \mathbb{Q}(\mu_N)$, and complete it wrt any λ).

We know

$$\begin{tikzcd} & \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \arrow[r, "\simeq"] \arrow[dr, "\rho_{\chi,N}"'] & (\mathbb{Z}/N\mathbb{Z})^\times \arrow[d, "\chi"] \\ G_\mathbb{Q} \arrow[ur, "res"] & & K_\lambda \end{tikzcd}$$

So get a map $\rho_\chi : G_\mathbb{Q} \longrightarrow K_\lambda$, which is a representation of dimension 1 of $G_\mathbb{Q}$ (in $GL_1(K_\lambda)$).

[Facts about the topology in $G_{\mathbb{Q}}$ (Krull)

1) Every open subgroup is closed $\left(H = G_{\mathbb{Q}} \setminus \bigcup_{\sigma \neq 1} \sigma H \right)$

2) If H is an open subgroup, then $H = Gal(\overline{\mathbb{Q}}/K)$, K finite

$\left(G_{\mathbb{Q}} = \underset{\text{all cosets}}{\dot{\bigcup}} \sigma H \right.$. It's a disjoint open cover $\overset{G_{\mathbb{Q}} \text{ compact}}{\Longrightarrow}$ finite subcover, but as it is disjoint, we deduce that it's a finite union $\Rightarrow$ H has finite index).]

Facts about the ℓ-adic topology

Basis of nbhds of 1 is $\{1 + \ell^n \mathbb{Z}_\ell^*\}_{n \geq 1}$. (in $\mathbb{Q}_\ell$) and $\mathbb{Z}_\ell = \{x \in \mathbb{Q}_\ell : |x| \leq 1\}$

On K_λ, $\exists$ "uniformizer" π s.t $|\pi|_\lambda = \ell_{K_\ell}^{-\frac{1}{e_\lambda}}$ and $\mathcal{O}_\lambda = \{\alpha \in K_\lambda : |\alpha| \leq 1\}$.

(and a basis of nbhds around 1 is $\{1 + \pi^n \mathcal{O}_\lambda^\times\}_{n \geq 1}$) (if $\ell \mathcal{O}_K = \pi_\lambda^{e_\lambda}$)

Back to the last example, we will check that ρ_χ is a representation.

- Continuous:

Image finite $\Rightarrow$ Image discrete, so need to show that $\rho_\chi^{-1}(\{1\})$ open.

$\rho_{\chi,N}^{-1}(1) =$ a sgp of $Gal(\mathbb{Q}(\mu_n)/\mathbb{Q}) = Gal(\mathbb{Q}(\mu_n)/F)$ some F.

So $\rho_\chi^{-1}(1) = Gal(\overline{\mathbb{Q}}/F)$, some F ($\Rightarrow$ open)

- Ramification: if $p \nmid N$, then $res(I_p) = \{1\}$, so ρ_χ is unramified at p.

But it will be ramified at $p \mid N$.

Also, $\rho_\chi(Frob_p) = \chi(p)$.

Chebotarev $\Rightarrow$ $\forall \sigma \in Gal(\mathbb{Q}(\mu_n)/\mathbb{Q})$, $\exists$ ∞-ly many p with $Frob_p = \sigma$.

(ie. ∞-many $p \equiv a \pmod N$). $\Leftarrow$ Dirichlet's Theorem.

Note: if $\rho : G_{\mathbb{Q}} \to K_{\lambda}$ has finite image, then $\rho = \rho_{\chi}$ for some Dirichlet character χ.

pf/ $\mathrm{Ker}(\rho) \triangleleft G_{\mathbb{Q}}$, and $\mathrm{Ker}(\rho)$ has finite index (as finite image).

So $G_{\mathbb{Q}}/\ker\rho = \mathrm{Gal}(F/\mathbb{Q})$ for some F.

Hence ρ factors through $\tilde{\rho} : \mathrm{Gal}(F/\mathbb{Q}) \longrightarrow K_{\lambda}$.

$\mathrm{Gal}(F/\mathbb{Q})$ is abelian $\Rightarrow F \subseteq \mathbb{Q}(\mu_N)$ for some N (Kronecker-Weber)

And then by the example, $\rho = \rho_{\chi}$ for some χ mod N. //

Example 2: (a 1-dim representation with infinite image)

ℓ-adic cyclotomic character:

$\mathbb{Q}(\mu_{\ell^n})$ = field of ℓ^n-th roots of 1, and define $\mathbb{Q}(\mu_{\ell^\infty}) := \bigcup \mathbb{Q}(\mu_{\ell^n})$.

Write $\mathrm{Gal}(\mathbb{Q}(\mu_{\ell^\infty})/\mathbb{Q}) =: G_{\mathbb{Q},\ell}$.

An element $\sigma \in G_{\mathbb{Q},\ell}$ acts on all μ_{ℓ^n} $\forall n$. $(\mu_{\ell^n} \longmapsto \mu_{\ell^n}^{a_n},\ \ell \nmid a_n)$

As $\sigma(\mu_{\ell^n}) = \sigma(\mu_{\ell^{n+1}})^{\ell} = (\mu_{\ell^{n+1}}{}^{a_{n+1}})^{\ell} = \mu_{\ell^n}^{a_{n+1}}$. $\Rightarrow a_{n+1} \equiv a_n \pmod{\ell^n}$

So $G_{\mathbb{Q},\ell} \simeq \mathbb{Z}_{\ell}^{\times}$. Let $\chi_{\ell} : G_{\mathbb{Q}} \xrightarrow{res} G_{\mathbb{Q},\ell} \xrightarrow{\sim} \mathbb{Z}_{\ell}^{\times}$ be this composition.

Continuous: $\chi_{\ell}^{-1}(1 + \ell^n \mathbb{Z}_{\ell}^{\times}) = \{\sigma \text{ s.t. fix } \mu_{\ell}, \mu_{\ell^2}, \dots, \mu_{\ell^n}\} = \underset{\uparrow}{\mathrm{Gal}}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_{\ell^n}))$

open!

Ramification: If $p \neq \ell$, then χ_{ℓ} is unramified at p:

If $\sigma \in I_{\mathfrak{p}}$, then $\sigma(\mu_{\ell^n}) \equiv \mu_{\ell^n} \bmod \mathfrak{p}$ $\forall n$.

By Math 540, as $(\mathfrak{p}, \ell) = 1$, then $\sigma(\mu_{\ell^n}) = \mu_{\ell^n}$ $\forall n$ $\Rightarrow \sigma \in \ker \chi_{\ell}$.

Also, $\chi_{\ell}(\mathrm{Frob}_{\mathfrak{p}}) = p$ (as $\mathrm{Frob}_{\mathfrak{p}}$ maps μ_{ℓ^n} to $\mu_{\ell^n}^{p}$ mod $\mathfrak{p}$ $\Rightarrow \mu_{\ell^n} \longmapsto \mu_{\ell^n}^{p}$).

∘ Modular Galois Representations.

Let $f \in S_k(\Gamma_0(N), \chi)$ be a normalized eigenform, $f = \sum \underset{a_n}{\underset{\shortparallel}{a_n(f)}} q^n$.

Let $K_f = \mathbb{Q}(a_1, a_2, \dots)$.

Thm: $[K_f : \mathbb{Q}] < \infty$

$\rho(G_\mathbb{Q})$ doesn't fix any one-dimensional subspace.

Let ℓ be any prime, $\ell \mathcal{O}_{K_f} = \prod_{\lambda | \ell} \lambda^{e_\lambda}$.

Thm: With f, λ as above, there is an irreducible 2-dimensional
(7.3) Galois representation $\rho_{f,\lambda} : G_\mathbb{Q} \longrightarrow GL_2(K_{f,\lambda})$

Such that:

1) $\rho_{f,\lambda}$ is unramified almost everywhere. ($p \nmid \ell N$)

2) $\mathrm{Tr}\left(\rho_{f,\lambda}(\mathrm{Frob}_p)\right) = a_p \quad \forall p \nmid \ell N$

3) $\det\left(\rho_{f,\lambda}(\mathrm{Frob}_p)\right) = \chi(p)\, p^{k-1} \quad \forall p \nmid \ell N$.

(due to: $k=2$: Eichler-Shimura
$k>2$: Deligne
$k=1$: Deligne-Serre)

Note: If V is a 2-dim vectorspace $/L$, then a choice of basis makes $GL_2(L) \simeq \mathrm{Aut}(V)$.
Different choice of basis gives another representation $\rho' : G_\mathbb{Q} \longrightarrow GL_2(L)$
$\sigma \longmapsto M^{-1}\rho(\sigma) M$
One calls ρ and ρ' equivalent (in particular, they'll have the same trace and determinant).

Note: ρ reducible $\Longleftrightarrow$ ρ is equivalent to an "upper triangular" representation:

$$\rho(\sigma) = \begin{pmatrix} \psi_1(\sigma) & * \\ 0 & \psi_2(\sigma) \end{pmatrix} \qquad \psi_1, \psi_2 \text{ 1-dim representations}$$

Prop: Suppose $\rho : G_{\mathbb{Q}} \to GL_2(L)$ is a (continuous) representation.
(7.4) Then ρ is equivalent to a rep'n, $\rho' : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_L)$.

Pf Deferred.

Recall (Thm 7.3): $f \in S_k(\Gamma_0(N), \chi)$ normalized, $f = \sum a_n q^n$, $K_f = \mathbb{Q}(a_1, a_2, \ldots)$
λ a prime over ℓ, then $\exists$ ~~normalized~~ irreducible cont. Gal. rep.

$\rho_{f,\lambda} : G_{\mathbb{Q}} \longrightarrow GL_2(K_{f,\lambda})$.

s.t. 1) unramified at $p \nmid N\ell$

2) $Tr(\rho_{f,\lambda}(Frob_p)) = a_p$, $Det(\rho_{f,\lambda}(Frob_p)) = \chi(p) p^{k-1}$ $\forall p \nmid N\ell$

So now we can replace $K_{f,\lambda}$ with $\mathcal{O}_{f,\lambda}$ by 7.4.

Notes: • $Det \circ \rho_{f,\lambda} = \chi \cdot \chi_\ell^{k-1}$ (they agree on $Frob_p$'s, and they are dense).

• $Det(\rho_{f,\lambda}(\text{cpx conj})) = \chi(-1)\chi_\ell(-1)^{k-1} = \chi(-1)(-1)^{k-1} = (-1)^k(-1)^{k-1} = -1$

We say that $\rho_{f,\lambda}$ is odd.

Conjecture (Fontaine-Mazur): Every 2-dim irreducible odd geometric ← we haven't defined this! representation comes from a cusp form. (say it's modular).

Recall Eisenstein series.

$$E_k^{\psi,\varphi}(\tau) = \text{const} + 2 \cdot \sum_{n \geq 1} \sigma_{k-1}^{\psi,\varphi}(n) q^n \;;\; \sigma_{k-1}^{\psi,\varphi}(n) = \sum_{d \mid n} \psi(n/d)\varphi(d) d^{k-1}$$

Note that for p prime, $\sigma_{k-1}^{\psi,\varphi}(p) = \psi(p) + \varphi(p) p^{k-1}$

Set $\chi := \psi \cdot \varphi$, and let $f := \frac{1}{2} E_k^{\psi,\varphi}$. Define $\rho_{f,\lambda} := \begin{bmatrix} \psi & 0 \\ 0 & \varphi \chi_\ell^{k-1} \end{bmatrix}$

Then $Tr(\rho_{f,\lambda}(Frob_p)) = \psi(p) + \varphi(p) p^{k-1} = a_p(f)$!!

$Det(\rho_{f,\lambda}(Frob_p)) = \psi \cdot \varphi(p) p^{k-1} = \chi(p) p^{k-1}$

Consider now $\Delta \in S_{12}(\Gamma_0(1))$, $E_{12} \in M_{12}(\Gamma_0(1))$

$\Delta\# = \sum \tau(n)\, q^n$, $\quad E_{12}^* := \frac{-B_{12}}{24} + \sum \sigma_{11}(n)\, q^n$.

Ramanujan proved that $\tau(p) \equiv 1 + p^{11} \pmod{691}$

Let $\ell = 691$.

Then $\rho_{\Delta,691} : G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_{691})$. Can take (Prop 7.4) $G_{\mathbb{Q}} \to GL_2(\mathbb{Z}_{691})$

So get a reduction $\tilde{\rho}_{\Delta,691} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/691\mathbb{Z})$.

Similarly, have $\tilde{\rho}_{E_{12}^*,691} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/691\mathbb{Z})$

Now the congruence is saying (equivalent to) that $\tilde{\rho}_{\Delta,691} \overset{\substack{\text{equivalent to}\\ \downarrow}}{\sim} \tilde{\rho}_{E_{12}^*,691}$

Divisibility of coefficients of modular forms. (Serre, 1974).

$f \in M_k(\Gamma_1(N))$, $f = \sum a(n)\, q^n$.

Let K be a number field, $\mathcal{O} = \mathcal{O}_K$ its ring of integers, and assume $a(n) \in \mathcal{O}\ \forall n$.

As M_k is finite-dimensional, then there is some D s.t. if $a(n) \in K\ \forall n$, then $D\, a(n) \in \mathcal{O}\ \forall n$. So the assumption $a(n) \in \mathcal{O}$ is not restrictive.

Let $M \in \mathbb{N}$, and say $a \equiv 0 \bmod M$ meaning $a \in M\mathcal{O}$.

Thm (Serre): f, M as above. Then $\dfrac{\#\{n \le x : a(n) \not\equiv 0 \bmod M\}}{x} \to 0$ as $x \to \infty$.

(i.e. "almost all" the coefficients of f are divisible by M)

Examples: $a(n) = \sigma_{k-1}(n)$

$a(n) = \tau(n)$ $\quad (\Delta = \sum \tau(n)\, q^n)$

$\theta(z) = \sum q^{n^2}$, $\quad \theta(z)^s = \sum r_s(n)\, q^n$, $\quad r_s(n) = \#$ representations of n as a sum of s squares.

Then if s is even, $\theta(z)^s$ has weight $\frac{s}{2}$ on $\Gamma_0(4)$.

A more precise version of the theorem:

Define $E_{f,M} := \{ n \in \mathbb{N} : a(n) \equiv 0 \bmod M \}$.

$E_{f,M}(x) := \# \{ n \leq x : n \in E_{f,M} \}$.

Thm: Given f, M, $\exists\, \alpha > 0$ s.t. $x - E_{f,M}(x) = O\left(\frac{x}{(\log x)^{\alpha}} \right)$

(the other theorem just asserted that $E_{f,M}(x) \sim x$)

We need some ingredients for the proof.

① Mod M representations.

Lemma: Let f be an eigenform of level N, with coefficients in $\mathcal{O}$, and $M \in \mathbb{N}$.

Then $\exists$ a finite Galois ext. F of $\mathbb{Q}$, unramified outside $M \cdot N$, and a representation $\rho : Gal(F/\mathbb{Q}) \to GL_2(\mathcal{O}/M\mathcal{O})$ such that $Tr(\rho(Frob_p)) \equiv a(p) \bmod M$ for all $p \nmid MN$.

Pf (sketch) Factor $M\mathcal{O} = \prod \lambda_i^{e_i}$, $\forall i$, $\exists\, \rho_i : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_{\lambda_i})$.

Reduce, to get $\bar{\rho}_i : G_{\mathbb{Q}} \to GL_2\left(\mathcal{O}_{\lambda_i} / \lambda_i^{e_i} \mathcal{O}_{\lambda_i}\right) \simeq GL_2\left(\mathcal{O} / \lambda_i^{e_i} \mathcal{O}\right)$

Define now $\rho := \prod \bar{\rho}_i : G_{\mathbb{Q}} \to \prod GL_2\left(\mathcal{O}/\lambda_i^{e_i}\mathcal{O}\right) \underset{\substack{\uparrow \\ CRT}}{\simeq} GL_2\left(\mathcal{O}/M\mathcal{O}\right)$

As the image of ρ is finite, the kernel is open (normal + finite index) $\Rightarrow$

$\Rightarrow Ker = Gal(\bar{\mathbb{Q}}/F) \Rightarrow \checkmark$.

//

Ⅱ Reduce to the case of an eigenform.

Given $\underset{\in M_k(\Gamma_1(N))}{f = \sum a(n) q^n}$, $a(n) \in \mathcal{O}$. Write $f = \sum \alpha_i f_i$, $f_i \in M_k(\Gamma_0(N), \chi_i)$

where the f_i are eigenforms. They have coefficients in $\bar{\mathbb{Z}}$.

The $\alpha_i \in \bar{\mathbb{Q}}$.

As $f=\sum \alpha_i f_i$ is a finite sum, can choose $D\neq 0$ s.t. $D\alpha_i \in \bar{\mathbb{Z}}$ $\forall i$.
Now enlarge O to contain all α_i and the coeff's of f_i.

If the n^{th} coefficient of each f_i is divisible by DM, then the n^{th} coefficient of f is divisible by M.
So if we prove the theorem for eigenforms, the general statement will follow.

III Artin L-series.

Zeta-function: $\zeta(s)=\sum n^{-s} = \prod(1+p^{-s}+p^{-2s}+\dots) = \prod_p \frac{1}{1-p^{-s}}$ Re $s>1$
s'ple pole at $s=1$.

$$\log \zeta(s) = \sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{ms}} = \sum_p \frac{1}{p} + \left(\sum_p \sum_{m\geq 2} \frac{1}{mp^{ms}}\right)$$ Converges (analytic). at $s=1$

Write $f(s)\sim g(s)$ if $f(s)-g(s)$ is analytic at $s=1$.

So: $\log \zeta(s) \sim \sum \frac{1}{p^s}$.

Artin L-functions: $G=\mathrm{Gal}(F/\mathbb{Q})$ unramified outside D.
Let χ be a character, $\chi: G\to \mathbb{C}^\times$. $\in G$ may not be abelian!

Artin L-function: $$L(s,\chi):=\prod_{p\nmid D} \frac{1}{1-\chi(\mathrm{Frob}_p)p^{-s}}$$

Note: if $\chi=1$, $L(s,1)$ has a simple pole at $s=1$.
if $\chi\neq 1$, $L(s,\chi)$ has analytic continuation to a holomorphic non-vanishing function at $s=1$.

One can see easily that $\log L(s,\chi) \sim \sum_{p\nmid D} \frac{\chi(\mathrm{Frob}\, p)}{p^s}$.

IV Key Theorem: $F/\mathbb{Q}$ finite Galois with group G, and $H\leq G$ stable under conjugation.
Let $P=\{2,3,5,7,\dots\}$ ~~and~~ $P(H)=\{p\in P: p\nmid D, \mathrm{Frob}_p \in H\}$.

Chebotarev: $$\frac{\#\{p\leq x: p\in P(H)\}}{(x/\log x)} \to \frac{h}{g}$$ where $\#H=h$, $\#G=g$.

exactly dividing n.

Set now $E_H := \{ n \in \mathbb{N} : \exists\, p \in P(H) \text{ with } p \| n \}$. ; $E_H(x) = \{ n \leq x : n \in E_H \}$

Key Thm: Suppose $H \neq G$. Then $\exists\, C > 0$ s.t $x - E_H(x) \sim C \frac{x}{\log^{\alpha} x}$, $\alpha = \frac{h}{g}$

Proof: If $H = \emptyset$, take $C = 1$ ✓. So spse $H \neq \emptyset$.

Define $f(s) := \sum_{n \notin E_H} n^{-s}$, which converges for $\mathrm{Re}(s) > 1$.

write $f(s) = \sum_{n=1}^{\infty} b_n n^{-s}$, $M(x) := \sum_{n \leq x} b_n$. ($b_n \in \{0,1\}$).

Note that $M(x) = \#\{ n \leq x : n \notin E_H \}$ is what we want to estimate!

"Tauberian Thm": relates the asymptotics of $M(x)$ to the behavior of $f(s)$ at $s=1$.

Thm: If $f(s) = \frac{c(s)}{(s-1)^{1-\alpha}}$, $0 < \alpha < 1$ where $c(s)$ hol. and $c(1) \neq 0$,

then $M(x) \sim \frac{Cx}{\log^{\alpha} x}$

~~Pf~~ Proved in the '40's. //.

There's an Euler product for $f(s)$: $f(s) = \prod_{p \notin P(H)} (1 + p^{-s} + p^{-2s} + \dots) \cdot \prod_{p \in P(H)} (1 + p^{-2s} + p^{-3s} + \dots)$

So $\log f(s) \sim \sum_{p \notin P(H)} \frac{1}{p^s}$ ← Approximated using Artin L-functions.

Correct definition of the Artin L-function

$$L(s,\chi) = \prod_{p \text{ unram.}} \frac{1}{1 - \chi(\mathrm{Frob}_p) p^{-s}} \prod_{\substack{p \text{ ram.} \\ \chi(I_p) = 1}} \frac{1}{1 - \chi(\mathrm{Frob}_p) p^{-s}}$$

So in this case, $L(s,1) = \zeta(s)$.

Then $\log L(s,\chi) \sim \sum \frac{\chi(\mathrm{Frob}_p)}{p^s}$

We use orthogonality of characters:

$$\frac{1}{g} \sum_{\chi} \chi(\sigma) = \begin{cases} 1 & \sigma = id \\ 0 & \text{else.} \end{cases}$$

(cont pf)

The characteristic function of $G \setminus H$ is $\rho(\tau) = \sum_{\chi} \mu_\chi \chi(\tau)$; $\mu_\chi = \frac{1}{g} \sum_{\sigma \notin H} \overline{\chi}(\sigma)$

Check: $\rho(\tau) = \sum_{\sigma \notin H} \frac{1}{g} \sum_{\chi} \chi(\tau\sigma^{-1}) = \begin{cases} 1 & \tau \notin H \\ 0 & \text{else.} \end{cases}$ ✓.

Note that $\mu_1 = \frac{1}{g}(g-h) = 1 - \frac{h}{g}$.

Define $g(s) := \sum_{\chi} \mu_\chi \log L(s,\chi) \sim \sum_{p} \frac{\rho(\mathrm{Frob}_p)}{p^s} \overset{\substack{\text{actually equals} \\ \downarrow}}{\sim} \sum_{p \notin P(H)} \frac{1}{p^s} = \log f(s)$

Exponentiating, $f(s) = h(s) \cdot e^{g(s)}$ where $h(s)$ is holomorphic an $\neq 0$ at $s=1$.

So $f(s) = h(s) \prod_{\chi} L(s,\chi)^{\mu_\chi}$.

If $\chi \neq 1$, then $L(s,\chi)$ is holomorphic and $\neq 0$ at $s=1$. Also, $L(s,1) = \zeta(s)$, which has a simple pole at $s=1$.

So $f(s) = \frac{c(s)}{(s-1)^{\mu_1}} = \frac{c(s)}{(s-1)^{1-h/g}}$. By the Tauberian theorem, we are done.

Lemma: Spz $f(z) = \sum a(n) q^n$ is a normalized eigenform, and $M \in \mathbb{N}$. Then $\exists$ ~~subset~~ finite Galois extension $F/\mathbb{Q}$, with Galois gp G, and a subset $\emptyset \neq H \subsetneq G$, stable under conjugation, such that

$$a(p) \equiv 0 \mod M \quad \forall p \in P(H)$$

Proof: Let ρ be the mod M Galois representation from last page.

i.e. $\rho : \mathrm{Gal}(F/\mathbb{Q}) \longrightarrow GL_2(\mathcal{O}/M\mathcal{O})$, s.t. $\mathrm{Tr}(\rho(\mathrm{Frob}_p)) \equiv a(p) \mod M$ (if $p \nmid MN$).

Let $H := \{\sigma \in G : \mathrm{Tr}(\rho(\sigma)) \equiv 0 \mod M\}$

H is stable under conjugation, as Tr is invariant under conj.

Also, $\mathrm{Tr}(\rho(\mathrm{id})) = \mathrm{Tr}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 2 \not\equiv 0 \mod M$ if $M \geq 3$ (if $M=2$, replace M by a multiple of it!)

Also, $\mathrm{Tr}(\rho(c)) = 0$ (if c = cpx conj. with $\underset{\downarrow}{\text{your}}$ poly X^2+1). ← if $F/\mathbb{Q}$ is real, just enlarge it so it has imaginary!

(cont pf of Lemma)

Again, let $E_M = \{ n : \exists p \in p(M) : p \| n \}$.

$f(z) = \sum a(n) q^n$, and $T_p f = \sum \left(a(pn) + \chi(p) p^{k-1} a(n/p) \right) q^n = a(p) \cdot \sum a(n) q^n$.

So if $p \nmid n$, then ~~$a(n)$~~ $\overset{\swarrow RHS}{a(p) a(n)} = a(pn)^{\leftarrow LHS}$.

So if $n' \in E_M$, then $a(n') \equiv 0$ because $n' = pn$ and $a(n') = a(p) a(n) \equiv 0 \pmod{M}$.

E.O.C.

From Silverman's elliptic curves te

if the periods ω_1 and ω_2 which generate Λ are linearly independent over $\mathbb{R}$. This turns out to be the case; and further, F gives a complex analytic isomorphism from $E(\mathbb{C})$ to $\mathbb{C}/\Lambda$. However, rather than proving these facts here, we will instead turn to the study of the space $\mathbb{C}/\Lambda$ for a given lattice Λ. In section 3 we will construct the inverse to the mapping F, and show that $\mathbb{C}/\Lambda$ is analytically isomorphic to $E_\Lambda(\mathbb{C})$ for a certain elliptic curve $E_\Lambda/\mathbb{C}$. The uniformization theorem (5.1) then says that every elliptic curve $E/\mathbb{C}$ is isomorphic to some E_Λ, from which we will be able to deduce (5.2) that the periods of $E/\mathbb{C}$ are $\mathbb{R}$-linearly independent and that F is a complex analytic isomorphism. (For a direct proof of the independence, which uses only Stokes' theorem in $\mathbb{R}^2$, see [Cle, §2.9].)

§2. Elliptic Functions

Let $\Lambda \subset \mathbb{C}$ be a *lattice*; that is, Λ is a discrete subgroup of $\mathbb{C}$ which contains an $\mathbb{R}$-basis for $\mathbb{C}$. In this section we will study meromorphic functions on the quotient space $\mathbb{C}/\Lambda$; or equivalently, meromorphic functions on $\mathbb{C}$ which are periodic with respect to the lattice Λ.

Definition. An *elliptic function* (*relative to the lattice* Λ) is a meromorphic function $f(z)$ on $\mathbb{C}$ which satisfies

$$f(z+\omega) = f(z) \qquad \text{for all } \omega \in \Lambda,\ z \in \mathbb{C}.$$

The set of all such functions is denoted $\mathbb{C}(\Lambda)$. $\mathbb{C}(\Lambda)$ is clearly a field.

Definition. A *fundamental parallelogram* for Λ is a set of the form

$$D = \{a + t_1\omega_1 + t_2\omega_2 : 0 \leqslant t_1, t_2 < 1\},$$

where $a \in \mathbb{C}$ and ω_1, ω_2 are a basis for Λ. Thus the map of sets $D \to \mathbb{C}/\Lambda$ is bijective. We denote the closure of D in $\mathbb{C}$ by $\bar{D}$. (A lattice and three different fundamental parallelograms are illustrated in Figure 6.6.)

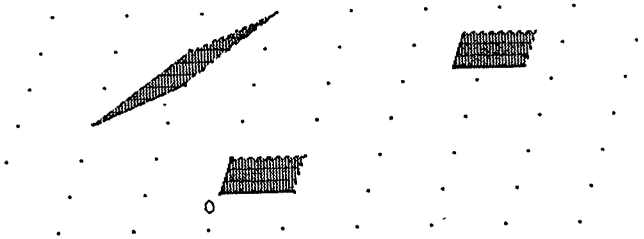


Figure 6.6

Proposition 2.1. *An elliptic function with no poles (or no zeros) is constant.*

Proof. Suppose that $f(z) \in \mathbb{C}(\Lambda)$ is holomorphic. Let D be a fundamental parallelogram for Λ. Then the periodicity of f implies that

$$\sup_{z\in\mathbb{C}} |f(z)| = \sup_{z\in\bar{D}} |f(z)|.$$

But f is continuous and $\bar{D}$ is compact, so $|f(z)|$ is bounded on $\bar{D}$, hence it is bounded on all of $\mathbb{C}$. Therefore, by Liouville's theorem ([Ahl, ch. 4, §2.3]), f is constant. Finally, if f has no zeros, look at $1/f$. □

Let f be an elliptic function, and let $w \in \mathbb{C}$. Then, as for any meromorphic function, we can define

$$\operatorname{ord}_w(f) = \text{order of vanishing of } f \text{ at } w, \text{ and}$$

$$\operatorname{res}_w(f) = \text{residue of } f \text{ at } w$$

(cf. [Ahl, ch. 4, §3.2, §5.1]). However, since f is elliptic, we see that the order and residue of f remain the same if w is replaced by $w + \omega$ for any $\omega \in \Lambda$. This prompts the following convention.

Notation. By $\Sigma_{w\in\mathbb{C}/\Lambda}$ we mean a sum over $w \in D$, where D is a fundamental parallelogram for Λ. (By implication, the resulting sum is independent of the choice of D.)

Notice that (2.1) is the complex analogue of (II.1.2), which says that an algebraic function without poles is constant. The next theorem and corollary continue this theme by proving for $\mathbb{C}/\Lambda$ results analogous to parts of (II.3.1) and (III.3.5).

Theorem 2.2. *Let* $f \in \mathbb{C}(\Lambda)$.

(a) $\sum_{w\in\mathbb{C}/\Lambda} \operatorname{res}_w(f) = 0.$

(b) $\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f) = 0.$

(c) $\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f) w \in \Lambda.$

Proof. Let D be a fundamental parallelogram for Λ such that $f(z)$ has no poles or zeros on the boundary ∂D of D. All three parts of the theorem are simple applications of the residue theorem [Ahl, ch. 4, thm. 19] applied to appropriately chosen functions on D.

(a) By the residue theorem,

$$\sum_{w\in\mathbb{C}/\Lambda} \operatorname{res}_w(f) = \frac{1}{2\pi i}\int_{\partial D} f(z)\,dz.$$

Now the periodicity of f implies that the integrals along the opposite sides of the parallelogram cancel, so the total integral around the boundary of D is zero.

(b) The periodicity of $f(z)$ implies that $f'(z)$ is also periodic, so applying (a) to the elliptic function $f'(z)/f(z)$ gives

$$\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f) = \frac{1}{2\pi i}\int_{\partial D}\frac{f'(z)}{f(z)}dz = 0.$$

(c) We apply the residue theorem to the function $zf'(z)/f(z)$

$$\begin{aligned}\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f)w &= \frac{1}{2\pi i}\int_{\partial D} zf'(z)/f(z)dz\\ &= \frac{1}{2\pi i}\left(\int_a^{a+\omega_1} + \int_{a+\omega_1}^{a+\omega_1+\omega_2} + \int_{a+\omega_1+\omega_2}^{a+\omega_2} + \int_{a+\omega_2}^{a}\right)zf'(z)/f(z)dz.\end{aligned}$$

Now in the second (respectively third) integral make the change of variable $z \to z - \omega_1$ (respectively $z - \omega_2$). Then using the periodicity of f'/f yields

$$\sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f)w = -\frac{\omega_2}{2\pi i}\int_a^{a+\omega_1}\frac{f'(z)}{f(z)}dz + \frac{\omega_1}{2\pi i}\int_a^{a+\omega_2}\frac{f'(z)}{f(z)}dz.$$

But for any meromorphic function $g(z)$, the integral

$$\frac{1}{2\pi i}\int_a^b \frac{g'(z)}{g(z)}dz$$

is the winding number around 0 of the path

$$[0, 1] \to \mathbb{C}, \qquad t \to g((1-t)a + tb);$$

and in particular, if $g(a) = g(b)$, then the integral is an integer. Hence the periodicity of $f'(z)/f(z)$ implies that $\Sigma \operatorname{ord}_w(f)w$ has the desired form. □

Definition. The *order* of an elliptic function is its number of poles (counted with multiplicity) in any fundamental parallelogram. (Note that from (2.2b), the order is also equal to the number of zeros.)

Corollary 2.3. *A non-constant elliptic function has order at least* 2.

PROOF. If $f(z)$ has a single simple pole, then from (2.2a) the residue at that pole is 0, so f is actually holomorphic. Now apply (2.1). □

We now define the *divisor group* $\operatorname{Div}(\mathbb{C}/\Lambda)$ to be the group of formal linear combinations $\Sigma_{w\in\mathbb{C}/\Lambda} n_w(w)$ with $n_w \in \mathbb{Z}$ and $n_w = 0$ for all but finitely many w. Then for $D = \Sigma n_w(w) \in \operatorname{Div}(\mathbb{C}/\Lambda)$, we define

$$\deg D = \text{degree of } D = \sum n_w \text{ and } \operatorname{Div}^0(\mathbb{C}/\Lambda) = \{D \in \operatorname{Div}(\mathbb{C}/\Lambda) : \deg D = 0\}.$$

From (2.2b), for any $f \in \mathbb{C}(\Lambda)^*$ we can define a divisor $\operatorname{div}(f) \in \operatorname{Div}^0(\mathbb{C}/\Lambda)$ by

$$\operatorname{div}(f) = \sum_{w\in\mathbb{C}/\Lambda} \operatorname{ord}_w(f)(w).$$

Clearly the map $\operatorname{div} : \mathbb{C}(\Lambda)^* \to \operatorname{Div}^0(\mathbb{C}/\Lambda)$ is a homomorphism, since each ord_w is a valuation. Finally, we define a *summation map*

$$sum\colon \operatorname{Div}^0(\mathbb{C}/\Lambda) \to \mathbb{C}/\Lambda \qquad sum\left(\sum n_w(w)\right) = \sum n_w w \pmod{\Lambda}.$$

The following exact sequence encompasses our main results on $\mathbb{C}/\Lambda$, as well as one fact (3.4) to be proven in the next section.

Theorem 2.4. *The sequence*

$$1 \to \mathbb{C}^* \to \mathbb{C}(\Lambda)^* \xrightarrow{\text{div}} \operatorname{Div}^0(\mathbb{C}/\Lambda) \xrightarrow{\text{sum}} \mathbb{C}/\Lambda \to 0$$

is exact.

PROOF. Exactness on the left is clear, and on the right follows from $sum((w) - (0)) = w$. Exactness at $\mathbb{C}(\Lambda)^*$ is (2.1), and exactness at $\operatorname{Div}^0(\mathbb{C}/\Lambda)$ is (2.2c) and (3.4). □

§3. Construction of Elliptic Functions

In order to show that the results of section 2 are not vacuous, we must construct some non-constant elliptic functions. By (2.3), any such function will have order at least 2. Following Weierstrass, we look for a function with a pole of order 2 at $z = 0$.

Definition. Let $\Lambda \subset \mathbb{C}$ be a lattice. The *Weierstrass* $\wp$*-function* (*relative to* Λ) is defined by the series

$$\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}.$$

The *Eisenstein series of weight* $2k$ (*for* Λ) is the series

$$G_{2k}(\Lambda) = \sum_{\substack{\omega\in\Lambda\\ \omega\neq 0}} \omega^{-2k}.$$

(For notational convenience, we write $\wp(z)$ and G_{2k} if the lattice Λ has been fixed.)

Theorem 3.1. *Let* $\Lambda \subset \mathbb{C}$ *be a lattice.*

(a) *The Eisenstein series* G_{2k} *for* Λ *is absolutely convergent for all* $k > 1$.

(b) *The series defining the Weierstrass* $\wp$*-function converges absolutely and*

From Koblitz

Collecting coefficients of a fixed power q^n in the last double sum, we obtain the sum in (2.6) as the coefficient of q^n. This completes the proof. □

Because of Proposition 6, it is useful to define the "normalized Eisenstein series", obtained by dividing $G_k(z)$ by the constant $2\zeta(k)$ in (2.7):

$$E_k(z) = \frac{1}{2\zeta(k)} G_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n. \tag{2.11}$$

Thus, $E_k(z)$ is defined so as to have *rational* q-expansion coefficients. The first few E_k are:

$$E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n) q^n;$$

$$E_6(z) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n) q^n;$$

$$E_8(z) = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n) q^n;$$

$$E_{10}(z) = 1 - 264 \sum_{n=1}^{\infty} \sigma_9(n) q^n;$$

$$E_{12}(z) = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_{11}(n) q^n;$$

$$E_{14}(z) = 1 - 24 \sum_{n=1}^{\infty} \sigma_{13}(n) q^n.$$

An alternate way of defining the normalized Eisenstein series is to sum only over relatively prime pairs m, n in (2.5):

$$E_k(z) = \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n)=1}} \frac{1}{(mz+n)^k}, \tag{2.12}$$

where (m, n) denotes the greatest common divisor. The equivalence of (2.12) and (2.11) will be left as an exercise (see below).

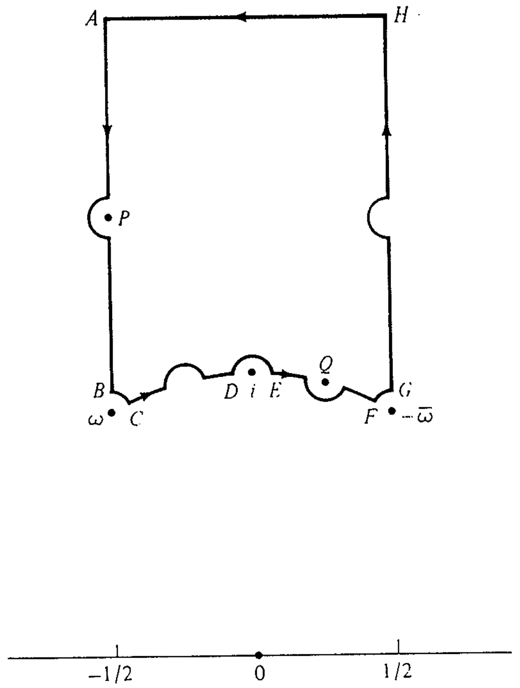


Figure III.4. Contour for the proof of Proposition 8.

The next result will play a basic role in determining the spaces $M_k(\Gamma)$ and $S_k(\Gamma)$ of modular forms and cusp-forms of given weight for Γ, and it will also be useful in proving that two modular forms defined in different ways are actually the same in certain cases.

Thm 3 .. *Let $f(z)$ be a nonzero modular function of weight k for Γ. For $P \in H$, let $v_P(f)$ denote the order of zero (or minus the order of pole) of $f(z)$ at the point P. Let $v_\infty(f)$ denote the index of the first nonvanishing term in the q-expansion of $f(z)$. Then*

$$v_\infty(f) + \frac{1}{2} v_i(f) + \frac{1}{3} v_\omega(f) + \sum_{P \in \Gamma\backslash H, P \neq i, \omega} v_P(f) = \frac{k}{12}. \tag{2.21}$$

(*Note*. It is easy to check that $v_P(f)$ does not change if P is replaced by γP for $\gamma \in \Gamma$.)

Proof. The idea of the proof is to count the zeros and poles in $\Gamma\backslash H$ by integrating the logarithmic derivative of $f(z)$ around the boundary of the fundamental domain F. More precisely, let C be the contour in Fig. III.4. The top of C is a horizontal line from $H = \frac{1}{2} + iT$ to $A = -\frac{1}{2} + iT$, where T is taken larger than the imaginary part of any of the zeros or poles of $f(z)$.

(*Note*. That this can be done, i.e., that $f(z)$ does not have poles or zeros with arbitrarily large imaginary part, follows from the fact that the change of variables $q = e^{2\pi iz}$ makes $f(z)$ into a meromorphic function of q in a disc around $q = 0$.) The rest of the contour follows around the boundary of F, except that it detours around any zero or pole on the boundary along circular arcs of small radius ε. This is done in such a way as to include every Γ-equivalence class of zero or pole exactly once inside C, except that i and ω (and $S\omega = -\bar{\omega}$) are kept outside of C if they are zeros or poles. In Fig. III.4 we have illustrated the case when the zeros and poles on the boundary of F consist of i, ω (and hence also $S\omega$), one point P on the vertical boundary line (and hence also the Γ-equivalent point on the opposite line), and one point Q on the unit circle part of the boundary (and hence also SQ).

According to the residue theorem, we have

$$\frac{1}{2\pi i}\int_C \frac{f'(z)}{f(z)}dz = \sum_{P\in\Gamma\backslash H,\, P\neq i,\omega} v_P(f). \tag{2.22}$$

On the other hand, we evaluate the integral in (2.22) section by section. First of all, the integral from A to B (see Fig. III.4) cancels the integral from G to H, because $f(z+1) = f(z)$, and the lines go in opposite directions. Next, we evaluate the integral over HA. To do this we make the change of variables $q = e^{2\pi iz}$. Let $\tilde{f}(q) = f(z) = \Sigma a_n q^n$ be the q-expansion. Since $f'(z) = \frac{d}{dq}\tilde{f}(q)\frac{dq}{dz}$, we find that this section of the integral in (2.22) is equal to the following integral over the circle of radius $e^{-2\pi T}$ centered at zero:

$$\frac{1}{2\pi i}\int \frac{d\tilde{f}/dq}{\tilde{f}(q)}dq.$$

Since the circle is traversed in a clockwise direction as z goes from H to A, it follows that this integral is minus the order of zero or pole of $\tilde{f}(q)$ at 0, and this is what we mean by $-v_\infty(f)$.

To evaluate the integral over the arcs BC, DE, and FG, recall the derivation of the residue formula. If $f(z)$ has Laurent expansion $c_m(z-a)^m + \cdots$ near a, with $c_m \neq 0$, then $f'(z)/f(z) = \frac{m}{z-a} + g(z)$, with $g(z)$ holomorphic at a. If we integrate $f'(z)/f(z)$ counterclockwise around a circular arc of angle θ centered at a with small radius ε, then as $\varepsilon \to 0$ this integral approaches $mi\theta$ (the usual residue formula results when $\theta = 2\pi$). We apply this to the section of (2.22) between B and C, letting $\varepsilon \to 0$. The angle approaches $\pi/3$, and so we obtain $-\frac{1}{2\pi i}(v_\omega(f)i\pi/3) = -v_\omega(f)/6$. (The minus sign is because the arc BC goes clockwise.) In the same way, we find that as $\varepsilon \to 0$ the part of (2.22) from D to E becomes $-v_i(f)/2$, and the part between F and G becomes $-v_{-\bar{\omega}}(f)/6 = -v_\omega(f)/6$.

What remains is the integral from C to D and from E to F. Combining the above calculations, we find from (2.22) that the left side of (2.21) is equal to that remaining section of the left side of (2.22). Thus, to prove Proposition 8, it remains to show that in the limit as $\varepsilon \to 0$

$$\frac{1}{2\pi i}\int_{CD}\frac{f'(z)}{f(z)}dz + \frac{1}{2\pi i}\int_{EF}\frac{f'(z)}{f(z)}dz \to \frac{k}{12}. \tag{2.23}$$

To compute the sum of these two integrals, we note that the transformation $S\colon z \mapsto -1/z$ takes CD to EF, or more precisely, to FE, i.e., Sz goes from F to E along the contour as z goes from C to D along the contour. The desired formula (2.23) will follow from the following more general lemma.

Lemma. *Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, with $c \neq 0$, and let $f(z)$ be a meromorphic function on H with no zeros or poles on a contour $C \subset H$. Suppose that $f(\gamma z) = (cz+d)^k f(z)$. Then*

$$\int_C \frac{f'(z)}{f(z)}dz - \int_{\gamma C}\frac{f'(z)}{f(z)}dz = -k\int_C \frac{dz}{z+(d/c)}. \tag{2.24}$$

The required equality (2.23) follows immediately from the lemma, where we set $\gamma = S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, note that $S(CD) = FE$, and compute that as $\varepsilon \to 0$

$$\frac{1}{2\pi i}\int_{CD}\frac{dz}{z} \to \int_{1/3}^{1/4} d\theta = -\frac{1}{12} \qquad (\text{where } z = e^{2\pi i\theta}).$$

Proof of the Lemma. Differentiating

$$f(\gamma z) = (cz+d)^k f(z), \tag{2.25}$$

we obtain

$$f'(\gamma z)\frac{d\gamma z}{dz} = (cz+d)^k f'(z) + kc(cz+d)^{k-1}f(z). \tag{2.26}$$

We now divide (2.26) by (2.25):

$$\frac{f'(\gamma z)}{f(\gamma z)}d\gamma z = \frac{f'(z)}{f(z)}dz + k\frac{cdz}{cz+d}.$$

Thus, the left side of (2.24) is equal to

$$\int_C \frac{f'(z)}{f(z)}dz - \frac{f'(\gamma z)}{f(\gamma z)}d\gamma z = -k\int_C \frac{cdz}{cz+d}.$$

This completes the proof of the lemma, and of Proposition 8. □

We now derive several very useful consequences of Proposition 8.

Thm 4. *Let k be an even integer, $\Gamma = SL_2(\mathbb{Z})$.*

- (a) *The only modular forms of weight 0 for Γ are constants, i.e., $M_0(\Gamma) = \mathbb{C}$.*
- (b) *$M_k(\Gamma) = 0$ if k is negative or $k = 2$.*
- (c) *$M_k(\Gamma)$ is one-dimensional, generated by E_k, if $k = 4, 6, 8, 10$ or 14; in other words, $M_k(\Gamma) = \mathbb{C}E_k$ for those values of k.*
- (d) *$S_k(\Gamma) = 0$ if $k < 12$ or $k = 14$; $S_{12}(\Gamma) = \mathbb{C}\Delta$; and for $k > 14$ $S_k(\Gamma) =$*

$\Delta M_{k-12}(\Gamma)$ (*i.e., the cusp forms of weight k are obtained by multiplying modular forms of weight $k-12$ by the function $\Delta(z)$*).

(e) $M_k(\Gamma) = S_k(\Gamma) \oplus \mathbb{C}E_k$ *for* $k > 2$.

PROOF. Note that for a modular *form* all terms on the left in (2.21) are nonnegative.

(a) Let $f \in M_0(\Gamma)$, and let c be any value taken by $f(z)$. Then $f(z) - c \in M_0(\Gamma)$ has a zero, i.e., one of the terms on the left in (2.21) is strictly positive. Since the right side is 0, this can only happen if $f(z) - c$ is the zero function.

(b) If $k < 0$ or $k = 2$, there is no way that the sum of nonnegative terms on the left in (2.21) could equal $k/12$.

(c) When $k = 4, 6, 8, 10$, or 14 we note that there is only one possible way of choosing the $v_P(f)$ so that (2.21) holds:

for $k = 4$, we must have $v_\omega(f) = 1$, all other $v_P(f) = 0$;
for $k = 6$, we must have $v_i(f) = 1$, all other $v_P(f) = 0$;
for $k = 8$, we must have $v_\omega(f) = 2$, all other $v_P(f) = 0$;
for $k = 10$, we must have $v_\omega(f) = v_i(f) = 1$, all other $v_P(f) = 0$;
for $k = 14$, we must have $v_\omega(f) = 2$, $v_i(f) = 1$, all other $v_P(f) = 0$.

Let $f_1(z)$, $f_2(z)$ be nonzero elements of $M_k(\Gamma)$. Since $f_1(z)$ and $f_2(z)$ have the same zeros, the weight zero modular function $f_1(z)/f_2(z)$ is actually a modular form. By part (a), f_1 and f_2 are proportional. Choosing $f_2(z) = E_k(z)$ gives part (c).

(d) For $f \in S_k(\Gamma)$ we have $v_\infty(f) > 0$, and all other terms on the left in (2.21) are nonnegative. Notice that when $k = 12$ and $f = \Delta$, (2.21) implies that the only zero of $\Delta(z)$ is at infinity. Hence, for any k and any $f \in S_k(\Gamma)$, the modular function f/Δ is actually a modular form, i.e., $f/\Delta \in M_{k-12}(\Gamma)$. This gives us all of the assertions in part (d).

(e) Since E_k does not vanish at infinity, given $f \in M_k(\Gamma)$ we can always subtract a suitable multiple of E_k so that the resulting $f - cE_k \in M_k(\Gamma)$ vanishes at infinity, i.e., $f - cE_k \in S_k(\Gamma)$. □

We now prove that any modular form for Γ is a polynomial in E_4, E_6 (see Problem 5 of §I.6 for a different proof of this fact).

Proposition 10. *Any* $f \in M_k(\Gamma)$ *can be written in the form*

$$f(z) = \sum_{4i+6j=k} c_{i,j} E_4(z)^i E_6(z)^j. \tag{2.27}$$

PROOF. We use induction on k. For $k = 4, 6, 8, 10, 14$ we note that E_4, E_6, E_4^2, E_4E_6, $E_4^2E_6$, respectively, is an element of $M_k(\Gamma)$, and so, by Proposition 9(c), must span $M_k(\Gamma)$. Now suppose that $k = 12$ or $k > 14$. It is clearly possible to find i and j such that $4i + 6j = k$, in which case $E_4^iE_6^j \in M_k(\Gamma)$. Given $f \in M_k(\Gamma)$, by the same argument as in the proof of Proposition 9(e)

we can find $c \in \mathbb{C}$ such that $f - cE_4^iE_6^j \in S_k(\Gamma)$. By part (d) of Proposition 9, we can write f in the form

$$f = cE_4^iE_6^j + \Delta f_1 = cE_4^iE_6^j + \frac{(2\pi)^{12}}{1728}(E_4^3 - E_6^2)f_1,$$

where $f_1 \in M_{k-12}(\Gamma)$. Applying (2.27) to f_1 by the induction assumption we obtain the desired polynomial for f. □

Math 595 notes. 9/1/06. Proofs of two results stated in class

Proposition 7 (Prop 1.2.4 in DS). *Suppose that Γ is a congruence subgroup, and that f is holomorphic on $\mathbb{H}$ and weight k invariant under Γ. Suppose that the coefficients in the Fourier expansion*

$$f(z) = \sum_{n=0}^{\infty} a(n) q_N^n$$

satisfy $|a(n)| \ll n^r$ for some constant r. Then the function $f[\alpha]_k$ is holomorphic at ∞ for every $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ (in other words, all of the cusp conditions are satisfied).

Proof. Using the triangle inequality, with $z = x + iy$, we get that

$$|f(z)| \leq |a(0)| + \sum_{n=1}^{\infty} n^r e^{-2\pi y n/N} \ll 1 + \sum_{n=1}^{\infty} g(n),$$

where $g(t) := t^r e^{-2\pi y t/N}$. The function $g(t)$ has an absolute maximum at $t = rN/2\pi y$. Therefore the sum can be overestimated by the corresponding integral, along with the area of a rectangle of width 2 and height $g(t)$. The area of this rectangle is $2g(rN/2\pi y) \ll 1/y^r$, and the integral is

$$\int_0^{\infty} t^{r+1} e^{-2\pi y t/N} \frac{dt}{t} = \frac{1}{y^{r+1}} \int_0^{\infty} t^{r+1} e^{-2\pi t/N} \frac{dt}{t} \ll 1/y^{r+1}$$

since the last integral converges. Putting this together we find that

$$|f(z)| \ll 1 + 1/y^{r+1} \quad \text{for all } z \in \mathbb{H}. \tag{1}$$

Note: this is only interesting for values of y near zero; otherwise it just says that $f(z)$ is bounded for values of z away from the real axis, which we already know to be true since f is periodic and holomorphic at ∞. Therefore the term y^{r+1} dominates (note that if $y > 1$ then $1/y^r$ is less than 1, so it can be ignored anyway). Now take $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Since f is weight k invariant on a congruence subgroup, we have an expansion $f[\alpha]_k = \sum b(n) q_N^n$ for some coefficients $b(n)$. Therefore it will suffice to show that $q_N f[\alpha]_k(z) \to 0$ as $z \to \infty$. By periodicity we may suppose that $0 \leq x \leq N$. Therefore it will suffice to show the following:

$$f[\alpha]_k(z) \text{ has polynomial growth as } y \to \infty. \tag{2}$$

To show this first note that $y \ll |cz + d| \ll y$ for large y. We have $\mathrm{Im}(\alpha z) = \frac{y}{|cz+d|^2}$, so $1/y \ll |\mathrm{Im}(\alpha z)| \ll 1/y$ for large y.

Together with (1), this shows that

$$|f[\alpha]_k(z)| = \left|(cz+d)^{-k} f(\alpha z)\right| \ll y^{-k}(1 + y^{r+1}) \ll y^{r+1-k} \quad \text{as } y \to \infty. \tag{3}$$

This proves (2). ☐

Proposition 9. *Suppose that $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ and $\Lambda' = \mathbb{Z}\omega_1' \oplus \mathbb{Z}\omega_2'$ are lattices with $\omega_1/\omega_2, \omega_1'/\omega_2' \in \mathbb{H}$. Then $\Lambda = \Lambda'$ if and only if*

$$\gamma \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} \quad \textit{for some } \gamma \in \mathrm{SL}_2(\mathbb{Z}). \tag{4}$$

Proof. If (4) holds then since γ is invertible, the members of each pair can be written as integral linear combinations of the other pair, so the lattices are equal. If the lattices are equal, then reversing this argument shows that we have (4) for some invertible matrix with integer entries. Note that $\omega_1/\omega_2 = \frac{a(\omega_1'/\omega_2')+b}{c(\omega_1'/\omega_2')+d}$. The determinant must be equal to 1 (and not -1) since by hypothesis both quotients of the periods lie in $\mathbb{H}$, and in general a computation shows that $\mathrm{Im}(\gamma z) = \det(\gamma)\frac{\mathrm{Im}(z)}{|cz+d|^2}$. ☐

[17] A. WEIL. *Sur les courbes algébriques et les variétés qui s'en déduisent,* Act. Sci. Ind. **1041**, Hermann, Paris, 1948.

[18] A. WEIL. *Variétés abéliennes et courbes algébriques,* Act. Sci. Ind. **1064**, Hermann, Paris, 1948.

[19] A. WEIL. *Number of solutions of equations in finite fields,* Bull. Amer. Math. Soc., **55** (1949), p. 497–508.

[20] A. WEIL. *Abstract versus classical algebraic geometry,* Proc. Int. Congress Math. 1954, vol. III, p. 550–558, North-Holland Publ. Cy., Amsterdam, 1956.

[21] A. WEIL. *Footnote to a recent paper,* Amer. J. of Math., **76** (1954), p. 347–350.

100.

Divisibilité des coefficients des formes modulaires de poids entier

C. R. Acad. Sci. Paris **279** (1974), série A, 679–682

1 Ramanujan a conjecturé, et Watson a démontré (1), que $\tau(n) \equiv 0 \pmod{691}$ pour presque tout (2) entier n. Nous montrons que ce résultat reste valable si l'on remplace 691 par n'importe quel entier $m \geqq 1$ et $\tau(n)$ par le n-ième coefficient d'une forme modulaire de poids entier sur un sous-groupe de congruence de $\mathbf{SL}_2(\mathbf{Z})$. La démonstration utilise un argument analytique de Landau (3) et Wintner (4), appliqué aux fonctions L associées aux représentations l-adiques construites par Deligne (5).

1. ÉNONCÉ DU THÉORÈME. — Soit

$$f = \sum_{n=0}^{\infty} c_n e^{2\pi i n z/\mathrm{M}}, \qquad \mathrm{M} \geqq 1,$$

une forme modulaire de poids entier $k \geqq 1$ sur un sous-groupe de congruence de $\mathbf{SL}_2(\mathbf{Z})$. On suppose que les c_n appartiennent à l'anneau $\mathfrak{O}_\mathrm{K}$ des entiers d'un corps de nombres algébriques K fini sur $\mathbf{Q}$. Si m est un entier $\geqq 1$, on écrit $a \equiv 0 \pmod{m}$ si $a \in m\,\mathfrak{O}_\mathrm{K}$. On note $\mathrm{E}_{f,m}$ l'ensemble des entiers $n \in \mathrm{N}$ tels que $c_n \equiv 0 \pmod{m}$. Si E est une partie de N, et si $x \geqq 1$, on note $\mathrm{E}(x)$ le nombre des $n \in \mathrm{E}$ tels que $n \leqq x$.

THÉORÈME 1. — *Soient f et m comme ci-dessus. Il existe $\alpha > 0$ tel que*

$$x - \mathrm{E}_{f,m}(x) = O(x/\log^\alpha x) \qquad \textit{pour} \quad x \to \infty.$$

En particulier, on a $\mathrm{E}_{f,m}(x) \sim x$: l'ensemble $\mathrm{E}_{f,m}$ est de densité 1. Autrement dit :

COROLLAIRE. — *On a $c_n \equiv 0 \pmod{m}$ pour presque tout n.*

Exemples. — On peut prendre pour c_n :

(i) le n-ième coefficient $\sigma_{k-1}(n)$ de la série d'Eisenstein de poids k du groupe $\mathbf{SL}_2(\mathbf{Z})$; c'est essentiellement le cas traité dans (1);

(ii) le n-ième coefficient $\tau(n)$ de

$$\Delta = e^{2\pi i z} \prod_{m=1}^{\infty} (1 - e^{2\pi i m z})^{24}$$

(*cf.* n° 4, th. 3);

(iii) le nombre de représentations de n par une forme quadratique positive non dégénérée, à coefficients entiers, en un nombre pair de variables.

2. UN RÉSULTAT AUXILIAIRE. — Soit M une extension galoisienne finie de $\mathbf{Q}$, de groupe de Galois G, non ramifiée en dehors d'un entier D. Soit H une partie de G, stable par conjugaison. Soit P l'ensemble des nombres premiers, et soit P(H) l'ensemble des $p \in \mathrm{P}$ qui ne

divisent pas D et qui sont tels que la classe de conjugaison de la substitution de Frobenius $F_p \in G$ appartienne à H. On sait que P(H) a une densité dans P égale à h/g, où $h = \text{Card}(H)$, $g = \text{Card}(G)$. Notons E_H l'ensemble des entiers $n \geqq 1$ tels qu'il existe $p \in P(H)$ avec $n \equiv 0 \pmod{p}$ et $n \not\equiv 0 \pmod{p^2}$.

THÉORÈME 2. — *On suppose* $H \neq G$. *Il existe alors une constante* $C > 0$ *telle que*

$$x - E_H(x) \sim C\,x/\log^\alpha x, \qquad \text{où} \quad \alpha = h/g.$$

(En particulier, E_H a pour densité 1 si $H \neq \varnothing$, résultat facile à prouver directement en utilisant le fait que $\sum_{p \in P(H)} 1/p = +\infty$.)

Démonstration. — Le cas $H = \varnothing$ est trivial (on prend $C = 1$). Supposons donc $H \neq \varnothing$. Considérons la série de Dirichlet suivante, qui converge pour $\mathscr{R}(s) > 1$:

$$f(s) = \prod_{p \in P(H)} (1+p^{-2s}+p^{-3s}+\ldots) \prod_{p \notin P(H)} (1+p^{-s}+p^{-2s}+\ldots)$$
$$= \sum_{n \notin E_H} n^{-s}.$$

Si l'on écrit cette série sous la forme $\sum_{n=1}^{\infty} b_n n^{-s}$, tout revient à prouver que

$$\sum_{n \leqq x} b_n \sim Cx/\log^\alpha x.$$

Pour cela, d'après (⁴), il suffit de montrer que $f(s)$ est de la forme $c(s)/(s-1)^{1-\alpha}$, où $c(s)$ est holomorphe dans le demi-plan $\mathscr{R}(s) \geqq 1$ et non nulle en $s = 1$.

On va comparer $f(s)$ à un produit de puissances des séries $L(s, \chi)$ d'Artin attachées aux différents caractères irréductibles χ du groupe G. Si φ désigne la fonction caractéristique de $G - H$, on a

$$\varphi = \sum_\chi u_\chi \chi, \qquad \text{où} \quad u_\chi = \frac{1}{g} \sum_{s \notin H} \bar{\chi}(s).$$

On a

$$\log L(s, \chi) \equiv \sum_p \chi(F_p)\,p^{-s} \pmod{\mathscr{F}_{1/2}},$$

où $\mathscr{F}_{1/2}$ désigne l'ensemble des fonctions holomorphes dans le demi-plan $\mathscr{R}(s) > 1/2$. Si l'on pose

$$g(s) = \sum_\chi u_\chi \log L(s, \chi),$$

on a donc

$$g(s) \equiv \sum_p \varphi(F_p)\,p^{-s} \equiv \sum_{p \notin P(H)} p^{-s} \pmod{\mathscr{F}_{1/2}},$$

d'où aussitôt

$$g(s) \equiv \log f(s) \pmod{\mathscr{F}_{1/2}}.$$

On en conclut que $f(s) = e^{g(s)}\,h(s)$, où $h(s)$ est holomorphe et $\neq 0$ pour $\mathscr{R}(s) > 1/2$ et en particulier pour $\mathscr{R}(s) \geqq 1$. D'autre part, la fonction $e^{g(s)}$ est une détermination de la fonction $\prod L(s, \chi)^{u_\chi}$; vu les propriétés connues des fonctions L, elle se prolonge en une fonction holomorphe non nulle en tout point $\neq 1$ de la droite $\mathscr{R}(s) = 1$. Au point 1, chacune des $L(s, \chi)$, $\chi \neq 1$, est holomorphe non nulle, et $L(s, 1) = \zeta(s)$ a un pôle simple; comme l'exposant u_1 de $L(s, 1)$ dans $e^{g(s)}$ est $1-(h/g) = 1-\alpha$, on en déduit bien que $f(s)$ est de la forme $c(s)/(s-1)^{1-\alpha}$, où $c(s)$ est holomorphe pour $\mathscr{R}(s) \geqq 1$ et $c(1) \neq 0$.

Remarques. — 1° Au lieu d'utiliser le théorème taubérien de Wintner (⁴), il est probable que l'on peut appliquer la méthode de Landau (³); c'est ce qu'a fait Watson (¹) dans le cas où M est *abélien* sur Q, i. e. où P(H) peut être défini par des *congruences*.

2° On peut généraliser le théorème 2 de la manière suivante : donnons-nous, pour tout $p \in P$, un ensemble A_p d'entiers $\geqq 0$, tel que $0 \in A_p$ pour tout p, et que $1 \in A_p$ si et seulement si $p \notin H$. Soit $S_{A,H}$ l'ensemble des entiers $n = \prod p^{a(p)}$ tels que $a(p) \in A_p$ pour tout p. *On a alors, si* $H \neq G$,

$$S_{A,H}(x) \sim C_1\,x/\log^\alpha x, \qquad \textit{avec} \quad C_1 \neq 0.$$

La démonstration est la même : on remplace simplement $f(s)$ par la somme des n^{-s} pour $n \in S_{A,H}$.

3. DÉMONSTRATION DU THÉORÈME 1. — On se ramène par des réductions standard [*cf.* (⁵)], au cas où f est une forme modulaire de type (k, ε) sur un groupe $\Gamma_0(N)$, et où f est fonction propre des opérateurs de Hecke T_p, $p \nmid N$, avec pour valeurs propres $a_p \in \mathfrak{O}_K$.

LEMME. — *Il existe une extension galoisienne finie* M *de* **Q**, *non ramifiée en dehors de* Nm, *et une partie* H *de* $G = \text{Gal}(M/\mathbf{Q})$, *stable par conjugaison, distincte de* $\varnothing$ *et de* G, *telle que, avec les notations du n° 2, on ait* $a_p \equiv 0 \pmod{m}$ *pour tout* $p \in P(H)$.

En effet, d'après Deligne (⁵), on peut trouver une extension M comme ci-dessus, et un plongement $\rho : G \to \mathbf{GL}_2(\mathfrak{O}_K/m\,\mathfrak{O}_K)$ tel que, pour tout $p \nmid Nm$, on ait

$$\text{Tr}(\rho(F_p)) \equiv a_p \pmod{m}.$$

On prend alors pour H le sous-ensemble de G formé des éléments s tels que $\text{Tr}(s) = 0$. On a $H \neq \varnothing$, car H contient l'image $\rho(c)$ de la conjugaison complexe c; on a $H \neq G$ si $m \geqq 3$ (ce qu'il est loisible de supposer, quitte à remplacer m par un multiple). Toutes les conditions du lemme sont bien satisfaites.

Le théorème 1 est maintenant immédiat. En effet, si n est divisible par p et pas par p^2, le fait que $f\,|\,T_p = a_p f$ entraîne

$$c_n = a_p\,c_{n/p},$$

d'où $c_n \equiv 0 \pmod{m}$ si $p \in P(H)$. Avec les notations du n° 2, on a donc $c_n \equiv 0 \pmod{m}$ pour tout $n \in E_H$, et on conclut en appliquant le théorème 2.

4. EXEMPLE : LA FONCTION τ DE RAMANUJAN. — Dans le cas où m est *premier*, on peut améliorer le théorème 1 :

THÉORÈME 3. — *Si* l *est premier, et* $x \geqq 1$, *notons* $S_l(x)$ *le nombre des entiers* $n \leqq x$ *tels que* $\tau(n) \not\equiv 0 \pmod{l}$. *On a*

$$S_2(x) \sim \frac{1}{2} x^{1/2} \qquad \textit{et} \qquad S_l(x) \sim c_l\,x/\log^{\alpha(l)} x \quad \textit{si} \ \ l \geqq 3,$$

avec $c_l > 0$ *et*

$$\alpha(l) = \begin{cases} l/(l^2-1) & si \quad l \neq 3,\ 5,\ 7,\ 23,\ 691; \\ \frac{1}{2},\ \frac{1}{4},\ \frac{1}{2},\ \frac{1}{2},\ \frac{1}{690} & si \quad l = 3,\ 5,\ 7,\ 23,\ 691. \end{cases}$$

Cela se déduit facilement de la remarque 2 du n° 2 [appliquée en prenant pour A_p l'ensemble des $r \geqq 0$ tels que $\tau(p^r) \not\equiv 0 \pmod{l}$], combinée avec les déterminations de groupes de Galois faites dans (⁶).

5. Généralisations. — On a des résultats analogues pour les coefficients des séries de Dirichlet attachées aux systèmes compatibles de représentations l-adiques rationnelles (⁷), pourvu que, dans chacune de ces représentations l'image de la conjugaison complexe c soit de trace 0. C'est notamment le cas pour les systèmes provenant de la cohomologie *de degré impair* d'une variété projective lisse.

(*) Séance du 12 août 1974.

(¹) *Cf.* G. N. Watson, *Math. Z.*, 39, 1935, p. 712-731, ainsi que G. H. Hardy, *Ramanujan*, Cambridge University Press, 1940, § 10.6.

(²) On dit qu'une relation a lieu *pour presque tout n* si l'ensemble des *n* qui y satisfont est de densité 1.

(³) E. Landau, *Arch. der Math. Phys.*, 13, 1908, p. 305-312.

(⁴) A. Wintner, *Amer. J. Math.*, 64, 1942, p. 320-326. (H. Stark m'a signalé que la démonstration de Wintner est insuffisante : le passage de la formule (18) à la formule (19) n'est pas justifié; des hypothèses un peu plus fortes sont nécessaires; ces hypothèses sont vérifiées dans le cas envisagé ici.)

(⁵) *Voir* P. Deligne, *Formes modulaires et représentations l-adiques*, [*Séminaire Bourbaki*, 1968-1969, exposé 355, *Lecture Notes*, 179, Springer, 1971] ainsi que le paragraphe 6 de P. Deligne et J-P. Serre, *Ann. Sci. Éc. Norm. Sup.*, 4ᵉ série, 7, 1974 (à paraître).

(⁶) H. P. F. Swinnerton-Dyer, *Lecture Notes*, 350, Springer, 1973, p. 1-55.

(⁷) *Cf.* J-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968, chap. I.

Collège de France,
75231 *Paris-Cedex* 05.

101.

(avec P. Deligne)

Formes modulaires de poids 1

Ann. Sci. Ec. Norm. Sup. 7 (1974), 507–530

A Henri Cartan,
à l'occasion de son
70ᵉ anniversaire

Introduction

La décomposition en produit eulérien, et l'équation fonctionnelle, des séries de Dirichlet associées par Hecke aux *formes modulaires de poids* 1 suggèrent que celles-ci correspondent à des *fonctions* L *d'Artin de degré* 2 *du corps* **Q**, autrement dit à des *repré-
sentations de* Gal $(\overline{\mathbf{Q}}/\mathbf{Q})$ *dans* $\mathbf{GL}_2(\mathbf{C})$. C'est une telle correspondance, conjecturée par
1 Langlands, que nous établissons ici.

Les trois premiers paragraphes sont préliminaires. Le paragraphe 4 contient l'énoncé du théorème principal, et quelques compléments. La démonstration occupe les paragraphes 5 à 9. Son principe est le suivant : on commence par construire, pour tout nombre premier l, une représentation de Gal $(\overline{\mathbf{Q}}/\mathbf{Q})$ en caractéristique l (*cf.* § 6); on montre ensuite que les images de Gal $(\overline{\mathbf{Q}}/\mathbf{Q})$ dans ces diverses représentations sont « petites », ce qui permet de les relever en caractéristique 0, et d'obtenir la représentation complexe cherchée (§§ 7 et 8); la « petitesse » en question résulte elle-même d'une majoration en moyenne des valeurs propres des opérateurs de Hecke (Rankin, *cf.* § 5). Le paragraphe 9 contient une estimation des coefficients des formes modulaires de poids 1.

Signalons que nous avons utilisé en un point essentiel (§ 6, th. 6.1) des résultats démon-
2 trés par l'un de nous (P. Deligne), mais dont aucune démonstration complète n'a encore
été publiée; en attendant une telle publication (ainsi que celle de SGA 5, dont ils dépen-
dent), nous demandons au lecteur de bien vouloir les admettre.

§ 1. Rappels (analytiques) sur les formes modulaires

1.1. Soit N un entier $\geqq 1$. On associe à N les sous-groupes

$$\Gamma(\mathrm{N}) \subset \Gamma_1(\mathrm{N}) \subset \Gamma_0(\mathrm{N})$$