Lecture 1. Introduction

Central area of research in modern number theory: Langlands programme

relation arithmetic objects $\longleftrightarrow$ 'analytic' objects
Galois representations ... automorphic forms/representations.

Ex. elliptic curves $\longleftrightarrow$ modular forms

$$E:\ y^2 + y = x^3 - x \longleftrightarrow f(z) = q\prod_{n\geq 1}(1-q^n)^2(1-q^{11n})^2 = \sum_{n=1}^{\infty} a_n q^n \qquad q = e^{2\pi i z}$$

$p \neq 11$ prime: $\# E(\mathbb{F}_p) = 1 + p - a_p$. (modular form)

Function $\eta(z) = q^{1/24}\prod_{n\geq 1}(1-q^n)$ studied first by Dedekind

$\eta(z+1) = e^{\pi i/12}\eta(z)$; $\eta(-1/z) = \left(\frac{z}{i}\right)^{1/2}\eta(z)$ one of simplest exs. of modular form

Relation between E & f can also be expressed using the L-series

$$L(E,s) = \sum_{n=1}^{\infty}\frac{a_n}{n^s}$$

– generalising Riemann ζ-fn: $\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$.

Course will study modular forms & L-functions ; obvious links with elliptic curve course.

To study Langlands programme properly, need to work with language of adeles : won't do this (except at very end).

Some tools we will use :–

§1. Characters (Fourier analysis).

(Won't be using any subtle analysis – this will be just function theory.)

G an abelian topological group.

A (unitary) character of G is a continuous homomorphism $\chi: G \to U(1) = \{z\in\mathbb{C} \mid |z|=1\}$

Set of all characters is an abelian group under multiplication, $\hat{G} \underset{def}{=} \mathrm{Hom}_{cts}(G, U(1))$.

Exs. $G = \mathbb{R}$; for $y\in\mathbb{R}$ let $\chi_y:\mathbb{R}\to U(1)$ be $\chi_y(x) = e^{2\pi i x y}$

Fact: $\hat{G} = \{\chi_y \mid y\in\mathbb{R}\} \simeq \mathbb{R}$. (example sheet)

$G = \mathbb{Z}$ (discrete topology) : obviously $\hat{G} \simeq U(1)$
$\chi \longmapsto \chi(1)$

$G = \mathbb{Z}/n\mathbb{Z}$ (..) : $\hat{G} \simeq \mu_n = \{\zeta \mid \zeta^n = 1\} \subset U(1)$
$\chi \longmapsto \chi(1)$

$G = G_1 \times G_1 \Rightarrow \hat{G} \simeq \hat{G}_1 \times \hat{G}_2$ eg. $G = \mathbb{R}^n$; $\hat{G} = \{\chi_y : x\mapsto e^{2\pi i(x\cdot y)} \mid y\in\mathbb{R}^n\}$

$G = \mathbb{R}^\times = \{\pm 1\}\times\mathbb{R}^\times_{>0}$: $\hat{G} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}$
$(x\mapsto \mathrm{sgn}(x)^\varepsilon . |x|^{i\sigma}) \longleftarrow (\varepsilon, \sigma)$

[Remark. $\hat{G}$ has a natural topology, for which the maps $\chi \mapsto \chi(g)$ $(g \in G)$ are continuous. This determines a homomorphism $G \to \hat{\hat{G}}$ which is an isomorphism if G is locally compact.] (1-2)

Proposition Let G be a finite abelian group. Then $\#\hat{G} = \#G$ and $G, \hat{G}$ are isomorphic (non-canonically).

Proof Since $G \simeq \prod_{i=1}^{k} \mathbb{Z}/n_i\mathbb{Z}$ is a product of cyclic groups,
$\hat{G} \simeq \prod_{i=1}^{k} \mu_{n_i}$ and $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$ □

Fourier transform. $f : \mathbb{R} \to \mathbb{C}$ an L^1-function (ie. $\int |f(x)|dx < \infty$)

$$\hat{f}(y) = \int_{-\infty}^{\infty} e^{-2\pi i x y} f(x)\,dx = \int \chi_y(x)^{-1} f(x)\,dx,$$ bounded cts. fn. on $\mathbb{R} = \hat{\mathbb{R}}$.

Only interested in $f \in \mathcal{S}(\mathbb{R}) = \{ f \in C^\infty(\mathbb{R}) \mid \forall k, n \ |x^n f^{(k)}(x)| \to 0 \text{ as } |x| \to \infty \}$ "Schwarz space"

– in which case $\hat{f} \in \mathcal{S}(\mathbb{R})$ as well, and have:

Fourier inversion formula: $\hat{\hat{f}}(x) = f(-x)$ for $f \in \mathcal{S}(\mathbb{R})$

Same for $\mathbb{R}^n$.

For $G = \mathbb{R}/\mathbb{Z}$, FT is Fourier series: $\chi_n(x) = e^{2\pi i n x}$

f a fn. on $\mathbb{R}/\mathbb{Z}$, $c_n(f) = \int_{\mathbb{R}/\mathbb{Z}} \chi_n(x)^{-1} f(x)\,dx = \int_0^1 e^{-2\pi i n x} f(x)\,dx$

Fourier inversion says (for suitable f eg. $f \in C^\infty(\mathbb{R}/\mathbb{Z})$) $f(x) = \sum_{n \in \mathbb{Z}} c_n(f) \cdot \chi_n(x)$

$G = \mathbb{Z}/N\mathbb{Z}$. $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$

$\hat{f} : \mu_N \to \mathbb{C}$, $\hat{f}(\zeta) = \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \zeta^{-a} f(a)$.

Prop: $f(x) = \frac{1}{N} \sum_{\zeta \in \mu_N} \zeta^x \hat{f}(\zeta)$. (proof next time)

[General picture:- G loc. compact abelian gp, μ Haar measure = translation-invariant measure on G.

$f \in L^1(G, \mu)$ $\hat{f}(\chi) = \int_G \chi(g)^{-1} f(g)\,d\mu(g)$ $\chi \in \hat{G}$

$\hat{\hat{f}}(x) = c f(-x)$ for c indep. of f.

- G discrete: $\mu(\{x\}) = 1$
- $G = \mathbb{R}^n, \mathbb{R}/\mathbb{Z}$ Lebesgue measure dx
- $G = \mathbb{R}^\times$; dx/x]

(end of lecture 1)

Recall: $G = \mathbb{Z}/N\mathbb{Z}$. $f : \mathbb{Z}/N\mathbb{Z} \to \mathbb{C}$

$$\hat{f} : \mu_N \to \mathbb{C}, \quad \hat{f}(\zeta) = \sum_{a \in \mathbb{Z}/N\mathbb{Z}} \zeta^{-a} f(a).$$

Prop: $$f(x) = \frac{1}{N} \sum_{\zeta \in \mu_N} \zeta^x \hat{f}(\zeta).$$

Proof. Both sides linear in $f = \sum_{a \in \mathbb{Z}/N\mathbb{Z}} f(a) . \delta_a$ $\quad \delta_a(x) = \begin{cases} 1 & x = a \\ 0 & x \neq a \end{cases}$

So enough to consider $f = \delta_a$. Then

$\hat{f}(\zeta) = \zeta^{-a}$, so RHS $= \frac{1}{N} \sum_{\zeta} \zeta^{x-a}$. Reduces to:–

Lemma $k \in \mathbb{Z}$. Then $$\sum_{\zeta \in \mu_N} \zeta^k = \begin{cases} 0 & \text{if } k \not\equiv 0 \ (N) \\ N & \text{if } k \equiv 0 \ (N) \end{cases}$$

(Pf. Let $\eta = e^{2\pi i/N}$. Then $\sum_{\zeta} \zeta^k = \sum_{\zeta} (\eta\zeta)^k = \eta^k \sum \zeta^k$, so $k \not\equiv 0 \Rightarrow \eta^k \neq 1$
omitted $\Rightarrow \sum \zeta^k = 0$. $\square$)

Poisson summation formula on $\mathbb{R}^n$: let $f \in \mathcal{S}(\mathbb{R}^n)$. Then

$$\sum_{a \in \mathbb{Z}^n} f(a) = \sum_{b \in \mathbb{Z}^n} \hat{f}(b).$$

Proof Let $g(x) = \sum_{a \in \mathbb{Z}^n} f(x+b). \in C^\infty(\mathbb{R}^n/\mathbb{Z}^n)$ (since $f \in \mathcal{S}(\mathbb{R}^n)$)

Then $g(x) = \sum_{b \in \mathbb{Z}} c_b(g) e^{2\pi i b.x}$ Fourier series,

$$c_b(g) = \int_{(\mathbb{R}/\mathbb{Z})^n} e^{-2\pi i b.x} g(x)\, dx = \sum_{a \in \mathbb{Z}^n} \int_{[0,1]^n} e^{-2\pi i b.x} f(x+a)\, dx = \int_{\mathbb{R}^n} e^{-2\pi i b.x} f(x) = \hat{f}$$

So $$\sum_{a \in \mathbb{Z}^n} f(a) = g(0) = \sum_{b \in \mathbb{Z}^n} c_b(g) = \sum_{b \in \mathbb{Z}^n} \hat{f}(b). \quad \square$$

§2 Mellin transform and Γ-function. (2-2)

$f : \mathbb{R}_{>0} \xrightarrow{\text{cts}} \mathbb{C}$, rapidly decreasing at ∞ ie. $y^n f(y) \to 0$ as $y \to \infty$ $\forall n$

moderate growth at 0 ie. $\exists m$ st. $|y^m f(y)|$ bounded as $y \to 0$.

$$M(f, s) = \int_0^\infty y^s f(y) \frac{dy}{y} \quad \text{converges to analytic fn. } \{\mathrm{Re}(s) > m\}.$$

Proof: $\int_r^R y^s f(y) \frac{dy}{y}$ is entire fn. of s & $\begin{cases} \int_R^\infty \to 0 \text{ as } R \to \infty & \text{unif. on compact subsets of } \mathbb{C} \text{ (b)} \\ \int_0^r \to 0 \text{ as } r \to 0 & \ldots\ldots \{\mathrm{Re}(s) > m\} \end{cases}$

Rem. Suppose $\int_0^\infty |f| \frac{dy}{y} < \infty$. Then integral converges on $\{s = i\sigma \in i\mathbb{R}\}$, and it equals the Fourier transform of $f \in L^1(\mathbb{R}^\times_{>0})$, $\hat{G} = \{y \mapsto y^{i\sigma}\}$ $= G$

– We are usually interested in f for which this $\int$ is unbounded.

Change of variables $\Rightarrow$ $\boxed{M(f(\alpha y), s) = \alpha^{-s} M(f, s) \quad \forall \alpha > 0}$

Ex $f(y) = e^{-y}$. $(m = 0)$ $\quad M(f, s) = \int_0^\infty e^{-y} y^s \frac{dy}{y} = \Gamma(s)$, Gamma function.

– analytic for $\mathrm{Re}(s) > 0$

Integration by parts $\Rightarrow$ $\Gamma(s+1) = s\Gamma(s)$, $\Gamma(1) = 1$, $\Gamma(n) = (n-1)!$ $\forall n \in \mathbb{Z}_{>0}$.

Therefore $\Gamma(s) = \frac{1}{s(s+1)\ldots(s+N-1)} \Gamma(s+N)$ $(N \geq 1)$, defining a meromorphic continuation to $\{\mathrm{Re}(s) > -N\}$ with simple pole at $s = 1-N$, residue $= \frac{(-1)^{N-1}}{(N-1)!}$

Other properties (see any good book on complex analysis – eg. Ahlfors Ch.2 §4)

① $\Gamma(s)^{-1} = e^{\gamma s} s \prod_{n=1}^\infty (1 - \frac{s}{n}) e^{s/n}$: in particular, $\Gamma(s) \neq 0$ $\forall s$

Here $\gamma = \lim_{n \to \infty} (1 + \frac{1}{2} + \ldots + \frac{1}{n} - \log n)$ (Euler-Mascheroni constant)

② Duplication & reflection formula:– $\pi^{1/2} \Gamma(2s) = 2^{2s-1} \Gamma(s) \Gamma(s + 1/2)$

$$\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi z}$$

Mellin transform converts power series into Dirichlet series:

let $f(z) = \sum_{n=1}^\infty a_n e^{2\pi i n z}$, $|a_n| < c.n^K$; $f(iy) = \sum a_n e^{-2\pi n y}$

Then if $\mathrm{Re}(s) > \max(0, K+1)$ (so that series is abs. cgt)

$$(2\pi)^{-s}\Gamma(s) \sum_{n=1}^\infty \frac{a_n}{n^s} = \sum_n a_n (2\pi n)^{-s} M(e^{-y}, s) = \sum_n a_n M(e^{-2\pi n y}, s)$$

$$= M(f(iy), s)$$

§3. Riemann ζ-function.

2-3

- is the function $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$, $\mathrm{Re}\, s > 1$ - abs. cvgt. + represents analytic function.

The Euler product. $\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1-p^{-s}}$ for $\mathrm{Re}(s) > 1$.

Proof: 1) formally: $\text{RHS} = \prod_p \left(1 + p^{-s} + (p^2)^{-s} + (p^3)^{-s} + \cdots\right) = \sum_{n \geq 1} n^{-s}$

by unique factorisation in $\mathbb{Z}$.

2) analytically. Infinite product converges $\Leftarrow \sum p^{-s}$ converges, which is certainly true for $\mathrm{Re}(s) > 1$.

Consider $\zeta(s) - \prod_{p \leq X} \frac{1}{1-p^{-s}} = \zeta(s) - \prod_{p \leq X} (1 + p^{-s} + p^{-2s} + \cdots)$

$$= \sum_{n \in \mathcal{N}_X} \frac{1}{n^s} \qquad \mathcal{N}_X = \{n \geq 1 \mid \text{at least one prime factor of } n \text{ is} \geq X\}.$$

$$\therefore \left| \zeta(s) - \prod_{p \leq X} \frac{1}{1-p^{-s}} \right| \leq \sum_{n \in \mathcal{N}_X} \frac{1}{|n^s|} = \sum_{n \geq X} \frac{1}{n^{\mathrm{Re}(s)}} \to 0 \text{ as } X \to \infty \text{ if } \mathrm{Re}(s) > 1.$$

$\square$

(End of lecture 2)

 Aim to show: $\zeta(s)$ has a meromorphic ctn. to $\mathbb{C}$. 3-1

Prove twice - get different information.

1st integral representation for $\zeta(s)$

Thm: If $Re(s)>1$ then

$$(2\pi)^{-s}\Gamma(s)\zeta(s) = \int_0^\infty \frac{y^s}{e^{2\pi y}-1}\frac{dy}{y}$$

$$= M(f(y), s), \quad f(y) = \frac{1}{e^{2\pi y}-1}.$$

Proof. $f(y) = e^{-2\pi y}/1-e^{-2\pi y} = \sum_{n\geq 1} e^{-2\pi n y}$ if $y>0$.

and $f(y) \sim \frac{1}{2\pi y}$ as $y \to 0$

$\therefore$ Mellin transform converges for $Re(s)>1$ and equals

$$\sum_{n\geq 1} M(e^{-2\pi n y}, s) = \sum_{n\geq 1} (2\pi n)^{-s} M(e^{-y}, s) = (2\pi)^{-s}\Gamma(s)\zeta(s). \qquad \square.$$

Corollary 1: $\zeta(s)$ has a meromorphic ctn. to $\mathbb{C}$ with a simple pole at $s=1$ as only singularity, res $=1$.

Proof $M(f,s) = M_0 + M_\infty$, $M_0 = \int_0^1 f(y)y^s\frac{dy}{y}$, $M_\infty = \int_1^\infty$.

Now $\int_1^\infty \frac{1}{e^{2\pi y}-1} y^s \frac{dy}{y}$ is entire fn. of s ;. as $f(y)$ has a pole at $y=0$

can write ($N>0$) $$f(y) = \sum_{n=-1}^{N-1} c_n y^n + y^N g_N(y), \quad g_N \in C^\infty(\mathbb{R}).$$

$$\Rightarrow M_0 = \underbrace{\sum_{n=-1}^{N-1} c_n \int_0^1 y^{s+n-1}\,dy}_{=\sum_{n=-1}^{N-1} c_n/(s+n)} + \underbrace{\int_0^1 g_N(y) y^{s+N-1}\,dy}_{\text{holomorphic for } Re(s)>-N}$$

So $(2\pi)^{-s}\Gamma(s)\zeta(s)$ can be meromorphically continued to $\{Re(s)>-N\}$ with at worst simple poles at $s=1-N, 2-N, \dots, 0, 1$, residue c_n. (any $N>0$)

Now $\Gamma(s)$ has a simple pole at $s=0,-1,\dots$, $\mathrm{res}_{s=1-n}\Gamma(s) = \frac{(-1)^{n-1}}{(n-1)!}$

$\therefore \zeta(s)$ has only a simple pole at $s=1$;

since $f(s) \sim \frac{1}{2\pi s}$ at $s=0$, $c_{-1} = \frac{1}{2\pi}$ hence $\mathrm{Res}_{s=1}\zeta(s) = \Gamma(1)^{-1} = 1$.

Bernoulli numbers B_n $(n \geq 0)$ defined by their generating series:

$$\sum_{n\geq 0} B_n \frac{t^n}{n!} = \frac{t}{e^t-1} = \left(1+\frac{t}{2!}+\frac{t^2}{3!}+\dots\right)^{-1}.$$

Obviously $B_n \in \mathbb{Q}$, $B_0 = 1$, $B_1 = -1/2$.

Prop^n $B_n = 0$ if $n \geq 3$, n odd

Proof Let $f(t) = \frac{t}{e^t-1} + \frac{t}{2} = \sum_{\substack{n\geq 0\\ n\neq 1}} B_n \frac{t^n}{n!}$

$$= \frac{t}{2}\cdot\frac{e^t+1}{e^t-1} = f(-t) \qquad \square.$$

Coroll 2. $\zeta(0) = B_1 = -1/2$ and $\forall n \geq 1$, $\zeta(1-n) = -\frac{B_n}{n}$;

in particular, $\zeta(1-n) \in \mathbb{Q}$ and $= 0$ if n odd >1.

Proof $(2\pi)^{-s}\Gamma(s)\zeta(s)$ has simple pole at $s = 1-n$, residue $= c_{n-1}$ where $\frac{1}{e^{2\pi y}-1} = \sum_{n\geq -1} c_n y^n$

$$\therefore\ c_{n-1} = (2\pi)^{n-1}\frac{B_n}{n!}$$

As $\mathrm{Res}_{s=1-n}\Gamma(s) = \frac{(-1)^{n-1}}{(n-1)!}$, $\zeta(1-n) = (-1)^{n-1}\frac{B_n}{n} = \begin{cases} -1/2 & n=1 \\ 0 & n \text{ odd} >1 \\ -\frac{B_n}{n} & n \text{ even} \end{cases}$ $\square$

[Remark. behaviour of L-fns. at integers has deep arithmetical significance (largely conjectural). Eg. the fact that $\zeta(1-n) = -\frac{B_n}{n}$ is related to Kummer criterion:

$$p \mid \text{class number of } \mathbb{Q}(\sqrt[p]{1}) \iff p \text{ divides } \prod$$

2nd integral representation. Let $\Theta(y) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 y} = 1 + 2\sum_{n=1}^{\infty} e^{-\pi n^2 y}$ $(y>0)$

So $\Theta(y) = \vartheta(iy)$, where $\vartheta(z) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z}$ – analytic for $\mathrm{Im}\, z > 0$.

$\Theta(y) \to 1$ as $y \to \infty$ so can't take its Mellin transform. But

Prop^n $M\left(\frac{\Theta(y)-1}{2}, \frac{s}{2}\right) = \pi^{-s/2}\Gamma(s/2)\zeta(s)$ $(\mathrm{Re}\, s > 1)$.

Proof. $\mathrm{LHS} = \sum_{n\geq 1} M\left(e^{-\pi n^2 y}, \frac{s}{2}\right) = \sum_{n\geq 1}(\pi n^2 y)^{-s/2} M\left(e^{-\pi y}, s/2\right)$

$$= \pi^{-s/2}\Gamma(s/2)\zeta(s). \qquad \square$$

4-1

Notation $\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2)$

$\Gamma_{\mathbb{C}}(s) = 2(2\pi)^{-s}\Gamma(s)$.

Functional equation of theta function.

Thm. Let $\mathrm{Im}(z)>0$. Then $\vartheta(-\frac{1}{z}) = \left(\frac{z}{i}\right)^{1/2}\vartheta(z)$

(where we take branch of $(z/i)^{1/2}$ which is >0 for $z=iy$, $y>0$)

So $\Theta(1/y) = y^{1/2}\,\Theta(y)$.

Proof By analytic continuation, enough to prove for $z=it$ ie. for $\Theta(it)$

Let $g_t(x) = e^{-\pi t x^2} = g_1(t^{1/2}x)$. We know $\hat{g}_1 = g_1$.

Lemma Fourier transform of $f(\alpha x)$ is $\alpha^{-1}\hat{f}(y/\alpha)$. □

So $\widehat{g_t}(y) = t^{-1/2}\hat{g}_1\left(\frac{y}{t^{1/2}}\right) = t^{-\frac{1}{2}}e^{-\pi y^2/t}$. By Poisson summation,

$$\Theta(t) = \sum_{n\in\mathbb{Z}} e^{-\pi n^2 t} = \sum_{n\in\mathbb{Z}} g_t(n) = \sum_{n\in\mathbb{Z}} \hat{g}_t(n) = \sum_{n\in\mathbb{Z}} t^{-1/2} e^{-\pi n^2/t} = t^{-\frac{1}{2}}\Theta\left(\frac{1}{t}\right)$$

□

Thm (Functional equation for ζ). Let $Z(s) = \Gamma_{\mathbb{R}}(s)\zeta(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$.

Then $Z(s)$ has a meromorphic ctn. to $\mathbb{C}$, only singularities simple poles at $s=1,0$, residues $1,-1$ resp, and

$$Z(1-s) = Z(s).$$

Proof For $\mathrm{Re}(s)>1$, $2Z(s) = M\left(\Theta(y)-1, \frac{s}{2}\right)$

$$= \int_0^\infty [\Theta(y)-1]\, y^{s/2}\frac{dy}{y}$$

$$\int_0^1 [\Theta(y)-1]y^{s/2}\frac{dy}{y} = \int_0^1 [\Theta(y)-y^{-1/2}]y^{s/2}\frac{dy}{y} + \int_0^1 y^{\frac{s-1}{2}} - y^{\frac{s}{2}}\frac{dy}{y}$$

$$= \int_0^1 \left[y^{-1/2}\Theta(\tfrac{1}{y}) - y^{-1/2}\right]y^{\frac{s}{2}}\frac{dy}{y} + \left[\frac{y^{\frac{s-1}{2}}}{(s-1)/2} - \frac{y^{s/2}}{s/2}\right]_0^1$$

$$= \int_1^\infty [\Theta(y)-1]\,y^{\frac{1-s}{2}}\frac{dy}{y} + \frac{2}{s-1} - \frac{2}{s}$$

$$\therefore\ 2Z(s) = \int_1^\infty [\Theta(y)-1]\left(y^{s/2} + y^{(1-s)/2}\right)\frac{dy}{y} + \frac{2}{s-1} - \frac{2}{s}$$

and integral is analytic $\forall s\in\mathbb{C}$ $\Rightarrow$ mero. ctn. of $Z(s)$ with only simple poles at $s=1,0$, residues $=1,-1$. RHS clearly invariant under $s\mapsto 1-s$. □

 §4. Dirichlet L-series

L-series associate to characters $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$, $N \geq 1$ (Dirichlet characters)

[$N=1$; $\mathbb{Z}/N\mathbb{Z} = \{0\} = (\mathbb{Z}/N\mathbb{Z})^\times$; so just one character viz. $\mathbb{1}$]
$0=1$

Definition χ is primitive if it does not factor

$$\begin{tikzcd} (\mathbb{Z}/N\mathbb{Z})^\times \arrow[r, "\chi"] \arrow[d, "\text{reduction hom.} = \mathrm{red}_{N,M}"'] & \mathbb{C}^\times \\ (\mathbb{Z}/M\mathbb{Z})^\times \arrow[ur, "\chi'"'] & \end{tikzcd} \qquad (*)$$

for any $M|N$ with $M<N$.

Say $\chi \pmod N$ and $\chi' \pmod{N'}$ are equivalent if $\forall x \in \mathbb{Z}$ with $(x, NN')=1$ $\chi(x \bmod N) = \chi'(x \bmod N')$

Prop^n: Let χ be a character mod N. Then there exists M and a primitive character χ^* mod M which is equivalent to χ; moreover, the characters equivalent to χ are precisely those of the form $\chi^* \circ \mathrm{red}_{N',M}$.

Proof Suppose $\chi_1 \pmod{N_1}$ and $\chi_2 \pmod{N_2}$ are equivalent. Let $N_3 = \gcd(N_1, N_2)$
Claim $\exists!\ \chi_3 \pmod{N_3}$ equivalent to χ_1 & χ_2.

$$\begin{tikzcd} & (\mathbb{Z}/N_1\mathbb{Z})^\times \arrow[dr] \arrow[drr, "\chi_1"] & & \\ (\mathbb{Z}/N_1N_2\mathbb{Z})^\times \arrow[ur] \arrow[dr] & & (\mathbb{Z}/N_3\mathbb{Z})^\times \arrow[r, dashed, "\chi_3"] & \mathbb{C}^\times \\ & (\mathbb{Z}/N_2\mathbb{Z})^\times \arrow[ur] \arrow[urr, "\chi_2"'] & & \end{tikzcd}$$

Let $(x, N_1N_2) = 1 = (y, N_1N_2)$. STP: if $x \equiv y \pmod{N_3}$
then $\chi_1(x) = \chi_1(y) = \chi_2(x) = \chi_2(y)$

Proof $N_3 = p_1N_1 + p_2N_2$ for $(p_1, p_2) = 1$.
$\therefore$ $y = x + c(p_1N_1 + p_2N_2)$, $x + cp_1N_1 = y - cp_2N_2 =: z$ say.

$$\left.\begin{array}{l} (x, N_1) = 1 \Rightarrow (z, N_1) = 1 \\ (y, N_2) = 1 \Rightarrow (z, N_2) = 1 \end{array}\right\} \Rightarrow (z, N_1N_2) = 1$$

and $\therefore$ $\chi_2(x) = \chi_1(x) = \chi_1(z) = \chi_2(z) = \chi_2(y) = \chi_1(y)$.

So if we take $M = \gcd\{N' \mid \exists\ \chi' \text{ mod } N' \text{ equivalent to } \chi\}$
then there will be $!\ \chi^*$ mod M equivalent to χ, by def^n primitive. $\square$

Def^n. $L(\chi, s) = \sum_{\substack{n \geq 1 \\ (n,N)=1}} \chi(n) n^{-s}$: Dirichlet L-series (convergent for $\mathrm{Re}(s) > 1$)

Euler product: $L(\chi, s) = \prod_{p \nmid N} \dfrac{1}{1 - \chi(p)p^{-s}} = \prod_{p \nmid N} (1 + \chi(p)p^{-s} + \chi(p^2)p^{-2s} + \dots)$

(same proof as for ζ, since χ is multiplicative).

Prop^n. Suppose $M|N$ and χ_M, χ_N are equivalent characters mod M, N respectively
Then $L(\chi_M, s) = \prod_{p \nmid M,\, p | N} \dfrac{1}{1 - \chi(p)p^{-s}} \cdot L(\chi_N, s)$ $\square$

Next aim is to analytically continue $L(\chi, s)$. Easier to do something more general. (5-1)

Let $\varphi: \mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{C}$ be any periodic function on $\mathbb{Z}$. Define

$$L(\varphi, s) = \sum_{n=1}^{\infty} \varphi(n) n^{-s}.$$

Then $(2\pi)^{-s}\Gamma(s) L(\varphi, s) = \sum_{n=1}^{\infty} \varphi(n) M(e^{-2\pi n y}, s) = M(f(y), s)$

since

$$f(y) = \sum_{n=1}^{\infty} \varphi(n) e^{-2\pi n y} = \sum_{n=1}^{N}\sum_{r=0}^{\infty} \varphi(n) e^{-2\pi(n+rN)y}$$

$$= \sum_{n=1}^{N} \varphi(n). e^{-2\pi n y} \Big/ 1 - e^{-2\pi N y} = \sum_{n=1}^{N} \varphi(n). \frac{e^{2\pi(N-n)y}}{e^{2\pi N y} - 1}$$

As $1 \le n \le N$, this is $O(e^{-2\pi y})$ as $y \to \infty$. So just as for $\zeta(s)$,

$(2\pi)^{-s}\Gamma(s) L(f, s)$ is the sum of an entire function $M_\infty(s) = \int_1^\infty f(y) y^s \frac{dy}{y}$

and $\quad M_0(s) = \sum_{n=1}^{N} \varphi(n). \int_0^1 \frac{e^{2\pi(N-n)y}}{e^{2\pi N y} - 1} . y^s \frac{dy}{y}$

Now

$$\frac{e^{2\pi(N-n)y}}{e^{2\pi N y} - 1} = \frac{1}{2\pi N y} + \sum_{r=0}^{L-1} c_{r,n} y^r + y^L g_{L,n}(y), \quad g_{L,n} \in C^\infty[0,1]$$

any $L \in \mathbb{N}$

hence

$$M_0(s) = \sum_{n \ge 1}^{N} \varphi(n) \left[\int_0^1 \frac{1}{2\pi N y} y^s \frac{dy}{y} + \sum_{r=0}^{L-1} c_{r,n} y^{r+s-1} dy \right]$$

$+$ (analytic for $Re(s) > -L$)

$$\Rightarrow (2\pi)^{-s}\Gamma(s) L(f, s) = \sum_{n \ge 1}^{N} \varphi(n) \left(\frac{1}{2\pi N(s-1)} + \frac{c_{0,n}}{s} + \dots + \frac{c_{L-1,n}}{s+L-1} \right) + (\text{analytic for } Re(s) > -L).$$

(*)

Since $\Gamma(s)$ has simple poles at $s = 0, -1, -2, \dots$, by taking

$$\varphi(n) = \begin{cases} \chi(n) & \text{if } (n, N) = 1 \\ 0 & \text{otherwise} \end{cases}$$

have proved first part of

<u>Thm</u>. i) $L(\chi, s)$ has a meromorphic continuation to $\mathbb{C}$ with at worst a simple pole at $s=1$.

ii) If χ is not the trivial character χ_0, $\chi_0(x) = 1 \ \forall x \in (\mathbb{Z}/N\mathbb{Z})^\times$ then $L(\chi, s)$ is analytic at $s=1$

If $\chi = \chi_0$ then $\operatorname{Res}_{s=1} L(\chi_0, s) = \frac{\varphi(N)}{N} = \prod_{p|N}(1 - \frac{1}{p})$

<u>Proof of (ii)</u>. $\operatorname{Res}_{s=1} L(\chi, s) = \sum_{n \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(n)/N$ by (*)

$$= \begin{cases} 0 & \text{if } \chi \ne \chi_0 \\ \frac{\#(\mathbb{Z}/N\mathbb{Z})^\times}{N} & \chi = \chi_0. \end{cases}$$

$\square$

Key fact: <u>Thm</u> If $\chi \neq \chi_0$ then $L(\chi, 1) \neq 0$.

<u>Proof</u> Let $\zeta_N(s) = \prod_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} L(\chi, s)$

$$= \prod_{p \nmid N} \prod_{\chi} (1 - \chi(p) p^{-s})^{-1}$$

<u>Lemma 1</u> $p \nmid N$. Then $\prod_{\chi \in (\mathbb{Z}/N\mathbb{Z})^\times} (1 - \chi(p) T) = (1 - T^{f_p})^{\varphi(N)/f_p}$

where f_p = order of p in $(\mathbb{Z}/N\mathbb{Z})^\times$.

(hence $\zeta_N(s) = \prod_{p \nmid N} (1 - p^{-f_p s})^{-\varphi(N)/f_p}$.)

<u>Proof.</u> Let $f = f_p$, $G = (\mathbb{Z}/N\mathbb{Z})^\times \supset H = \langle \bar{p} \rangle$, $\bar{p} = p \bmod N$, $\# H = f$.

$\hat{G} = \{ \chi : G \to \mathbb{C}^\times \} \supset \widehat{G/H} = \{ \chi \mid \chi(p) = 1 \}$; $\# \widehat{G/H} = \#(G/H) = (G:H)$

and $\hat{G} / \widehat{G/H} \xrightarrow{\sim} \hat{H} \simeq \mu_f$ as $H \simeq \mathbb{Z}/f\mathbb{Z}$

$$\prod_{\chi \in \hat{G}} (1 - \chi(p) . T) = \prod_{\chi \in \hat{H}} (1 - \chi(\bar{p}) T)^{\# \widehat{G/H}} = \prod_{\zeta \in \mu_f} (1 - \zeta T)^{\varphi(N)/f} = (1 - T^f)^{\varphi(N)/f} \qquad \square$$

<u>Lemma 2</u> Let $D(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ be a Dirichlet series with $a_n \geq 0$ $\forall n$, abs. convergent for $\mathrm{Re}(s) > \sigma_1 > 0$. If $D(s)$ can be analytically continued to an analytic function $\tilde{D}(s)$ on $\{\mathrm{Re}(s) > 0\}$ then the series converges for all real $s \in (0, \infty)$.

<u>Proof</u> Let $\rho > \sigma_1$. The analytic continuation implies: $\forall s$ with $|s - \rho| < \rho$,

$$\tilde{D}(s) = \sum_{k=0}^{\infty} \frac{1}{k!} D^{(k)}(\rho) . (s - \rho)^k, \text{ and } \tilde{D}^{(k)}(\rho) = D^{(k)}(\rho) = \sum_{n=1}^{\infty} a_n . (-\log n)^k . n^{-\rho} \quad (\text{since } \rho > \sigma)$$

So for $0 < x < \rho$ have $\tilde{D}(x) = \sum_{k=0}^{\infty} \frac{1}{k!} (\rho - x)^k \sum_{n \geq 1} a_n (\log n)^k n^{-\rho}$

which is a double series with ≥ 0 terms, hence absolutely convergent, so can be rearranged.

So $\tilde{D}(x) = \sum_{n \geq 1} a_n n^{-\rho} . \sum_{k \geq 0} ((\rho - x) \log n)^k / k! = \sum_{n \geq 1} a_n n^{-\rho} . e^{(\rho - x) \log n} = \sum_{n \geq 1} a_n n^{-x}$.

Converges $\square$

Now $\zeta_N(s) = L(\chi_0, s) . \prod_{\chi \neq \chi_0} L(\chi, s)$, and

- $L(\chi, s)$ holo. for $\mathrm{Re}(s) > 0$ $(\chi \neq \chi_0)$
- $L(\chi_0, s)$ - .... apart from simple pole at $s = 1$, residue $= \frac{\varphi(N)}{N}$.

So if some $L(\chi, 1) = 0$, product $\zeta_N(s)$ is holomorphic for $\mathrm{Re}(s) > 0$, so by Lemma, series defining $\zeta_N(s)$ is convergent for $s = x \in (0, \infty)$.

But $\zeta_N(x) = \prod_{p \nmid N} (1 + p^{-f_p x} + p^{-2 f_p x} + \ldots)^{\varphi(N)/f_p}$

$$\geq \sum_{p \nmid N} p^{-\varphi(N) x} \text{ which diverges if } 0 < x \leq \frac{1}{\varphi(N)}.$$

This last step by part (i) of: 6-13

Lemma. 3 (i) $\sum_p p^{-x} \sim -\log(x-1)$ as $x \to 1+$.

(ii) $\chi \neq \chi_0$ a D.C. mod N. Then $\sum_{p \nmid N} \chi(p) p^{-x}$ is bounded as $x \to 1+$.

Proof For any χ mod N, $x>1$,

$$\log L(\chi, x) = \sum_{p\nmid N} -\log(1-\chi(p)p^{-x}) = \sum_{p \nmid N} \sum_{r \geq 1} \frac{\chi(p)^r . p^{-rx}}{r}$$

so
$$\left| \log L(\chi,x) - \sum_{p\nmid N} \chi(p) p^{-x} \right| \leq \sum_{p\nmid N} \sum_{r \geq 2} p^{-rx}$$
$$= \sum_{p \nmid N} p^{-2x} / 1-p^{-x} \leq \sum_{n \geq 2} \frac{n^{-2}}{1-1/2} = C < \infty$$

(i) $N=1$, $\chi = \chi_0$. $\left| \zeta(x) - \frac{1}{x-1} \right|$ bounded as $x \to 1+$

$\Rightarrow$ $\log \zeta(x) \sim -\log(x-1)$ as $x \to 1$

This finishes proof that $L(\chi, 1) \neq 0$ for $\chi \neq \chi_0$.

(ii) $\chi \neq \chi_0$. $L(\chi, 1) \neq 0 \Rightarrow \log L(\chi, x)$ bounded as $x \to 1+$. $\square$.

Remark: $\zeta_N(s)$ equals, up to finite # of Euler factors, Dedekind ζ-fn. of $K = \mathbb{Q}(\sqrt[N]{1})$

$$\zeta_K(s) = \sum_{\mathfrak{n}} \frac{1}{(N\mathfrak{n})^s} \quad (\mathfrak{n} \subset \mathcal{O}_K \text{ nonzero ideals})$$

Dirichlet's theorem on primes in AP $1 \leq a < N$, $(a,N)=1$.

Then $\exists\ \infty$ many p with $p \equiv a \pmod N$

Proof. Consider the series
$$\sum_{p \equiv a \,(\mathrm{mod}\, N)} p^{-x} = \frac{1}{\varphi(N)} \sum_{\chi \in \widehat{(\mathbb{Z}/N\mathbb{Z})^\times}} \sum_{p \nmid N} \chi(a)^{-1} \chi(p) . p^{-x}$$

Lemma 3 $\Rightarrow$ For $\chi = \chi_0$, $\sum_{p\nmid N} = \sum_{p \nmid N} p^{-x} \sim -\log(1-x)$ as $x \to 1+$

and remaining terms $\chi \neq \chi_0$ are bounded as $x \to 1+$

So LHS $\sim \frac{1}{\varphi(N)} \cdot \underbrace{-\log(1-x)}_{\to \infty}$ as $x \to 1+$. Hence $\#\{p \equiv a \text{ mod } N\} = \infty$ $\square$

Remark: the argument gives

$$\lim_{x \to 1+} \left(\frac{\sum_{p \equiv a \text{ mod } N} p^{-x}}{\sum_{\text{all } p} p^{-x}} \right) \longrightarrow \frac{1}{\varphi(N)} \text{ as } x \to 1+.$$

So in some sense, $\frac{1}{\varphi(N)}$ of the primes are $\equiv a$ mod N.

(analytic density)

In fact one knows: (though harder to prove) $\lim_{X \to \infty} \frac{\#\{p \equiv a \text{ mod } N,\ p < X\}}{\#\{p < X\}} \longrightarrow \frac{1}{\varphi(N)}$.

§5. The modular group.

Have already seen fns. on $\mathfrak{H} = \{z \in \mathbb{C} \mid \operatorname{Im}(z) > 0\}$ which transform under Möbius maps:

$$\vartheta(z) = \sum_{n\in\mathbb{Z}} e^{\pi i n^2 z} = \underset{\begin{pmatrix}1&2\\0&1\end{pmatrix}}{\vartheta(z+2)} = \underset{\begin{pmatrix}0&-1\\1&0\end{pmatrix}}{(z/i)^{-1/2}\,\vartheta(-1/z)}$$

Systematic study of such functions (modular forms). First investigate action of sgps. of Möbius group.

$GL_2(\mathbb{R})$ acts on $\mathbb{C}\setminus\mathbb{R}$ and $\mathbb{R}\cup\{\infty\}$ on left by $\gamma = \begin{pmatrix}a&b\\c&d\end{pmatrix} : z \mapsto \frac{az+b}{cz+d}$

$$\operatorname{Im}\gamma(z) = \frac{1}{2i}\left(\frac{az+b}{cz+d} - \frac{a\bar{z}+b}{c\bar{z}+d}\right) = \frac{1}{2i}\frac{(ad-bc)(z-\bar{z})}{|cz+d|^2} = \det\gamma \cdot \frac{\operatorname{Im} z}{|cz+d|^2}.$$

So $\operatorname{Im} z$, $\operatorname{Im}\gamma(z)$ have same sign $\Leftrightarrow \det\gamma > 0$.

$\therefore$ $GL_2(\mathbb{R})^+ = \{\gamma \in GL_2(\mathbb{R}) \mid \det\gamma > 0\}$ maps $\mathfrak{H}$ to itself; centre $\mathbb{R}^\times\cdot\begin{pmatrix}1&0\\0&1\end{pmatrix}$ acts trivially

$\Rightarrow$ action $PGL_2(\mathbb{R})^+ \underset{\text{def}}{=} GL_2(\mathbb{R})^+/\mathbb{R}^\times\cdot\begin{pmatrix}1&0\\0&1\end{pmatrix} \longrightarrow \operatorname{Aut}\mathfrak{H}$

$GL_2(\mathbb{R})^+ = \left\langle \mathbb{R}^\times\begin{pmatrix}1&0\\0&1\end{pmatrix}, SL_2(\mathbb{R})\right\rangle$ so $PSL_2(\mathbb{R}) = SL_2(\mathbb{R})/\{\pm1\} \xrightarrow{\sim} PGL_2(\mathbb{R})^+$.

which identifies $PSL_2(\mathbb{R})$ with the group of holomorphic automorphisms of $\mathfrak{H}$.
(Later see that it is useful to consider GL, not just SL).

Action is transitive, stabiliser of $z = i$ is $SO(2)/\{\pm1\}$, a maximal compact subgroup of $PSL_2(\mathbb{R})$. This follows easily from Iwasawa decomposition

$$SL_2(\mathbb{R}) = KAN = NAK, \qquad K = SO(2) = \left\{\begin{pmatrix}\cos\theta & -\sin\theta\\ \sin\theta & \cos\theta\end{pmatrix}\right\}$$

$$A = \begin{pmatrix}*&0\\0&*\end{pmatrix}, \quad N = \begin{pmatrix}1&*\\0&1\end{pmatrix}$$

(= Gram-Schmidt orthonormalisation)

since $z = x + iy = \begin{pmatrix}1&x\\0&1\end{pmatrix}\begin{pmatrix}\sqrt{y}&0\\0&1/\sqrt{y}\end{pmatrix}(i)$.

7.1

$\Gamma \subset SL_2(\mathbb{R})$ sgp; $\bar{\Gamma}$ = image in $PSL_2(\mathbb{R}) \cong \Gamma/\Gamma \cap \{\pm 1\}$.

Mainly interested in $\Gamma = SL_2(\mathbb{Z})$ & sgps of finite index

$\bar{\Gamma} = PSL_2(\mathbb{Z})$ is the modular group. Describe action as explicitly as possible.

Let $S = \pm\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \pm\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \bar{\Gamma}$.

Thm. The set $\mathcal{D} = \left\{ z \in \mathfrak{H} \;\middle|\; \begin{array}{l} -\frac{1}{2} < Re(z) \le \frac{1}{2},\ |z| \ge 1, \\ |z| = 1 \Rightarrow Re(z) \ge 0 \end{array} \right\}$

is a fundamental domain for action of $\Gamma = SL_2(\mathbb{Z})$ on $\mathfrak{H}$

ie. $\Gamma \times \mathcal{D} \longrightarrow \mathfrak{H}$, $(\gamma, z) \longmapsto \gamma(z)$ is bijective (so $\mathcal{D} \simeq \Gamma \backslash \mathfrak{H}$). Stabilisers:-

If $z \in \mathcal{D}$, and $\bar{\Gamma}_z \ne \{1\}$ then either $z = i$, $\bar{\Gamma}_i = \langle S \rangle \cong \mathbb{Z}/2$

or $z = \rho := e^{\pi i/3}$, $\bar{\Gamma}_\rho = \langle TS \rangle \cong \mathbb{Z}/3$

Finally, $\bar{\Gamma} = \langle S, T \rangle$.

Prop. Step 1. Let $\bar{\Gamma}^* = \langle S, T \rangle \subset \bar{\Gamma}$. Will show that $\forall z \in \mathfrak{H}$, $\exists \gamma \in \bar{\Gamma}^*$ st. $\gamma(z) \in \mathcal{D}$.

Since $z \notin \mathbb{R}$, $\mathbb{Z} + z\mathbb{Z} \subset \mathbb{C}$ is a discrete sgp. of $\mathbb{C}$
$\Rightarrow \{ |cz+d| : c, d \in \mathbb{Z} \}$ is a discrete subset of $\mathbb{R}$.

$\therefore \left\{ Im\, \gamma(z) = \dfrac{Im\, z}{|cz+d|^2} \;\middle|\; \gamma \in \bar{\Gamma}^* \right\}$

is a discrete subset of $\mathbb{R}_{>0}$, bounded above.

$\therefore \exists \gamma \in \bar{\Gamma}^*$ with $Im\, \gamma(z)$ maximal. Replacing γ with $T^n\gamma$, may assume $|Re\, \gamma(z)| \le 1/2$.

If $|\gamma(z)| < 1$, then $Im\, S\gamma(z) = Im \dfrac{-1}{\gamma(z)} = \dfrac{Im\, \gamma(z)}{|\gamma(z)|^2} > Im\, \gamma(z)$

contradicting maximality of $Im\, \gamma(z)$; so $|\gamma(z)| \ge 1$.

ie $\gamma(z) \in \mathcal{D}^{cl}$. If $Re\, \gamma(z) = -1/2$ then $Re\, T\gamma(z) = 1/2$.
ie. $T\gamma(z) \in \mathcal{D}$

If $\frac{1}{2} < Re\, \gamma(z) < 0$ and $|\gamma(z)| = 1$ then $|S\gamma(z)| = 1$ and $0 < Re\, S\gamma(z) < \frac{1}{2}$ ie. $S\gamma(z) \in \mathcal{D}$.

Step 2. It's enough to show that if $z, z' \in \mathcal{D}$ and $z' = \gamma(z)$ for $\gamma = \pm\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \bar{\Gamma}$, then $z = z'$ and either:

- $\gamma = 1$
- $z = i$ and $\gamma = S$
- $z = \rho$ and $\gamma = TS$ or $(TS)^2$.

 WLOG : $\operatorname{Im}(z') = \frac{\operatorname{Im} z}{|cz+d|^2} \geq \operatorname{Im}(z)$ i.e. $|cz+d| \leq 1$. 7.2

$\Rightarrow 1 \geq |\operatorname{Im}(cz+d)| = |c| \operatorname{Im} z \geq |c| \frac{\sqrt{3}}{2}$ as $z \in \mathcal{D}$

$\Rightarrow c \in \{0, \pm 1\}$. WLOG $c = 0$ or 1. (as $\gamma = -\gamma$).

$\boxed{c=0}$ $\Rightarrow \gamma = \pm \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$, $z' = z + m$ $(m \in \mathbb{Z})$ $\Rightarrow m = 0$, $\gamma = 1$, $z = z'$.

$\boxed{c=1}$ $\Rightarrow |z+d| \leq 1$, and $|z| \geq 1$ since $z \in \mathcal{D}$. 2 possibilities:

- $d = 0 \Rightarrow |z| = 1$, $\gamma = \pm \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}$, $z' = a - 1/z$ $(a \in \mathbb{Z})$
  $\Rightarrow$ $a = 0$, $z = z' = i$ $\gamma = S$
  or $a = 1$, $z = z' = \rho$ $\gamma = TS = \pm \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$
- $d = -1 \Rightarrow |z-1| \leq 1$, and $|z| \geq 1$, $\operatorname{Re}(z) \leq 1/2$ $\Rightarrow z = \rho$.
  Then $|cz+d| = |z-1| = 1 \Rightarrow \operatorname{Im} z' = \operatorname{Im} z = \frac{\sqrt{3}}{2} \Rightarrow z' = \rho$ as well.
  Then $\frac{a\rho + b}{\rho - 1} = \rho \Rightarrow \rho^2 - (a+1)\rho - b = 0 \Rightarrow b = -1, a = 0$.
  $\therefore \gamma = (TS)^2 = \pm \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$. $\square$

<u>Remark</u>. This is the same as Gauss's proof of reduction of pos. definite binary quadratic forms.

<u>Important consequence</u>: quotient $\Gamma \backslash \mathfrak{H}$ has <u>finite invariant measure</u>:

<u>Prop$^{\underline{n}}$</u>. (i) The measure $d\mu = \frac{dx\,dy}{y^2}$ $(z = x+iy)$ on $\mathfrak{H}$ is invariant under $PSL_2(\mathbb{R})$

(ii) If $\Gamma \subset SL_2(\mathbb{Z})$ is a sgp. of finite index, then $\mu(\bar{\Gamma} \backslash \mathfrak{H}) < \infty$.

<u>Proof (i)</u>: Consider the associated 2-form

$$\eta = \frac{dx \wedge dy}{y^2} = \frac{i\, dz \wedge d\bar{z}}{2(\operatorname{Im} z)^2}.$$

STP this is invariant under $PSL_2(\mathbb{R})$. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$.

Then $\gamma'(z) = \frac{a(cz+d) - c(az+b)}{(cz+d)^2} = \frac{1}{(cz+d)^2}$ and $\operatorname{Im} \gamma(z) = \frac{\operatorname{Im} z}{|cz+d|^2}$ $\Rightarrow \eta$ invariant under γ.

 (8-1)

(ii) $M = (PSL_2(\mathbb{Z}) : \bar{\Gamma}) < \infty$. Then a fundamental domain for $\bar{\Gamma}$ is M translates of $\mathcal{D}$.

$$\mu(\bar{\Gamma}\backslash\mathfrak{H}) = M.\,\mu(\mathcal{D}) < M \int_{\substack{y \geq \sqrt{3}/2 \\ |x| \leq 1/2}} \frac{dx\,dy}{y^2} < \infty.$$ ☐

(Exercise: show $\mu(\mathcal{D}) = \pi/3$).

__Useful finite index subgroups of $SL_2(\mathbb{Z})$:-__

$N \geq 1$. $\Gamma(N) = \{\gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv I \pmod N\}$

– __principal congr. sgp. of level N__

Any $\Gamma \subset SL_2(\mathbb{Z})$ with $\Gamma \supset \Gamma(N)$ is a __congruence sgp__: minimal such N is the __level__ of Γ.

__Exs.__

$$\Gamma_0(N) = \{\gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in SL_2(\mathbb{Z}) \mid c \equiv 0 \pmod N\}$$

$$\Gamma_1(N) = \{\gamma \in \Gamma_0(N) \mid d \equiv 1 \pmod N\}$$
$(\Rightarrow a \equiv 1 \bmod N)$

$\Gamma^0(N)$, $\Gamma^1(N)$
– transposed matrices.

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

__Rem.__ $\exists$ many finite index sgps of $\Gamma(1)$ which are __not__ congruence subgroups.]

__§6. Modular forms of level 1.__

__Def^{n}__ Let $f : \mathfrak{H} \longrightarrow \mathbb{C}$ be a holomorphic fn.

f is a __modular form of weight $k \in \mathbb{Z}$ and level 1__ if

i) $f(\gamma(z)) = (cz+d)^k f(z)$ $\quad \forall \gamma = \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in \Gamma(1)$.

ii) f is holomorphic at ∞ (see below).

__Remarks.__ a) taking $\gamma = -I \in \Gamma(1)$ in (i)

$f(z) = (-1)^k f(z)$ __ie__ if f not identically 0, $k \in 2\mathbb{Z}$.

b) Will see below that $f \overset{\gamma}{\mapsto} (cz+d)^{-k} f(\gamma z)$ is a group action. Granted this:-

As $\overline{\Gamma(1)} = \langle S, T\rangle$, i) is equivalent to :-

i)' $f(z+1) = f(z) = z^{-k} f(-1/z)$.

8-2

<u>Explanation of (ii).</u> Let $q = e^{2\pi i z}$ ($z \in \mathfrak{H} \iff |q|<1$).

Then as $f(z) = f(z+1)$ by (i), $\exists \tilde{f} : \{0<|q|<1\} \to \mathbb{C}$ holomorphic with $\tilde{f}(e^{2\pi i z}) = f(z)$. $[\tilde{f}(q) = f(\frac{\log q}{2\pi i})]$.

So $\tilde{f}$ has Laurent series
$$\tilde{f}(q) = \sum_{n=-\infty}^{\infty} a_n(f) q^n.$$
– called the <u>Fourier expansion</u> or <u>q-expansion</u> of f.

f is <u>meromorphic at ∞</u> if $\tilde{f}$ meromorphic at 0 ie. $a_n(f) = 0$ for $n \ll 0$.

<u>holomorphic at ∞</u> if $\tilde{f}$ holomorphic at 0 ie. $a_n(f) = 0$ for $n<0$.

<u>Defn:</u> A modular form f is a <u>cusp form</u> if $a_0(f) = 0$.

<u>ie.</u> $\tilde{f} = \sum_{n\geq 1} a_n(f) q^n$.

(In future, we'll just write $f(z) = \sum a_n(f) q^n$ and dispense with $\tilde{f}$.)

Also: a <u>weak modular form</u> is a holo. f satisfying (i) which is <u>meromorphic at ∞</u>.

OK, so 2 qus:-

1) example of a modular form?
2) why would anyone think up such a definition?

<u>1st ex.:</u> <u>Eisenstein series.</u>

Let $k \geq 4$ be <u>even</u>. Define
$$G_k(z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^k} \overset{\text{notation}}{=} \sum_{(m,n)}{}' \frac{1}{(mz+n)^k}.$$
(' means 0 omitted)

<u>Thm.</u> The series converges absolutely, and G_k is a modular form of weight k and level 1. Moreover, its q-expansion is:-
$$G_k(z) = 2\zeta(k)\left[1 - \frac{2k}{B_k}\sum_{n\geq 1}\sigma_{k-1}(n) q^n\right] \qquad \sigma_r(n) = \sum_{0<d|n} d^r. \qquad (1)$$

(In fact cvges for all $k\geq 3$, but if k is odd, series is identically 0.)

8-3

Proof We begin with convergence. As $z \notin \mathbb{C}$, $\{1, z\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.
More generally:-

Prop^n: Let $(e_1, \dots, e_d)$ be a basis for $\mathbb{R}^d$. Then the series $(r \in \mathbb{R})$

$$\sum_{\underline{m} \in \mathbb{Z}^d}{}' \|m_1 e_1 + \dots + m_d e_d\|^{-r} \quad \text{converges iff } r > n.$$

Proof. The function $(x_i) \in \mathbb{R}^d \longmapsto \|\sum x_i e_i\|$ is a norm. By equivalence of norms on $\mathbb{R}^n$, $\exists\, C > c > 0$ s.t. $\forall\, \underline{x} \in \mathbb{R}^d$,

$$c . \|\underline{x}\|_\infty \leq \|\sum x_i e_i\| \leq C \|\underline{x}\|_\infty$$

where $\|\underline{x}\|_\infty = \max\{|x_i| : 1 \leq i \leq d\}$. So series converges iff $\sum_{\underline{m} \in \mathbb{Z}^d}{}' \|\underline{m}\|_\infty^{-r}$ converges.

But if $1 \leq N \in \mathbb{Z}$ then

$$\#\{\underline{m} \in \mathbb{Z}^d \mid \|\underline{m}\|_\infty = N\} = \#\{\|\underline{m}\|_\infty \leq N\} - \#\{\|\underline{m}\| \leq N-1\} = (2N+1)^d - (2N-1)^d \sim 2d(2N)^{d-1}$$

so $\sum' \|\underline{m}\|^{-r}$ converges iff $\sum_{N \geq 1} N^{-r} . 2d(2N)^{d-1} = d2^d \sum_{N \geq 1} N^{d-r-1}$ does ie. iff $r > d$. $\square$

So $G_k(z)$ cvges absolutely $\forall z \in \mathfrak{H}$, and

$$G_k(z+1) = \sum_{m,n}{}' (mz + (m+n))^{-k} = G_k(z) \qquad (m,n) \longleftrightarrow (m, m+n)$$

$$G_k(-1/z) = \sum_{m,n}{}' z^k (m - nz)^{-k} = z^k G_k(z) \qquad (m,n) \longleftrightarrow (-n, m).$$

So (i)' holds. It remains to show G_k holomorphic on $\mathfrak{H}$ and holomorphic at ∞.
For this, we'll obtain the series expansion (i).

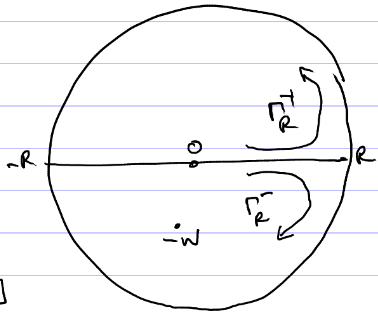
Lemma. $\displaystyle\sum_{n=-\infty}^{\infty} \frac{1}{(n+w)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{d=1}^{\infty} d^{k-1} e^{2\pi i d w}$ if $w \in \mathfrak{h}$, and $k \geq 2$.

This follows from ∞ series for cotangent (see Serre), or by Poisson summation:–

$f(x) = \dfrac{1}{(x+w)^k}$. Compute: $\hat{f}(y) = \displaystyle\int_{-\infty}^{\infty} \frac{e^{-2\pi i x y}}{(x+w)^k}\, dx$.

Now if $y > 0$, $\hat{f}(y) = \displaystyle\lim_{R\to\infty} \int_{\Gamma_R^-} \frac{e^{-2\pi i y z}}{(z+w)^k}\, dz = -2\pi i \operatorname{Res}_{z=-w}\left(e^{-2\pi i y z}\right) = -2\pi i \frac{(-2\pi i y)^{k-1}}{(k-1)!} \cdot e^{2\pi i y w}$

If $y \geq 0$, $\hat{f}(y) = \displaystyle\lim_{R\to\infty} \int_{\Gamma_R^+} = 0$



$\therefore \displaystyle\sum_n \frac{1}{(n+w)^k} = \sum_n f(n) = \sum_d \hat{f}(d) = \frac{(-2\pi i)^k}{(k-1)!} \sum_{d\geq 1} d^{k-1} e^{2\pi i d w}$

(NB: check proof of Poisson Σ works for this f.) $\square$

Apply to $G_k(z) = 2\displaystyle\sum_{n>0} n^{-k} + 2\sum_{m>0} \sum_{n\in\mathbb{Z}} (mz+n)^{-k}$
(m = 0 terms)

$= 2\zeta(k) + 2\dfrac{(2\pi i)^k}{(k-1)!} \displaystyle\sum_{m\geq 1}\sum_{d\geq 1} d^{k-1} q^{md} = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{n\geq 1} \sigma_{k-1}(n) q^n$ $\quad (n = md)$.

Final formula follows from: $\zeta(k) = -\frac{1}{2}(2\pi i)^k B_k / k!$ for even $k \geq 2$ (Ex I.5) $\square$

It's convenient to define the <u>normalised Eisenstein series</u>

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

If $d = \gcd(m,n)$, $m = dm_1$, $n = dn_1$ then $(mz+n)^{-k} = d^{-k} \cdot (m_1 z + n_1)^{-k}$, from which obtain

$$E_k(z) = \frac{1}{2} \sum_{\substack{m,n\in\mathbb{Z} \\ (m,n)=1}} \frac{1}{(mz+n)^k} .$$

<u>Exs.</u> $B_2 = 1/6$, $B_4 = -1/30$, $B_6 = 1/42$, $B_8 = -1/30$, $B_{10} = 5/66$, $B_{12} = -\dfrac{691}{2730}$, $B_{14} = 7/6$.

$\therefore$ $E_4 = 1 + 240 \sum \sigma_3(n) q^n$ (NB. except for E_{12}, these coefficients follow a simple rule)

$E_6 = 1 - 504 \sum \sigma_5(n) q^n$

$E_8 = 1 + 480 \sum \sigma_7(n) q^n$

$E_{10} = 1 - 264 \sum \sigma_9(n) q^n$

$E_{12} = 1 + \dfrac{65520}{691} \sum \sigma_{11}(n) q^n$

$E_{14} = 1 - 24 \sum \sigma_{13}(n) q^n$.

Next: important group-theoretic interpretation of Eis. series.

Def$^{\underline{n}}$. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \gamma \in GL_2(\mathbb{R})^+$, $z \in \mathfrak{H}$, $f : \mathfrak{H} \to \mathbb{C}$ a fnctn.

$$j(\gamma, z) := cz + d \quad ; \quad (f|_k \gamma)(z) := (\det \gamma)^{k/2} j(\gamma, z)^{-k} f(z)$$

$$\left(f|_k \gamma = f \text{ if } \gamma = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \text{ and } a^k > 0. \right)$$

So condition (i) in defn of modular form can be rewrittn:

(i) $\forall \gamma \in \Gamma(1)$, $f|_k \gamma = f$.

Note that $\gamma \begin{pmatrix} z \\ 1 \end{pmatrix} = j(\gamma, z) \begin{pmatrix} \gamma(z) \\ 1 \end{pmatrix}$ (*)

Prop$^{\underline{n}}$. (i) $j(\gamma\delta, z) = j(\gamma, \delta(z)) j(\delta, z)$ (j is a $\underline{\text{1-cocycle}}$)

$j(\gamma^{-1}, z) = j(\gamma, \gamma^{-1}(z))^{-1}$.

(ii) $\gamma : f \longmapsto f|_k \gamma$ is a (right) action ; $(f|_k\gamma)|_k \delta = f|_k(\gamma\delta)$.

Proof. (i) $j(\gamma\delta, z) \begin{pmatrix} \gamma\delta(z) \\ 1 \end{pmatrix} = \gamma\delta \begin{pmatrix} z \\ 1 \end{pmatrix} = j(\delta, z) . \gamma \begin{pmatrix} \delta(z) \\ 1 \end{pmatrix} = j(\delta, z) . j(\gamma, \delta(z)) \begin{pmatrix} \gamma\delta(z) \\ 1 \end{pmatrix}$ by (*)

2$^{\text{nd}}$ identity follows, taking $\delta = \gamma^{-1}$.

(ii) $((f|_k\gamma)|_k\delta)(z) = (\det \delta)^{k/2} j(\delta, z)^{-k} (f|_k \gamma)(\delta(z)) = (\det \delta)^{k/2} j(\delta, z)^{-k} (\det \gamma)^{k/2} j(\gamma, \delta(z))^{-k} f(\gamma\delta(z))$

$= (f|_k \gamma\delta)(z)$ by (i) □

Back to Eis. series. $SL_2(\mathbb{Z}) = \Gamma(1) \supset \Gamma(1)_\infty = \left\{ \pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}, n \in \mathbb{Z} \right\}$

Ex. sheet?

stabiliser of ∞.

If $\delta = \pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ then $j(\delta\gamma, z) = j(\delta, \gamma(z)) j(\gamma, z) = \pm j(\gamma, z)$, so $j(\gamma, z)^2$ depends only on coset $\Gamma(1)_\infty \cdot \gamma$

Moreover, if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $\gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z})$ then

$$\Gamma(1)_\infty \cdot \gamma = \Gamma(1)_\infty \cdot \gamma' \iff (c, d) = \pm (c', d')$$

Since $\gcd(c, d) = 1 \iff \exists a, b$ with $ad - bc = 1$, get:

$$\boxed{E_k(z) = \sum_{\gamma \in \Gamma(1)_\infty \backslash \Gamma(1)} j(\gamma, z)^{-k}.}$$

($\Gamma(1)_\infty \backslash \Gamma(1)$ = set of cosets $\Gamma(1)_\infty \cdot \gamma$.)

$\underline{\text{A useful estimate.}}$ (Ex. sheet ?) (Later will see generalisations of this.)

Prop$^{\underline{n}}$ Let $f : \mathfrak{H} \to \mathbb{C}$ be holomorphic, $f|_k \gamma = f$ $\forall \gamma \in \Gamma(1)$, $k > 0$. Then f is a cusp form $\iff$ $y^{k/2} |f(x + iy)|$ is bounded on $\mathfrak{H}$.

Proof $\operatorname{Im} \gamma(z) = \dfrac{\operatorname{Im} z}{|j(\gamma, z)|^2}$ $\Rightarrow$ $y^{k/2} |f|$ is $\underline{\text{invariant}}$ under $z \mapsto \gamma(z)$, $\gamma \in \Gamma(1)$.

- If $a_n(f) \neq 0$ for some $n \leq 0$ then $y^{k/2}|f|$ obviously unbounded as $y \to \infty$.
- $a_n(f) = 0$ $\forall n \leq 0 \Rightarrow y^{k/2} |f| = O(y^{k/2} e^{-y}) \to 0$ as $y \to \infty$ uniformly in x.

So $y^{k/2}|f|$ bounded on $\mathfrak{D}$ hence (by invariance) on $\mathfrak{H}$. □

§7. The space of modular forms.

($k \in \mathbb{Z}$) Let $M_k(\Gamma(1)) = \{$modular forms of wt k, level $1\} = M_k$ for short.

$\quad\quad\quad\quad\quad\quad\quad\cup$

$\quad\quad\quad\quad\quad\quad S_k(\Gamma(1)) = \{$cusp — " — — " —$\}. = S_k$

These are $\mathbb{C}$-vector spaces, zero for k odd, and from definition we have

$$M_k \cdot M_\ell \subset M_{k+\ell}, \quad S_k \cdot M_\ell \subset M_{k+\ell}$$

and $S_k = \ker$ of map $M_k \longrightarrow \mathbb{C}$

$$f \longmapsto a_0(f).$$

We will determine M_k, S_k explicitly.

> Rem. $M_* = \bigoplus_k M_k$, $S_* = \bigoplus_k S_k$
>
> M_* is a graded ring, S_* a graded ideal.

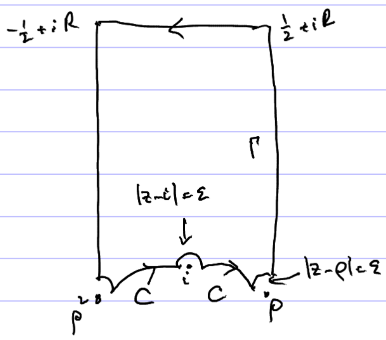
Prop. Let f be a weak modular form of wt k, not identically zero. Then

$$\sum_{z_0 \in \mathcal{D} \setminus \{i, \rho\}} \mathrm{ord}_{z_0} f + \frac{1}{2}\mathrm{ord}_i f + \frac{1}{3}\mathrm{ord}_\rho f + \mathrm{ord}_\infty f = k/12$$

where $\mathrm{ord}_\infty f = $ (order of $\tilde{f}(q)$ at $q=0$). (NB. if $z_1 = \gamma(z_0)$, $\gamma \in \Gamma(1)$ then $\mathrm{ord}_{z_1} f = \mathrm{ord}_{z_0} f$)

Proof. The fn. $\tilde{f}(q)$ is $\neq 0$ for $0 < |q| \leq \varepsilon$, ε suff. small, by isolated zeros.
$\therefore$ $f \neq 0$ for $\mathrm{Im}(z) \geq R$ if $\varepsilon = e^{-2\pi R}$, hence # of zeros of f in $\mathcal{D}$ is finite.

Integrate f'/f around contour Γ; assume first f has no zero on boundary except perhaps at i, ρ (so also ρ^2).



- $\int_\Gamma f'/f \, dz = 2\pi i \sum_{z_0 \in \mathcal{D} \setminus \{i, \rho\}} \mathrm{ord}_{z_0} f$
- $f(z) = f(z+1) \Rightarrow$ integrals on vertical lines cancel.
- integral $\int_{1/2+iR}^{-1/2+iR} = -\int_{|q|=\varepsilon} \frac{\tilde{f}'(q)}{\tilde{f}(q)} dq = -2\pi i \,\mathrm{ord}_\infty f$

  as $\frac{d\tilde{f}}{dq} \cdot dq = \frac{df}{dz} \cdot dz$
- integral along arc around $i \longrightarrow -\pi i \,\mathrm{ord}_i f$ as $\varepsilon \to 0$
- ——————— around $\rho, \rho^2 \longrightarrow -\frac{\pi i}{3}\mathrm{ord}_\rho f = -\frac{\pi i}{3}\mathrm{ord}_{\rho^2} f$ as $\varepsilon \to 0$

- S maps arc C to arc C' (with opposite orientation as $S(i) = i$)

  and $\frac{df(Sz)}{f(Sz)} = k\frac{dz}{z} + \frac{df(z)}{f(z)}$ as $f(Sz) = z^k f(z)$.

$$\therefore \int_C + \int_{C'} = \int_{C'} \frac{f'}{f}dz - \left(k\frac{dz}{z} + \frac{f'}{f}dz\right) = -\int_{C'} k\frac{dz}{z} \xrightarrow[\varepsilon \to 0]{} \int_\rho^i k\frac{dz}{z} = \left[k \log z\right]_\rho^i = \frac{\pi i k}{6}.$$

Putting together gives formula. (If f vanishes at some other points on boundary, make indentations in usual way.) $\square$

First applications: (1) If $k<0$ then $M_k = \{0\}$ (if $f \in M_k$, LHS ≥ 0) (10-2)

(2) $M_0 = \mathbb{C}$, $S_0 = \{0\}$. Proof. Obviously $\mathbb{C} \subset M_0$ (as (i) is then $f(\gamma(z)) = f(z)$).

If $f \in M_0$, then let $g = f - f(i)$. Then $\mathrm{ord}_i\, g \geq 1$, $\mathrm{ord}_{z_0} g \geq 0$ $\forall z_0$ (incl. ∞)

So LHS ≥ 1 > RHS $= 0$ $\Rightarrow$ $g \equiv 0$, $f = f(i)$ constant.

Then $f(z) = \tilde{f}(0) = a_0(f)$, so $a_0(f) = 0 \Rightarrow f \equiv 0$. $\square$

(3) $\dim M_k \leq 1 + \frac{k}{12}$. Proof. Let $f_0, \dots, f_d$ be $(d+1)$ elts. of M_k, & choose distinct $z_1, \dots, z_d \in \mathcal{D} \setminus \{i, \rho\}$. Then $\exists \lambda_0, \dots, \lambda_d \in \mathbb{C}$ not all 0 s.t. $f = \sum_{i=0}^{d} \lambda_i f_i$ vanishes at $z_1, \dots, z_d$. If $d > \frac{k}{12}$, Prop^n $\Rightarrow f \equiv 0$, so $\{f_i\}$ are lin. dependent i.e. $\dim M_k \leq d$. $\square$

(4) $M_2 = \{0\}$ and $M_k = \mathbb{C}.E_k$ for $4 \leq k \leq 10$; moreover $E_8 = E_4^2$, $E_{10} = E_4 E_6$.

Proof. By (3), $\dim M_k \leq 1$ if $k < 12$, and $0 \neq E_k \in M_k$ for $k \geq 4$.

$\Rightarrow M_k = \mathbb{C}.E_k$ for $4 \leq k \leq 10$. As $E_4^2 \in M_8$ and $E_4 E_6 \in M_{10}$ get last statement (after comparing const. term of q-expansion).

$k=2$: Suppose $0 \neq f \in M_2$. By Prop^n, $\frac{1}{6} = a + \frac{b}{2} + \frac{c}{3}$ for integers $a, b, c \geq 0$, impossible. $\square$

(5) The cusp form Δ of weight 12

$$E_4^3 - E_6^2 = (1 + 240 \textstyle\sum \sigma_3(n) q^n)^3 - (1 - 504 \textstyle\sum \sigma_5(n) q^n)^2$$
$$= (3.240 + 2.504)\, q + \dots = 1728\, q + \dots$$

which is therefore a cusp form of weight 12. Let $\Delta(z) = \frac{E_4^3 - E_6^2}{1728} \in S_{12}(\Gamma(1))$.

$$= \sum_{n \geq 1} \tau(n) q^n, \quad \tau(1) = 1$$

Ramanujan's τ-function.

Prop^n $\Delta(z) \neq 0$ for $z \in \mathfrak{H}$.

Proof. Apply prop^n to Δ, $k=12$; as $\mathrm{ord}_\infty(\Delta) = 1$, $\mathrm{ord}_{z_0} \Delta = 0$ $\forall z_0 \in \mathcal{D}$ and so also $\forall z \in \mathfrak{H}$. $\square$

Prop^{n}. The map $f \mapsto \Delta f$ is an isomorphism $M_{k-12}(\Gamma(1)) \xrightarrow{\sim} S_k(\Gamma(1))$.

Proof If $g \in S_k$ then g/Δ is holomorphic on $\mathfrak{H}$ as $\Delta(z) \neq 0$, and holomorphic at ∞ since $\mathrm{ord}_\infty \Delta = 1 \leq \mathrm{ord}_\infty g$. So the (obviously injective) map is an $\cong$. $\square$

Theorem. (i) $\dim M_k(\Gamma(1)) = \begin{cases} 0 & \text{if } k<0 \text{ or } k \text{ odd} \\ \lfloor \frac{k}{12} \rfloor & \text{if } k \equiv 2\ (12),\ k>0 \\ 1+\lfloor \frac{k}{12} \rfloor & \text{if } k \not\equiv 2\ (12) \text{ even } >0. \end{cases}$

(ii) If $k \geq 4$ even, $M_k = \mathbb{C}.E_k \oplus S_k$.

(iii) Every elt. of M_k is a polynomial in E_4 and E_6.

(iv) Let $b=0$ if $k \equiv 0 \pmod 4$, $=1$ if $k \equiv 2 \pmod 4$. Then the forms $h_j = \Delta^j E_6^b E_4^{(k-12j-6b)/4}$ $(0 \leq j < \dim M_k)$ form a basis for M_k.

Proof (ii) The map $M_k \xrightarrow{a_0} \mathbb{C}$, $f \mapsto a_0(f)$ has kernel S_k. If $k \geq 4$, $E_k \in M_k$ so a_0 is surjective and (ii) follows.

(i) already seen for $k<12$, by (1)–(4) above.

By last prop^{n}, $\dim M_{k-12} = \dim S_k$ $\forall k$, and so (ii) $\Rightarrow$ $\dim M_k = 1+\dim M_{k-12}$ if $k \geq 4$. $\therefore$ (i) holds $\forall k$.

(iii) True for $k<12$ by above. Now if $k \geq 12$, $\exists a,b \geq 0$ st. $4a+6b=k$. So $E_4^a E_6^b \in M_k \setminus S_k$. ie. $M_k = \mathbb{C}.E_4^a E_6^b \oplus \Delta.M_{k-12}$ and as $\Delta \in \mathbb{C}[E_4, E_6]$, (iii) follows by induction on k.

(iv) As $\dim M_k = \lfloor \frac{k}{12} \rfloor + 1$ or $\lfloor \frac{k}{12} \rfloor$ according as $k \not\equiv 2$, $k \equiv 2 \pmod{12}$, $k-12j-6b \geq 0$ for $j < \dim M_k$, so $h_j \in M_k$. As q-exp. of h_j begins with q^j, they are linearly independent. $\square$

Arithmetic of Δ. Set $\Delta = \sum_{n=1}^{\infty} \tau(n) q^n \in \mathbb{Q}[[q]]$, $\tau(1)=1$.

$\tau(n)$ is Ramanujan's function.

Prop^{n} (i) $\tau(n) \in \mathbb{Z}$ $\forall n \in \mathbb{Z}$. (ii) $\tau(n) \equiv \sigma_{11}(n) \pmod{691}$.

Proof (i)
$$1728\Delta = (1+240A_3(q))^3 - (1-504A_5(q))^2 \qquad A_r(q) = \sum \sigma_r(n) q^n$$
$$= 3.240 A_3 + 3.240^2 A_3^2 + 240^3 A_3^3 \qquad 1728 = 12^3$$
$$+ 2.504 A_5 - 504^2.A_5^2 \qquad 504 = 21.24$$
$$\equiv 720 A_3 + 1008 A_5 \mod 1728$$
$$\Rightarrow 12\Delta \equiv 5A_3 + 7A_5 \mod 12$$

So STP $5\sigma_3(n) + 7\sigma_5(n) \equiv 0 \mod 12$ n.

$\text{LHS} = \sum_{d|n} 5d^3 + 7d^5 \equiv \sum_d 7d^2(d^2-1)$ and $\forall d \in \mathbb{Z}$, $d^2(d^2-1) \equiv 0 \pmod{12}$.

 11-2

(ii) Consider $E_4^3 = 1 + \sum_{n\geq 1} b_n q^n$, $b_n \in \mathbb{Z}$, $b_1 = 720$ and $E_{12} = 1 + \frac{65520}{691} \sum \sigma_{11}(n) q^n$.

$E_{12} - E_4^3 \in S_{12}(\Gamma(1))$ so $= \lambda \Delta$ for some λ

ie $\forall n \geq 1$, $\frac{65520}{691}\sigma_{11}(n) - b_n = \lambda \tau(n)$.

$$65520\,\sigma_{11}(n) - 691 b_n = \mu . \tau(n)$$

$n=1$ $\tau(1) = \sigma_{11}(1) = 1 \Rightarrow \mu \in \mathbb{Z}$, $\mu \equiv 65520 \pmod{691}$

$\Rightarrow \sigma_{11}(n) \equiv \tau(n) \pmod{691}$ $\forall n \geq 1$. $\square$

Later will prove: (Jacobi) $\Delta = q \prod_{m\geq 1} (1-q^m)^{24}$.

(Mordell-Hecke) $\tau(mn) = \tau(m)\tau(n)$ if $(m,n) = 1$.

and explain relation between the sequence $(\tau(p))_p$ and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

<u>Rationality & integrality properties</u> $R \subset \mathbb{C}$ a subring. Define

$$M_k(R) = M_k(\Gamma(1), R) = \{ f \in M_k \mid \forall n,\ a_n(f) \in R \}$$

and $S_k(R) = S_k \cap M_k(R)$. So $M_k \hookrightarrow R[[q]]$ by q-exp. map.

$S_k \hookrightarrow qR[[q]]$

<u>Thm.</u> (i) Suppose $\dim M_k = d+1 \geq 1$. Then $\exists$ basis $\{g_j \mid 0 \leq j \leq d\}$ for M_k with

- $g_j \in M_k(\mathbb{Z})$ $\forall j \in \{0, \dots d\}$
- $a_n(g_j) = \delta_{nj}$ $\forall j, n \in \{0, \dots d\}$.

(ii) $\forall R$, $M_k(R) \simeq R^{d+1}$, generated by $\{g_j\}$.

<u>Proof.</u> (i) Let $b = 0$ if $4|k$, $b = 1$ otherwise. Consider

$$h_j = \Delta^j . E_6^b E_4^{(k-6b-12j)/4} \in M_k(\mathbb{Z}) \qquad (0 \leq j \leq d)$$

Then $\{h_j\}$ is a basis for M_k, and $a_n(h_j) = \begin{cases} 0 & n<j \\ 1 & n=j \end{cases}$. So by elementary row operations we can find $c_{ij} \in \mathbb{Z}$ $(0 \leq j < i \leq d)$ such that

$g_j = h_j + \sum_{j<i\leq d} c_{ij} h_i$ has the desired properties.

(ii) The isom$^{=}$ is given by $f \longmapsto (a_j(f))_{0\leq j \leq d}$

$$\sum_{j=0}^{d} c_j g_j \longleftarrow (c_j).$$ $\square$