Modular Forms II

(by H. Darmon)

Hecke Theory

Let $f \in S_k(SL_2(\mathbb{Z}))$, $f = \sum_{n=1}^{\infty} a_n q^n$ $(a_n \in \mathbb{C})$. $(q = e^{2\pi i \tau}, \tau = x+iy)$

Consider its L-series $L(f,s) := \sum_{n=1}^{\infty} a_n n^{-s}$.

Q: Where does this converge?

Prop: $|f(x+iy)| << Ce^{-2\pi y}$ as $y \to +\infty$.

Pf/ $f(x+iy) = \sum_1^{\infty} a_n e^{-2\pi n y} e^{2\pi i n x} = e^{-2\pi y}\left(\sum_1^{\infty} a_n e^{-2\pi i (n-1) y} e^{2\pi i n x}\right)$

$<< e^{-2\pi y}$ //

Prop (Behaviour of f when $y \to 0$):

Uniformly in x, $|f(x+iy)| << y^{-k/2}$ as $y \to 0$.

Pf/ From its definition, $f(\gamma\tau) = (c\tau+d)^k f(\tau)$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.

Hence $|f(\gamma\tau)|^2 = (c\tau+d)^k (c\bar{\tau}+d)^k |f(\tau)|^2$.

Note that $y(\tau) = \frac{\tau - \bar{\tau}}{2i}$, and $y(\gamma\tau) = \frac{\gamma\tau - \overline{\gamma\tau}}{2i} = \frac{y(\tau)}{(c\tau+d)(c\bar{\tau}+d)}$

This suggests to define $G(\tau) := y^k |f(\tau)|^2$, and observe that $G(\tau)$ is invariant under $SL_2(\mathbb{Z})$. Hence $G(\tau) << 1$.

(b/c it's continuous on the compactified fundamental domain $\mathcal{H}^* / SL_2(\mathbb{Z})$).

From this, a fortiori, $|f(\tau)| << y^{-k/2}$, as wanted. //

Prop: $|a_n| << n^{k/2}$

Pf $\int_0^1 f(x+iy)\, e^{-2\pi i n x}\, dx = a_n e^{-2\pi n y}$ (for y fixed).

Thus $|a_n| e^{-2\pi n y} << y^{-k/2}$. By setting $y = 1/n$, we are done //

Rk: We didn't make any serious use of f being a cusp form.
In fact, if we work harder we would get, for cusp forms, $|a_n| << n^{\frac{k-1}{2}}$.

Corollary: $L(f,s)$ converges absolutely for $\mathrm{Re}(s) > k/2 + 1$.

Pf $\sum a_n n^{-s} << \sum n^{k/2} n^{-\mathrm{Re}(s)} < +\infty$ //.

Integral Representation of $L(f,s)$.

Let $\Gamma(s) := \int_0^\infty t^s e^{-t} \frac{dt}{t}$ be the Gamma-function.

Set $\Lambda(f,s) := (2\pi)^{-s} \Gamma(s) L(f,s)$

Prop: $\Lambda(f,s) = \int_0^\infty f(it)\, t^s \frac{dt}{t}$

Rk: $\left| \int_0^\infty f(it) t^s \frac{dt}{t} \right| << \int_1^\infty t^{-k/2+s} \frac{dt}{t}$, which converges provided that $s > k/2$.

Pf $\Lambda(f,s) = (2\pi)^{-s} \left(\int_0^\infty t^s e^{-t} \frac{dt}{t} \right) \left(\sum_1^\infty a_n n^{-s} \right) = \sum_1^\infty a_n \int_0^\infty \left(\frac{t}{2\pi n} \right)^s e^{-t} \frac{dt}{t}$

Change variable $t \mapsto \frac{t}{2\pi n}$, and get $= \sum_1^\infty a_n \int_0^\infty t^s e^{-2\pi n t} \frac{dt}{t} =$

$= \int_0^\infty \left(\sum_{n=1}^\infty a_n e^{-2\pi n t} \right) t^s \frac{dt}{t} = \int_0^\infty f(it)\, t^s \frac{dt}{t}$. //

Theorem: $\Lambda(f,s) = \int_1^\infty f(it)\, t^s \frac{dt}{t} + i^k \int_1^\infty f(it)\, t^{k-s} \frac{dt}{t}$.

Pf $\Lambda(f,s) = \int_1^\infty + \int_0^1 f(it)\, t^s \frac{dt}{t}$.

The modularity of $f \Rightarrow f\left(-\frac{1}{it}\right) = (it)^k f(t)$. Apply $t \mapsto \frac{1}{t}$ (or change of variables), to get $\int_0^1 f(it)\, t^s \frac{dt}{t} = \int_\infty^1 f(i/t)\, t^{-s}\left(-\frac{dt}{t}\right) =$

$= i^k \int_1^\infty f(it)\, t^{k-s} \frac{dt}{t}$ as wanted //

Rk: This gives the analytic continuation of $\Lambda(f,s)$, as well as that of $L(f,s)$.

Moreover, we get also the functional equation:

$$\left[i^k \Lambda(f, k-s) = \Lambda(f,s) \right].$$

• Forms on $\Gamma_0(N)$

Let $f \in S_k(\Gamma_0(N))$, $\Lambda(f,s) = \int_0^\infty f(it) t^s \frac{dt}{t}$.

However, $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ does not belong to $\Gamma_0(N)$ for $N > 1$ (and there is no $\gamma \in \Gamma_0(N)$ s.t. $\gamma \cdot 0 = \infty$).

Let $S_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. We have $S_N \begin{pmatrix} a & b \\ c & d \end{pmatrix} S_N^{-1} = \begin{pmatrix} d & -c/N \\ -bN & a \end{pmatrix}$,

and so $S_N \Gamma_0(N) S_N^{-1} = \Gamma_0(N)$.

Q: What is the relationship between $f(it)$ and $f(i/Nt)$?

(we'll see it later).

• Slash Operators.

Let $M \in GL_2^+(\mathbb{Q})$, $f \in S_k(\Gamma)$.

Def: $(f|_k M)(\tau) := (\det M)^{k/2} (c\tau + d)^{-k} f(M\tau)$.

Remarks:

1) $f \in S_k(\Gamma) \iff f|_k \gamma = f \quad \forall \gamma \in \Gamma \leq SL_2(\mathbb{Z})$. (+ cusp conditions).

2) $f|_k (M_1 M_2) = (f|_k M_1)|_k M_2$.

3) $f|_k \begin{pmatrix} d & 0 \\ 0 & d \end{pmatrix} = f$

4) For $f \in S_k(\Gamma)$, $f|_k M \in S_k(M^{-1}\Gamma M)$.

5) $f|_k S_N \in S_k(\Gamma_0(N))$.

Def (Fricke involution): as $W_N := \cdot|_k S_N$, $W_N : S_k(\Gamma_0(N)) \to S_k(\Gamma_0(N))$.

Thm: $$\Lambda(f,s) = \int_{\frac{1}{\sqrt{N}}}^{\infty} f(it) t^s \frac{dt}{t} + i^k N^{k/2 - s} \int_{\frac{1}{\sqrt{N}}}^{\infty} g(it) t^{k-s} \frac{dt}{t}$$

where $g = f|_k S_N = W_N(f)$.

Also, there is a Functional eq: $\Lambda(f,s) = i^k N^{k/2 - s} \Lambda(W_N(f), k-s)$.

Pf Exercise!

Important special case: if f is an eigenvector for W_N, then $f|_k S_N = \varepsilon f$, where $\varepsilon \in \{\pm 1\}$, and $\Lambda(f,s) = \varepsilon i^k N^{\frac{k}{2} - s} \Lambda(f, k-s)$

Example: Suppose that E is an e.c. and f is its associated modular form on $\Gamma_0(N)$, with $N = \mathrm{cond}(E)$, of weight $k=2$. Then the F.eq. is:

$$\Lambda(E, s) = -\varepsilon N^{1-s} \Lambda(E, 2-s),$$

where ε is defined by $w_N(f) = \varepsilon \cdot f$

→ If $\varepsilon = 1$, then $\Lambda(E,1) = 0$ ($\Rightarrow L(E,1) = 0$). In this case, the Birch–Swinnerton-Dyer conjecture predicts that $\#E(\mathbb{Q}) = \infty$

→ If $\varepsilon = -1$, then $\mathrm{ord}_{s=1} \Lambda(E,s)$ is even. Again, BSD predicts $\mathrm{rk}(E(\mathbb{Q}))$ is <u>even</u>.

Q: When does $L(f,s)$ admit an Euler product expression? If so, what is the shape of this Euler product?

$$\sum_{1}^{\infty} a_n n^{-s} = \prod_p \left(\sum_0^{\infty} a_{p^r} p^{-rs} \right)$$

if $n \mapsto a_n$ is multiplicative (i.e. $a_{mn} = a_n a_m$ for $(n,m)=1$).

To give a criterion for the existence of such an Euler product for $L(f,s)$, Hecke introduced the so-called "Hecke Operators". We will restrict ourselves at the beginning to $SL_2(\mathbb{Z})$.

• Hecke operators.

Recall: Think of modular forms as functions on lattices.

$$f(\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2) = \omega_2^{-k} f\left(\omega_1/\omega_2\right) \quad \text{if } \operatorname{Im}\left(\tfrac{\omega_1}{\omega_2}\right) > 0$$

Conversely,

$$f(\tau) := f\left(\mathbb{Z}\tau + \mathbb{Z}\right), \quad \tau \in \mathcal{H}.$$

The weight has to be imposed, as well:

$$f(\lambda\Lambda) = \lambda^{-k} f(\Lambda) \qquad \text{(weight } k\text{)}.$$

The Hecke operator T_n.

• First, as a function on lattices:

$$(T_n f)(\Lambda) := n^{k-1} \sum_{\Lambda' \subseteq \Lambda \text{ of index } n} f(\Lambda') \qquad (\text{def})$$

One would need to check the growth conditions at ∞, but we'll do it later.

• Second, the double-coset point of view:

Consider $M_n := \left\{ \alpha \in M_2(\mathbb{Z}) : \alpha \cdot (\mathbb{Z} \oplus \mathbb{Z}) \subseteq_{n \text{ (index } n)} \mathbb{Z} \oplus \mathbb{Z} \right\}$.

Claim: 1) $M_n = SL_2(\mathbb{Z}) \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix} SL_2(\mathbb{Z})$

2) If $M_n = \dot{\bigcup_{i=1}^{t}} SL_2(\mathbb{Z})\,\alpha_i$ (decomposition of left cosets),

then $\mathbb{Z}^2\alpha_1, \dots, \mathbb{Z}^2\alpha_t$ are a complete set of the distinct lattices Λ with $\Lambda \subseteq_n \mathbb{Z}^2$.

Pf / Exercise.

One then defines (check that this is the same def. as before):

$$(T_n f)(\tau) = n^{\frac{k}{2}-1} \cdot \sum_{i=1}^{t} (f|_k \alpha_i)(\tau) = \quad \text{(independent on the choice of rep, and mod-form of wt } k \text{ on } SL_2(\mathbb{Z})\text{)}$$

$$= n^{k-1} \sum_{i=1}^{t} j(\alpha_i, \tau)^{-k} f(\alpha_i \tau) \qquad \text{where } j(\alpha_i, \tau) = c\tau + d \text{ if } \alpha_i = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Basic Properties:

1) $T_n : S_k(SL_2(\mathbb{Z})) \to S_k(SL_2(\mathbb{Z}))$ is $\mathbb{C}$-linear.

2) Multiplicativity: if $(m,n)=1$, then $T_{mn} = T_m \circ T_n \ (= T_n \circ T_m)$.

Proof:

Let $\mathcal{L}$ = free $\mathbb{Z}$-module generated by the lattices in $\mathbb{C}$:

$$\mathcal{L} = \left\{ \sum_{i=1}^{t} n_i [\Lambda_i] : n_i \in \mathbb{Z} \right\}.$$

$$\widetilde{T}_n : \mathcal{L} \longrightarrow \mathcal{L}$$
$$[\Lambda] \longmapsto \sum_{\Lambda' \overset{c}{n} \Lambda} [\Lambda'] \qquad \text{(note that } (T_n f)(\Lambda) = n^{k-1} f\left(\widehat{\widetilde{T}}_n([\Lambda])\right)\text{)}.$$

If $\Lambda' \overset{c}{mn} \Lambda$, then there exists a unique Λ'' with $\Lambda' \overset{c}{m} \Lambda'' \overset{c}{n} \Lambda$.

The assignment $\Lambda' \longleftrightarrow (\Lambda', \Lambda'')$ is a bijection, so:

$$\widetilde{T}_{mn}([\Lambda]) = \sum_{\Lambda' \overset{c}{mn} \Lambda} [\Lambda'] = \sum_{\Lambda'' \overset{c}{n} \Lambda} \left(\sum_{\Lambda' \overset{c}{m} \Lambda''} [\Lambda'] \right) = \sum_{\Lambda'' \overset{c}{n} \Lambda} \widetilde{T}_m([\Lambda''])$$

$$= \widetilde{T}_m \left(\sum_{\Lambda'' \overset{c}{n} \Lambda} [\Lambda''] \right) = \widetilde{T}_m \left(\widetilde{T}_n([\Lambda]) \right) \Rightarrow \widetilde{T}_{mn} = \widetilde{T}_m \circ \widetilde{T}_n$$

and we get the result.

It is enough now to understand T_{p^r}

Lemma: $T_p \circ T_{p^{r-1}} = T_{p^r} + p^{k-1} T_{p^{r-2}}$ if $r \geq 2$

(and so $T_p \cdot T_{p^{r-1}} = T_{p^{r-1}} \cdot T_p$!)

Pf/ $\left(\widetilde{T}_p \circ \widetilde{T}_{p^{r-1}}\right)([\Lambda]) = \widetilde{T}_{p^r}([\Lambda]) + p\,\widetilde{T}_{p^{r-2}}([p\Lambda])$ (exercise)

and the lemma follows from this:

$$\left(T_p \circ T_{p^{r-1}} f\right)(\Lambda) = T_p\left(p^{(k-1)(r-1)} f\left(\widetilde{T}_{p^{r-1}}([\Lambda])\right)\right) = p^{r(k-1)} f\left(\widetilde{T}_{p^{r-1}}\left(\widetilde{T}_p[\Lambda]\right)\right)$$

$$= p^{r(k-1)} f\left(\widetilde{T}_{p^r}([\Lambda]) + p\,\widetilde{T}_{p^{r-2}}([p\Lambda])\right) = \cdots$$

Explicit formulas (for the Hecke operators)

Note that, from the above results, it is enough to find formulas for T_p.

Lemma: $SL_2(\mathbb{Z})\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} SL_2(\mathbb{Z}) = \left(\bigcup_{j=0}^{p-1} SL_2(\mathbb{Z})\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}\right) \cup SL_2(\mathbb{Z})\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$

Pf/ Just note that:

$$SL_2(\mathbb{Z})\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \left\{ \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in M_2(\mathbb{Z}) \text{ of det } p \text{ (= det } p) \text{ s.t. } (a'\ b') = \lambda(a, b) \pmod p \right\}$$

Corollary: $\left(T_p f\right)(\tau) = \frac{1}{p} \sum_{j=0}^{p-1} f\left(\frac{\tau + j}{p}\right) + p^{k-1} f(p\tau)$

Corollary: If $f(q) = \sum_{n=1}^{\infty} a_n q^n$ is a (cusp form) q-expansion, then

$$\left(T_p f\right)(q) = \sum_{p \mid n} a_n q^{n/p} + p^{k-1} \sum a_n q^{np}$$

Note that, in particular, if $p \nmid n$, then $a_n(T_p f) = a_{pn}(f)$

This is proven by a direct calculation:

$$(T_p f)(\tau) = \frac{1}{p}\sum_{j=0}^{p-1} f\left(\frac{\tau+j}{p}\right) + p^{k-1} f(p\tau) = \frac{1}{p}\sum_{j=0}^{p-1}\sum_{n=0}^{\infty} a_n e^{2\pi i n\frac{\tau+j}{p}} + p^{k-1}\sum_{n=1}^{\infty} a_n e^{2\pi i n p\tau}$$

$$= \sum_{n=1}^{\infty} \frac{1}{p}\left(\sum_{j=0}^{p-1} e^{2\pi i \frac{n}{p} j}\right) a_n e^{2\pi i n\tau/p} + p^{k-1}\sum_{n=1}^{\infty} a_n e^{2\pi i n p\tau} =$$

$\left(\sum_{j=0}^{p-1} e^{2\pi i \frac{n}{p} j}\right)$: 0 if $p \nmid n$; p if $p \mid n$

$$= \sum_{n=1}^{\infty} a_n q^{n/p} + p^{k-1}\sum a_n q^{np} \quad //$$

We have a more general formula for the other Hecke operators:

$$a_n(T_m f) = \sum_{d \mid (m,n)} d^{k-1} a_{\frac{mn}{d^2}}(f)$$

In particular, if $n=1$:

$$a_1\left(T_m(f)\right) = a_m(f)$$

Def Let $\mathbb{T}_k$ be the $\mathbb{C}$-subalgebra of $\mathrm{End}_{\mathbb{C}}\left(S_k(Sl_2(\mathbb{Z}))\right)$ generated by the Hecke operators T_n $n=1,2,\ldots$

It is called the Hecke algebra (of weight k and level 1).

complex (could use the integral or rational, ...)

There is a bilinear pairing:

$$\langle \cdot, \cdot \rangle : \mathbb{T}_k \times S_k(SL_2(\mathbb{Z})) \longrightarrow \mathbb{C}$$
$$(T, f) \longmapsto a_1(T.f)$$

Claim: $\langle , \rangle$ is non-degenerate on the right; ie

if $\langle T, f \rangle = 0 \ \forall T \in \mathbb{T}$, then $f = 0$.

Pf/ $\langle T, f \rangle = 0 \ \forall T \Rightarrow \langle T_n, f \rangle = 0 \ \forall n \Rightarrow a_n(f) = 0 \ \forall n \geq 1 \Rightarrow f = 0$. ∎

Hence

$$S_k(SL_2(\mathbb{Z})) \hookrightarrow \mathbb{T}_k^{\vee} = \mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_k, \mathbb{C})$$

and so $\dim_{\mathbb{C}}(\mathbb{T}_k) \geq t = \dim_{\mathbb{C}} S_k(SL_2(\mathbb{Z}))$.

We will get more information on $\mathbb{T}_k$ in the following lectures.

Def: A modular form $f \in S_k(SL_2(\mathbb{Z}))$ is an <u>eigenform</u> if it is an eigenvector for <u>all</u> the T_n.

Rk: if we let λ_n be the eigenvalue of T_n acting on f, then

$$a_n(f) = \lambda_n a_1(f) \qquad (\text{as } a_n(f) = a_1(T_n f) = a_1(\lambda_n f)).$$

Hence: if f is an eigenform, $a_1(f) \neq 0$ (or $f = 0$) and so it can be scaled.

We say that f is <u>normalized</u> if $a_1(f) = 1$.

In this case, $T_n(f) = a_n(f) \cdot f$. (*)

We now get to the important theorem of Hecke:

Thm (Hecke): If $f = \sum a_n q^n$ is a normalized eigenform for T_k, then:

a) $a_{mn} = a_m a_n$ for $(m,n)=1$.

b) $a_{p^r} = a_p a_{p^{r-1}} - p^{k-1} a_{p^{r-2}}$

In particular,

c) $L(f,s) = \sum_{n\geq 1} a_n n^{-s} = \prod_p \left(1 - a_p p^{-s} + p^{k-1-2s}\right)^{-1}$.

Pf (a) and (b) are obvious from the corresponding statements for T_m, in light of (*)

For (c), multiplicativity (a).

$$\sum a_n n^{-s} = \prod_p \left(1 + a_p p^{-s} + a_{p^2} p^{-2s} + \cdots\right)$$

By (b), $\left(1 + a_p p^{-s} + a_{p^2} p^{-2s} + a_{p^3} p^{-3s} + \cdots\right)\left(1 - a_p p^{-s} + p^{k-1-2s}\right) = 1$

Rk: The converse is also true: properties (a), (b) imply that f is a normalized eigenform.

Example: $S_{12}(SL_2(\mathbb{Z})) = \mathbb{C}\Delta$, $\Delta = q\prod(1-q^n)^{24} = \sum \tau(n) q^n$

So $\sum \tau(n) n^{-s} = \prod_p \left(1 - \tau(p) p^{-s} + p^{11-2s}\right)^{-1}$

Q: How many eigenforms are there on $S_k(SL_2(\mathbb{Z}))$?

• Petersson scalar product.

We need the following lemma:

Lemma: If $f, g \in S_k(SL_2(\mathbb{Z}))$, then:

1) The function $G(\tau) = y^k f(\tau)\overline{g(\tau)}$ is invariant under $SL_2(\mathbb{Z})$.

2) The differential 2-form $\frac{dx\,dy}{y^2}$ on $\mathcal{H}$ is invariant under $SL_2(\mathbb{R})$.

Pf

- If $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $\quad y(\gamma\tau) = (c\tau+d)^{-1}(c\bar{\tau}+d)^{-1} y(\tau)$.

So (1) is clear.

For (2), note that $\frac{dx\,dy}{y^2} = \frac{i}{2}\frac{d\tau\, d\bar{\tau}}{y^2}$ and then it follows from $d(\gamma\tau) = \frac{d\tau}{(c\tau+d)^2}$. //

Def Define $\langle f, g\rangle := \int_{SL_2(\mathbb{Z})\backslash\mathcal{H}} y^k f(\tau)\overline{g(\tau)}\frac{dx\,dy}{y^2}$, the Petersson scalar product.

This is a Hermitian pairing on $S_k(SL_2(\mathbb{Z}))$ (in particular, non-degenerate)

Rk: it converges, even if one of f, g is not a cusp form (but problems arise if neither is a cusp form!).

Thm: The Hecke operators T_n are self-adjoint with respect to $\langle \cdot, \cdot \rangle$

Rk: in particular, it will imply that the T_n's are diagonalizable!

To prove the thm, we will use some previous result.

Lemma 1: Let $\alpha \in M_2(\mathbb{Z})$, $\det \alpha \neq 0$.

Then $G(\alpha\tau) = y^k \overline{(f|_k\alpha)(\tau)\cdot(g|_k\alpha)(\tau)}$

Pf/ A direct calculation//

If $f, g \in S_k(\Gamma)$, for $\Gamma \subseteq SL_2(\mathbb{Z})$ any subgroup, we will denote by:

$$\langle f, g\rangle_\Gamma := \int_{\Gamma\backslash\mathcal{H}} G(\tau)\,\frac{dxdy}{y^2}$$

Lemma 2: If $f, g \in S_k(\Gamma)$, then $f|_k\alpha, g|_k\alpha \in S_k(\alpha^{-1}\Gamma\alpha)$.

Then: $\langle f|\alpha, g|\alpha\rangle_{\alpha^{-1}\Gamma\alpha} = \langle f, g\rangle_\Gamma$

Pf/ A change of variables, using Lemma 1.//

Lemma 3: Suppose $f, g \in S_k(SL_2(\mathbb{Z}))$. Suppose $\Gamma \subseteq SL_2(\mathbb{Z}) \cap (\alpha^{-1}SL_2(\mathbb{Z})\alpha) \cap (\alpha SL_2(\mathbb{Z})\alpha^{-1})$

Then:

$$\langle f|\alpha, g\rangle_\Gamma = \langle f, g|\alpha^{-1}\rangle_\Gamma = \langle f, g|\alpha'\rangle_\Gamma$$

where $\alpha' := \alpha^{-1}\cdot\det(\alpha)$.

Pf/ Follows directly from Lemma 2.//

Now we have the tools to actually prove the theorem.

↓

Proof (of Thm):

It is enough to show that T_p (for p prime) is self-adjoint.

$$\langle T_p f, g \rangle_{SL_2(\mathbb{Z})} = \frac{1}{d} \langle T_p f, g \rangle_\Gamma \quad \text{if} \quad \Gamma \subseteq SL_2(\mathbb{Z}),\ [SL_2(\mathbb{Z}) : \Gamma] = d.$$

The last quantity is $= \frac{p^{\frac{k}{2}-1}}{d} \left\langle \sum_{j=1}^{p+1} f|\alpha_j , g \right\rangle_\Gamma$

where $SL_2(\mathbb{Z}) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} SL_2(\mathbb{Z}) = \bigsqcup_{j=1}^{p+1} SL_2(\mathbb{Z}) \alpha_j$

Choose Γ so that $\Gamma \subseteq SL_2(\mathbb{Z}) \cap \left(\alpha_j SL_2(\mathbb{Z}) \alpha_j^{-1}\right) \cap \left(\alpha_j^{-1} SL_2(\mathbb{Z}) \alpha_j\right)$

(eg. $\Gamma := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{p} \right\}$ works).

We can then move α_j's to the other side:

$$= \frac{p^{\frac{k}{2}-1}}{d} \sum_{j=1}^{p+1} \langle f, g|\alpha_j' \rangle_\Gamma$$

However, in principle the α_j' are a set of right coset reps, not left!

Lemma: There exists $\{\alpha_1, \dots, \alpha_{p+1}\}$ such that

$$SL_2(\mathbb{Z}) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} SL_2(\mathbb{Z}) = \bigcup SL_2(\mathbb{Z}) \alpha_j = \bigcup SL_2(\mathbb{Z}) \alpha_j'$$

Pf Write $SL_2(\mathbb{Z}) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} SL_2(\mathbb{Z}) = \bigcup_{j=1}^{p+1} L_j = \bigcup_{j=1}^{p+1} R_j$ (left cosets / right cosets)

(Rk: Check that $\left\{ \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \right\} \cup \left\{ \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right\}$ do not have the property of the lemma).

Note that $L_j \cap R_j \neq \emptyset$ for all j. Then choose, for each j, $\alpha_j \in L_j \cap R_j$. Now $\bigcup \alpha_j SL_2(\mathbb{Z}) = \bigcup SL_2(\mathbb{Z}) \alpha_j'$. //

Exercise: find such a system $\{\alpha_1, \dots, \alpha_{p+1}\}$.

(continues proof)

Then $$\frac{1}{d} p^{\frac{k}{2}-1} \sum \langle f, g|\alpha_j' \rangle_\Gamma = \frac{1}{d} \langle f, T_p g \rangle_\Gamma = \langle f, T_p g \rangle_{SL_2(\mathbb{Z})}.$$

Corollary:

1) $S_k(SL_2(\mathbb{Z}))$ has a (canonical) basis of normalized eigenforms.

2) $\mathbb{T}_k \simeq \mathbb{C}^d$ as a $\mathbb{C}$-algebra, where $d = \dim_{\mathbb{C}} S_k(SL_2(\mathbb{Z}))$.
(i.e. $\mathbb{T}_k$ has a basis of simultaneous eigenforms for all the T_n's).

pf

1) $S_k(SL_2(\mathbb{Z})) = \bigoplus_{f \text{ eigenforms}} V^f = \bigoplus_{i=1}^{d} \mathbb{C} f_i$ b/c V^f are all 1-dimensional

2) is obvious.

Remark: $\mathbb{T}_k = \mathrm{Hom}_{\mathbb{C}}(S_k(SL_2(\mathbb{Z})), \mathbb{C})$ as vector spaces, or

equivalently, $S_k(SL_2(\mathbb{Z})) = \mathrm{Hom}_{\mathbb{C}}(\mathbb{T}_k, \mathbb{C})$.

$$\left\{ \begin{array}{l} \text{normalized} \\ \text{eigenforms in} \\ S_k(SL_2(\mathbb{Z})) \end{array} \right\} = \mathrm{Hom}_{\mathbb{C}\text{-alg}}(\mathbb{T}_k, \mathbb{C}) = \mathrm{Spec}(\mathbb{T}_k)$$

(an integral domain over a field k which is finite dim as k-algebra is also a field.)

• Rationality properties of the Fourier coeffs of eigenforms.

Recall that $S_k(SL_2(\mathbb{Z}))$ has a basis consisting of modular forms with rational q-expansions.

Define then $S_k(SL_2(\mathbb{Z}), \mathbb{Q}) :=$ modular forms with rational q-exps $\overset{\mathbb{Q}\text{-vect sp}}{\simeq} \mathbb{Q}^d$

Note that T_n acts on $S_k(SL_2(\mathbb{Z}), \mathbb{Q})$, and hence the eigenvalues of T_n are algebraic numbers of degree $\leq d$.

Let then:

Def $T_{n,\mathbb{Q}} :=$ sub-$\mathbb{Q}$-algebra of $\mathrm{End}_{\mathbb{Q}}\left(S_k(SL_2(\mathbb{Z}), \mathbb{Q})\right)$ generated by $\{T_n\}$.

Then $T_{n,\mathbb{Q}} \simeq \bigoplus_{i=1}^{t} F_i$, where the F_i's are number fields.

- $\sum_{i=1}^{t} [F_i : \mathbb{Q}] = d$
- The F_i's are totally real.

  (because F_i's are generated by eigenvalues of some T_n, and these are real by Hermitianity of T_n).

Q: What if $SL_2(\mathbb{Z})$ is replaced by $\Gamma = \Gamma_0(N)$?

Prop: The Hecke operators T_n for $(n, N) = 1$ are self-adjoint for $\langle \cdot, \cdot \rangle_\Gamma$

Ref: Exercise.pp

Rk: It is crucial to take $(n, N) = 1$!

Define by $\mathbb{T}' :=$ algebra generated by $\{T_n : (n,N)=1\}$.

As before,

$$S_k(\Gamma_0(N)) = \bigoplus_{i=1}^{t} V_i$$

where V_i is a $\mathbb{T}'$-eigenspace. (but now $\dim V_i$ may not be 1 !)

Suppose that $f, g \in V_i$. Then:

$$a_n(f) = \lambda_n a_1(f) \quad \forall (n,N)=1$$
$$a_n(g) = \lambda_n a_1(g) \quad \forall (n,N)=1$$

But $a_1(f)$ may be 0! (without f being 0). Or even if $a_1(f)=a_1(g)$, not necessarily $f=g$.

Example: an (obvious) way of constructing V_i of $\dim V_i > 1$:

Let $f \in S_k(\Gamma_0(d))$, $d' d \mid N$.

Then $f(d'\tau) \in S_k(\Gamma_0(N))$

Lemma: If $f \in S_k(\Gamma_0(d))$ (is an eigenform), then $\{f(d'\tau) : d' \mid \frac{N}{d}\}$ belongs to a common eigenspace for $\mathbb{T}'$.

Pf/ Exercise.

Atkin-Lehner Theory:

Def: Let $S_k^{old}(\Gamma_0(N)) := \mathrm{Span}\langle \{f(d'\tau) : f \in S_k(\Gamma_0(d)),\ d \mid N,\ d \neq N,\ d' \mid \frac{N}{d}\} \rangle$

Define then $S_k^{new}(\Gamma_0(N)) := \left(S_k^{old}(\Gamma_0(N))\right)^{\perp}$ wrt Petersson scalar product.

The main result, which we won't prove, is:

Theorem (Atkin-Lehner):

$$S_k^{\text{new}}(\Gamma_0(N)) = \bigoplus_{i=1}^{d} \mathbb{C} f_i$$

where the f_i's are normalized eigenforms, and each $\mathbb{C} f_i$ is a T'-eigenspace.

Pf/ Omitted //.

The f_i's appearing in the previous theorem are called **newforms**.

(So f newform $\Leftrightarrow$ eigenform in $S_k^{\text{new}}(\Gamma_0(N))$, which is normalized).

Consequence: if f is a newform in $S_k^{\text{new}}(\Gamma_0(N))$, then

$$W_N : \mathbb{C} f \longrightarrow \mathbb{C} f$$

and so $W_N(f) = w \cdot f$, where $w \in \{+1, -1\}$.

- **Important Special Case.**

$k=2$. So consider $S_2^{\text{new}}(\Gamma_0(N))$.

The Modularity Theorem (Shimura Taniyama conj, Wiles Theorem):

Let $E/\mathbb{Q}$ be an elliptic curve. Let N be its conductor. (reduced curve $E \pmod p$)

($p \mid N \Leftrightarrow E$ has bad reduction at p], and for $p>3$, have $\begin{cases} \propto \Rightarrow p \| N \\ \prec \Rightarrow p^2 \| N \end{cases}$)

Then $\exists$ a newform $f \in S_2^{\text{new}}(\Gamma_0(N))$ such that

$$L(E,s) = L(f,s)$$

Proof: no way in this course :) //

Applications (of Modularity)

1) Remark: if E_1, E_2 are two elliptic curves $/\mathbb{Q}$ with $L(E_1,s) = L(E_2,s)$, then these two elliptic curves are isogenous: $E_1 \underset{\text{isog. over } \mathbb{Q}}{\sim} E_2$

(i.e. $\exists\ \varphi : E_1 \to E_2$ with finite kernel).

(Result of Faltings, known as the isogeny conjecture).

2) There is a bijection:

$$\left\{\begin{array}{l}\text{isogeny classes of} \\ \text{elliptic curves of conductor } N\end{array}\right\} \quad \underset{\text{Eichler-Shimura}}{\overset{\text{Wiles}}{\overset{\curvearrowright}{\underset{\curvearrowleft}{1:1}}}} \quad \left\{\begin{array}{l}\text{newforms in} \\ S_2^{\text{new}}(\Gamma_0(N)) \\ \text{with rational Fourier coeffs}\end{array}\right\} = \text{Hom}_{\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}\left(T_{\mathbb{Q},2,N}, \mathbb{Q}\right)$$

number fields $\neq \mathbb{Q}$.

So if we write $T_{\mathbb{Q},2,N} \simeq \mathbb{Q}^a \times F_1 \times \cdots \times F_s$

then $a = \#\{\text{isogeny classes of } E/\mathbb{Q}\}$.

3) Write $\Lambda(E,s) = (2\pi)^{-s}\Gamma(s)L(E,s)$.

Then $\Lambda(E,s) = -w \cdot N^{1-s}\Lambda(E,2-s)$ (thanks to the connection with modular forms)

The Birch-Swinnerton-Dyer conjecture says that

$$\text{ord}_{s=1} L(E,s) = \text{rank}\left(E(\mathbb{Q})\right).$$

Thus now makes sense, as $L(E,s)$ is meromorphic at $s=1$ ($\zeta(s)$ is not).

Twisting of L-series

Let χ be a Dirichlet character of ~~conductor~~ period m.

(so $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$, and is extended to $\mathbb{Z}$ by $\chi(n) = \begin{cases} 0 & (n,m) > 1 \\ \chi(\bar{n}) & (n,m) = 1 \end{cases}$)

We make the further assumption that χ is a primitive Dirichlet char.

(that is, $\nexists\, \chi'$ of ~~conductor~~ period $d \mid m$, $d \neq m$ s.t. $\chi(n) = \chi'(n)\ \forall (n,m) = 1$).

In this case, one calls m the level of χ.

Def: The twisted L-series attached to $f = \sum a_n q^n$ and χ is:

$$L(f, \chi, s) = \sum_{n=1}^{\infty} a_n \chi(n) n^{-s}$$

We want to extend the Hecke theory to the twisted L-series.

Q: integral representation of $L(f, \chi, s)$?

Lemma:
$$\int_0^\infty f\left(\frac{a}{m} + it\right) t^s \frac{dt}{t} = (2\pi)^{-s} \Gamma(s) \left(\sum_{n=1}^{\infty} a_n e^{2\pi i \frac{a}{m} n} n^{-s} \right)$$

if $\frac{a}{m}$ is any rational number ((a,m) not necessarily 1).

Rx: when $a = 0$, this is just the integral representation of $L(f,s)$ given earlier.

pf
$$\int_0^\infty f\left(\tfrac{a}{m} + it\right) t^s \frac{dt}{t} = \int_0^\infty \sum_{n=1}^{\infty} a_n e^{2\pi i n \left(\frac{a}{m} + it\right)} t^s \frac{dt}{t} =$$

$$= \sum_{n=1}^{\infty} a_n e^{2\pi i \frac{a}{m} n} \int_0^\infty e^{-2\pi n t} t^s \frac{dt}{t} = (2\pi)^{-s} \Gamma(s) \sum_{n=1}^{\infty} a_n e^{2\pi i \frac{a}{m} n} n^{-s}$$

//

Remark: The function $n \mapsto e^{2\pi i \frac{a}{m} n}$ is an additive character on $\mathbb{Z}/m\mathbb{Z}$. Let $\psi_a(n) := e^{2\pi i \frac{a}{m} n}$

Let $L(f, \psi_a, s) := \sum_n a_n \psi_a(n) n^{-s}$.

The problem now is to express $L(f, \chi, s)$ as a (linear) combination of different $L(f, \psi_a, s)$. This is a problem in Fourier analysis.

It is enough to express χ as a linear combination of the ψ_a's.

Fourier analysis on $(\mathbb{Z}/m\mathbb{Z}, +)$

Write $L^2(\mathbb{Z}/m\mathbb{Z}) := \{\mathbb{C}\text{-valued functions on } \mathbb{Z}/m\mathbb{Z}\}$.

$\langle f, g \rangle := \frac{1}{m} \sum_{j=0}^{m-1} f(j) \overline{g(j)}$ gives $L^2(\mathbb{Z}/m\mathbb{Z})$ the structure of a Hilbert space,

and $\{\psi_0, \psi_1, \dots, \psi_{m-1}\}$ are an orthonormal basis for $L^2(\mathbb{Z}/m\mathbb{Z})$.

So $\chi = \sum_{a=0}^{m-1} \underbrace{\langle \chi, \psi_a \rangle}_{\text{Gauss sums!}} \cdot \psi_a$

Def: The complex number $\tau_a(\chi) := m \cdot \langle \chi, \psi_a \rangle = \sum_{j=0}^{m-1} \chi(j) e^{-2\pi i \frac{a}{m} j}$ is called the Gauss sum associated to χ and a.

Proposition:

1) If $\lambda \in (\mathbb{Z}/m\mathbb{Z})^\times$, then $\tau_{\lambda a}(\chi) = \overline{\chi(\lambda)}\,\tau_a(\chi)$.

2) If $(a,m) \neq 1$, then $\tau_a(\chi) = 0$.

Pf

1) $\tau_{\lambda a}(\chi) = \sum_{j=0}^{m-1} \chi(j)\, e^{-2\pi i \frac{\lambda a}{m} j} \overset{\text{change } j \rightsquigarrow \lambda' j}{=} \sum_{j=0}^{m-1} \chi(\lambda' j)\, e^{-2\pi i \frac{a}{m} j}$

and just note that, if $\lambda' \equiv \lambda^{-1} \pmod m$, then $\chi(\lambda') = \overline{\chi(\lambda)}$.

2) If $d := (a,m)$, then $\lambda a \equiv a \pmod m$ $\forall \lambda \equiv 1 \pmod{m/d}$.

Using (1), have:

$$\tau_{\lambda a}(\chi) = \tau_a(\chi) \quad \forall \lambda \equiv 1 \pmod{m/d} \Rightarrow \overline{\chi(\lambda)}\,\tau_a(\chi) = \tau_a(\chi) \quad \forall \lambda \equiv 1 \pmod{m/a}$$

$\Rightarrow \overline{\chi(\lambda)} = 1$ $\forall \lambda \equiv 1 \pmod{m/a}$ (if $\tau_a(\chi) \neq 0$)

This contradicts the primitivity of χ. So $\tau_a(\chi) = 0$.

So it is enough to know about $\tau(\chi) := \tau_1(\chi)$.

Corollary: $\chi = \frac{1}{m}\,\tau(\chi) \sum_{a=0}^{m-1} \overline{\chi(a)}\,\psi_a$

Hence: $L(f\chi, s) = \frac{1}{m}\,\tau(\chi) \sum_{a=0}^{m-1} \overline{\chi(a)}\, L(f, \psi_a, s)$

and this gives: $\sum_{(a,m)=1}$ ← by (2) of Prop.

$$\Lambda(f, \chi, s) = \frac{1}{m}\,\tau(\chi) \sum_{\substack{a=0 \\ (a,m)=1}}^{m-1} \overline{\chi(a)} \int_0^\infty f\left(\frac{a}{m} + it\right) t^s \frac{dt}{t}$$

(integral expression for the twisted L-series).

We want to use the integral representation to get a functional equation for $L(f,x,s)$. $\left(\Lambda(f,x,s) = (2\pi)^{-s}\Gamma(s)L(f,x,s)\right)$.

Functional Equation We have: (assume $\gcd(m,N)=1$)

$$\Lambda(f,x,s) = \frac{\tau(x)}{\tau(\bar{x})} i^k N^{\frac{k}{2}-s} \Lambda(f,\bar{x},k-s)$$

Goal: prove this.

We need to rewrite $\int_0^\infty f\left(\frac{a}{m}+it\right)t^s\frac{dt}{t}$

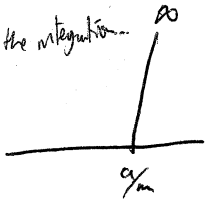
Note that

$$\int_0^\infty f\left(\frac{a}{m}+it\right)t^s\frac{dt}{t} = w\int_0^\infty (f|\gamma)\left(\frac{a}{m}+it\right)t^s\frac{dt}{t}$$

where γ is any matrix of the form $\begin{pmatrix} r & s \\ tN & u\end{pmatrix}\begin{pmatrix} 0 & -1 \\ N & 0\end{pmatrix}$ $\in \Gamma_0(N)$

nothing to do with the integration...

We need $rm - stN = 1$

We need that our γ moves the line  to some other vertical line.

Need to require that $\gamma\frac{a}{m} = \infty$ (then it will send ∞ to $\frac{s}{u}$)

$$\gamma = \begin{pmatrix} sN & -r \\ uN & -tN\end{pmatrix}$$

We want $\gamma = \begin{pmatrix} sN & -r \\ mN & -aN\end{pmatrix}$. The $\det = N$ condition is:

$$-asN + rm = 1.$$

To solve this equation (in r,s), write $s = a'$, where a' is any solution of $(-aN)a' \equiv 1 \pmod m$.

Set then r to be the solution to the resulting equation

We find that $\gamma = \begin{pmatrix} a'N & -r \\ mN & -aN \end{pmatrix}$

Lemma: $\Lambda\left(f, \frac{a}{m}, s\right) = w \cdot (Nm)^{\frac{k}{2}-s}\, i^{-k}\, \Lambda\left(f, \frac{a'}{m}, k-s\right)$

where * $w \cdot f = W_N(f)$ $\quad (w \in \{\pm 1\})$

* $a' \in \mathbb{Z}$ is any integer s.t. $a'(-Na) \equiv 1 \pmod{m}$.

Pf

$$\Lambda\left(f, \tfrac{a}{m}, s\right) = \int_0^\infty f\left(\tfrac{a}{m} + it\right) t^s \frac{dt}{t}$$

Let $\gamma = \begin{pmatrix} a'N & -r \\ mN & -aN \end{pmatrix} \in \Gamma_0(N) \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$

where r is chosen s.t. $\det \gamma = N$ $\quad (-aa'N + rm = 1)$

Hence:

$$\Lambda\left(f, \tfrac{a}{m}, s\right) = w \int_0^\infty (f|\gamma)\left(\tfrac{a}{m} + it\right) t^s \frac{dt}{t} = w \cdot \int_0^\infty N^{\frac{k}{2}} (mNit)^{-k} f\left(\tfrac{a'}{m} + \tfrac{i}{m^2 N t}\right) t^s \frac{dt}{t}$$

$$= w N^{-\frac{k}{2}} m^{-k} i^{-k} \int_0^\infty t^{-k} f\left(\frac{a'}{m} + \frac{i}{m^2 N} t^{-1}\right) t^s \frac{dt}{t}.$$

Change $t = \frac{1}{m^2 N y}$, and get $= w N^{\frac{k}{2}-s} m^{k-2s} i^{-k} \int_0^\infty f\left(\frac{a'}{m} + iy\right) y^{k-s} \frac{dy}{y}$ //

Theorem (Functional equation for $L(f, \chi, s)$:

$$\Lambda(f, \chi, s) = \underline{i^{-k} w \chi(-N)} \frac{\tau(\chi)}{\tau(\bar{\chi})} (N m^2)^{\frac{k}{2}-s} \Lambda(f, \bar{\chi}, k-s)$$

↑ called the root number (± 1)
(at least, for even k, and χ quadratic)

Pf $\Lambda(f, \chi, s) = \frac{\tau(\chi)}{m} \sum_{a=0}^{m-1} \bar{\chi}(a) \Lambda\left(f, \frac{a}{m}, s\right) \overset{\text{lemma}}{=} \cdots$ //

Corollary: Suppose that f is of weight 2, and χ is a quadratic character.

Then, if $-w\chi(-N) = -1$, then $\Lambda(f,\chi,1) = 0$. !

Arithmetic meaning of twisting.

First, note that $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^\times$ canonically, ($\zeta_m = e^{\frac{2\pi i}{m}}$)

$$[\zeta \mapsto \zeta^a] \longleftrightarrow a$$

so that χ can be thought of $\chi : \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \to \mathbb{C}^\times$

Assume now that $f \in S_2(\Gamma_0(N))$ is a newform, and also assume that f corresponds (via ~~Atkin-Lehner~~-Shimura-Taniyama corresp.) to an elliptic curve $E/\mathbb{Q}$.

Birch-Swinnerton-Dyer Conjecture (twisted form). (E has a Galois action (b/c E is def/$\mathbb{Q}$))

$$\mathrm{ord}_{s=1} L(f,\chi,s) = \dim_{\mathbb{C}} \left(E(\mathbb{Q}(\zeta_m)) \otimes_{\mathbb{Z}} \mathbb{C} \right)^\chi \quad \text{(conjecture)}$$

where $\left(E(\mathbb{Q}(\zeta_m)) \otimes_{\mathbb{Z}} \mathbb{C} \right)^\chi = \{ P \in E(\mathbb{Q}(\zeta_m)) \otimes_{\mathbb{Z}} \mathbb{C} : \sigma P = \chi(\sigma) \cdot P \ \forall \sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \}$.

The collection of special values

$$\{ L(f,\chi,1) \}_{\chi \in \{\text{all Dirichlet characters of conductor prime to } N = \text{level of } f\}}$$

carries a tremendous amount of arithmetic information.

The study of this leads to the p-adic L-series, as we will see.

Theorem (Shimura)

Let $f \in S_2(\Gamma_0(N))$ a newform corresponding to $E/\mathbb{Q}$ (so $f = \sum a_n q^n$, $a_n \in \mathbb{Z}$, $a_1 = 1$)

There exists a lattice $\Lambda_f \subseteq \mathbb{C}$ such that:

$$\Lambda(f, \alpha, 1) \in \Lambda_f \quad \text{for all } \alpha \in \mathbb{Q}.$$

More precisely, one can choose $\Lambda_f = \mathbb{Z}\,\Omega_f^+ \oplus i\,\mathbb{Z}\,\Omega_f^-$ (rectangular lattice)

and $\Lambda(f,\alpha,1) = \Omega_f^+ \Lambda^+(f,\alpha,1) + i\,\Omega_f^- \Lambda^-(f,\alpha,1)$

(where $\Lambda^{\pm}(f,\alpha,1)$ are integers).

We will prove this theorem using first some lemmas.

Lemma: $\Lambda(f, \frac{a}{m}, 1) = \frac{-1}{2\pi} \int_{[\frac{a}{m}, i\infty]} \omega_f$

where $[\frac{a}{m}, i\infty]$ = the path in $\mathcal{H}$ = upper half-plane going from $\frac{a}{m}$ to $i\infty$

and $\omega_f = 2\pi i f(z)\,dz \in \Omega^1(X_0(N)(\mathbb{C}))$

Pf Just a change of variables, using the integral representation for $\Lambda(f, \frac{a}{m}, 1)$ //

So now it is enough to show that there is a lattice Λ_f such that $\int_{[\frac{a}{m}, i\infty)} \omega_f \in \Lambda_f$.

geodesics

We replace $[\frac{a}{m}, i\infty] = [\frac{a}{m}, 0] + [0, i\infty]$.

Then $[\frac{a}{m}, 0]$ will be a closed path, and $[0, i\infty]$ doesn't depend on $\frac{a}{m}$!

(in $X_0(N)(\mathbb{C})$).

We will need to assume $(m, N) = 1$, which is fine if we are interested in χ of conductor coprime to N.

Remark: • The theorem of Shimura is also valid for $(m, N) > 1$ as well, but we will do it only for $(m, N) = 1$.

• The theorem can be extended to $S_k(\Gamma_0(N))$ $(k \neq 2)$, but we don't get into it for now.

We have a pairing:

$$H^1_{dR}(X_0(N)(\mathbb{C})) \times H_1(X_0(N)(\mathbb{C}), \mathbb{C}) \longrightarrow \mathbb{C}$$

$$([\omega], \gamma) \longmapsto \int_\gamma \omega$$

or algebraically,

$H^1_{dR}(X_0(N))$ is defined to be the space of closed (algebraic) differential forms of the second kind (modulo exactness).

(and second kind means that $\mathrm{Res}_P(\omega) = 0 \ \forall P$).

(so we admit singularities, but those singularities won't affect the integration)

Let then $\Omega^1(X_0(N))$ = space of closed complex differentials regular (i.e holomorphic) everywhere

the only exact diffs which "are" holomorphic everywhere "are" the 0.

So we have an exact sequence:

$$0 \longrightarrow \Omega^1(X_0(N)) \longrightarrow H^1_{dR}(X_0(N)) \longrightarrow H^1(X_0(N), \mathcal{O}_{X_0(N)}) \longrightarrow 0.$$

This 0 called a Hodge filtration.

Serre duality says that $\left(\Omega^1(X_0(N))\right)^\vee = H^1\left(X_0(N), \mathcal{O}_{X_0(N)}\right)$.

To represent $H^1_{dR}(X_0(N))$, we write $X_0(N) = U \cup V$ (two Zariski opens)

and $H^1_{dR}(X_0(N)) = \left\{ (\omega_U, \omega_V, f) : \omega_U \in \Omega^1(U),\ \omega_V \in \Omega^1(V),\ \omega_U - \omega_V = df \text{ in } U \cap V \right\}$
$f \in \mathcal{O}_{U \cap V}$

The map $H^1_{dR}(X_0(N)) \to H^1\left(X_0(N), \mathcal{O}_{X_0(N)}\right)$ is defined by

$$(\omega_U, \omega_V, f) \mapsto f$$

and $\omega \in \Omega^1(X_0(N)(\mathbb{C}))$ gets sent to $(\omega|_U, \omega|_V, 0)$.

$\longleftarrow$

Let now $K_f :=$ field generated by $a_n(f)$, $n = 1, 2, \ldots$

where $f \in S_2(\Gamma_0(N))$ is a newform (normalised eigen. in S_2^{new}).

Let $\mathcal{O}_f :=$ ring of integers of K_f.

We know that $[K_f : \mathbb{Q}] < \infty$ and K_f is totally-real.

In fact, also $a_n(f) \in \mathcal{O}_f$: this is because $S_2\left(\Gamma_0(N), \mathbb{Z}\right)$ is preserved by the Hecke operators.

Define $\Lambda^+\left(f, \frac{a}{m}, 1\right) := \Lambda\left(f, \frac{a}{m}, 1\right) + \Lambda\left(f, -\frac{a}{m}, 1\right)$

$$\Lambda^-\left(f, \frac{a}{m}, 1\right) := \Lambda\left(f, \frac{a}{m}, 1\right) - \Lambda\left(f, -\frac{a}{m}, 1\right)$$

This allows us to state the theorem we mentioned before:

$\downarrow$

Theorem: There exists $\Omega^+ \in \mathbb{R}$, $\Omega^- \in i\mathbb{R}$ such that: (Shimura)

$$\Lambda^+\left(f, \tfrac{a}{m}, 1\right) \in \Omega^+ \mathcal{O}_f$$
$$\Lambda^-\left(f, \tfrac{a}{m}, 1\right) \in \Omega^- \mathcal{O}_f \qquad \forall \tfrac{a}{m} \in \mathbb{Q}.$$

Proof:

From the theory of Riemann Surfaces: let X be any compact R.S of genus g.

$\Omega^1(X)$ = Holomorphic differentials on $X \simeq \mathbb{C}^g$

$$\Omega^1(X)^\vee := \mathrm{Hom}_{\mathbb{C}}(\Omega^1(X), \mathbb{C})$$

$$H_1(X,\mathbb{Z}) \hookrightarrow \Omega^1(X)^\vee$$
$$\gamma \longmapsto [\omega \mapsto \textstyle\int_\gamma \omega]$$

Fact: The previous map is injective, and the image of $H_1(X,\mathbb{Z})$ is a lattice in $\Omega^1(X)^\vee \simeq \mathbb{C}^g$. $\left(\text{So } H_1(X,\mathbb{Z}) \simeq \mathbb{Z}^{2g}\right)$.

In particular, if $X = X_0(N)(\mathbb{C})$, we have a lattice

$$\Lambda \subseteq \Omega^1(X)^\vee = S_2(\Gamma_0(N))^\vee.$$
$$\| $$
$$H_1(X_0(N)(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}^{2g} \quad \text{where} \quad g = \dim_{\mathbb{C}}\left(S_2(\Gamma_0(N))\right).$$

We need a result:

Prop: The lattice Λ is preserved by the action of the T_n, $(n,N)=1$.

Pf Given $\gamma \in H_1(X,\mathbb{Z})$, let $\varphi_\gamma(\omega) = \int_\gamma \omega$.

Then $\varphi_\gamma \in S_2(\Gamma_0(N))^\vee$. So $T_n(\varphi_\gamma)(\omega) = \int_\gamma (\omega | T_n)$

Recall $\Gamma_0(N)\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}\Gamma_0(N) = \bigcup_{i=1}^{t} \Gamma_0(N)\alpha_i$

The group $\Gamma_0(N)$ acts transitively on the set of t cosets (by right mult).

(cont pf of Prop)

Note that $\int_\gamma \omega = \int_{z_0}^{\gamma z_0} \omega$ (different paths) for some $\gamma \in \Gamma_0(N)$

because $\mathcal{H}^* \longrightarrow X_0(N)(\mathbb{C})$ is a covering space, and $\mathcal{H}^*$ is simply connected.

Hence if $P \in X_0(N)(\mathbb{C})$ and z_0 is a lift $(z_0 \mapsto P)$,

A path (γ) in $X_0(N)(\mathbb{C})$ lifts uniquely to a path starting at z_0, and ending at z_0' (s.t $z_0' \mapsto P$ as well).

Hence $\gamma z_0 = z_0'$ for some $\gamma \in \Gamma_0(N)$.

We can now partition $\Gamma_0(N)\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}\Gamma_0(N) = \coprod_{i=1}^{r} \left(\Gamma_0(N)\alpha_i \sqcup \Gamma_0(N)\alpha_i\gamma \sqcup \cdots \sqcup \Gamma_0(N)\alpha_i\gamma^{t_i-1} \right)$

where t_i is the smallest integer >1 s.t $\Gamma_0(N)\alpha_i = \Gamma_0(N)\alpha_i\gamma^{t_i}$.

That is, $\alpha_i \gamma^{t_i} \alpha_i^{-1} \in \Gamma_0(N)$

Now write

$$\int_\gamma \omega|T_n = \int_{z_0}^{\gamma z_0} \omega|T_n = \sum_{i=1}^{r} \int_{z_0}^{\gamma z_0} (\omega|\alpha_i + \omega|\alpha_i\gamma + \cdots + \omega|\alpha_i\gamma^{t_i-1}) = \left[\begin{matrix}\text{change} \\ \text{variables}\end{matrix}\right]$$

$$= \sum_{i=1}^{r} \int_{\alpha_i z_0}^{\alpha_i \gamma z_0} \omega + \int_{\alpha_i\gamma z_0}^{\alpha_i\gamma^2 z_0} \omega + \cdots + \int_{\alpha_i\gamma^{t_i-1} z_0}^{\alpha_i \gamma^{t_i} z_0} \omega = \sum_{i=1}^{r} \int_{\alpha_i z_0}^{\alpha_i \gamma^{t_i} z_0} \omega =$$

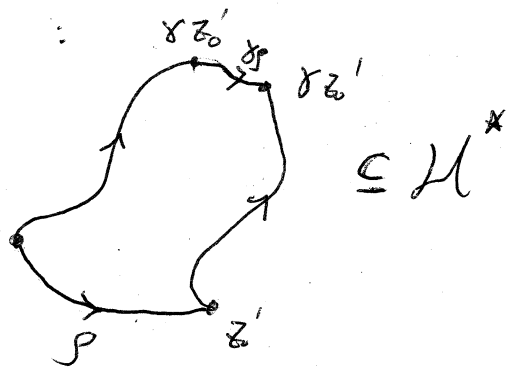
$$= \sum_{i=1}^{r} \int_{\alpha_i z_0}^{(\alpha_i\gamma^{t_i}\alpha_i^{-1})\alpha_i z_0} \omega \overset{\alpha_i\gamma^{t_i}\alpha_i^{-1} \in \Gamma_0(N)}{=} \sum_{i=1}^{r} \int_{z_0}^{\alpha_i\gamma^{t_i}\alpha_i^{-1} z_0} \omega = \left(\sum_{i=1}^{r} \varphi_{\alpha_i\gamma^{t_i}\alpha_i^{-1}}\right)(\omega)$$

$\in \Lambda$. //

Remark: $\int_{z_0}^{\gamma z_0} \omega = \int_{z_0'}^{\gamma z_0'} \omega$ if $\gamma \in \Gamma_0(N)$:

$$\int_{z_0}^{\gamma z_0} \omega - \int_{z_0'}^{\gamma z_0'} \omega = \int_{\gamma\rho} \omega - \int_{\rho} \omega = 0 \quad \checkmark$$

($\gamma \in \Gamma_0(N)$ — change variable).



$\subseteq \mathcal{H}^*$

We now continue the proof of the theorem of Shimura.

Choose a basis $\{f_1, \dots, f_g\}$ of $S_2(\Gamma_0(N))$ consisting of modular forms with real Fourier coefficients (could take them rational!).

(it's a fact that $S_2(\Gamma_0(N), \mathbb{Q}) \simeq \mathbb{Q}^g$ — use Eisenstein series, ...).

We get then an identification:

$$S_2(\Gamma_0(N))^\vee \xrightarrow{\sim} \mathbb{C}^g$$
$$\lambda \longmapsto (\lambda(f_1), \dots, \lambda(f_g)).$$

Let $c : S_2(\Gamma_0(N))^\vee \to S_2(\Gamma_0(N))^\vee$ be the involution induced by complex conjugation on $\mathbb{C}^g$.

Prop: Λ is stable under c, and moreover c commutes with the T_n.

Pf $(c(\varphi_\gamma))(\omega) = \overline{\int_\gamma \omega} \overset{\omega = 2\pi i f(z) dz}{=} \overline{\int_{z_0}^{\gamma z_0} 2\pi i f(z) dz} \overset{\text{if } f \text{ has real Fourier coeffs} \Rightarrow \overline{f(z)} = f(-\bar{z})}{=} \int_{z_0}^{\gamma z_0} -2\pi i f(-\bar{z}) d\bar{z} =$

$$= \int_{z_0}^{\gamma z_0} 2\pi i f(-\bar{z}) d\bar{z} = \int_{-\bar{z}_0}^{\gamma' \cdot -\bar{z}_0} 2\pi i f(z) dz$$

where $\gamma' = \begin{pmatrix} a & -b \\ -c & d \end{pmatrix} \in \Gamma_0(N)$ also!

(if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$)

$$= \varphi_{\gamma'}(\omega_f) \quad //$$

(Cont pf of Prop)

Now we need to see that c commutes with T_n.

This is an exercise :) //

Define now $\Lambda_{\mathbb{Q}} := \Lambda \otimes_{\mathbb{Z}} \mathbb{Q} \simeq \mathbb{Q}^{2g}$.

One can decompose $\Lambda_{\mathbb{Q}} = \Lambda_{\mathbb{Q}}^+ \oplus \Lambda_{\mathbb{Q}}^-$ where c acts as

1 (resp -1) in $\Lambda_{\mathbb{Q}}^+$ (resp $\Lambda_{\mathbb{Q}}^-$).

As c commutes with T_n, then T_n's respect the $\Lambda_{\mathbb{Q}}^+$ and $\Lambda_{\mathbb{Q}}^-$.

Note: $\Lambda \supset \Lambda^+ \oplus \Lambda^-$ with finite index (at most 2^g).

Recall $\mathbb{T}_{\mathbb{Z}}$ = $\mathbb{Z}$-algebra generated by the matrices $T_1, T_2, \dots$, $(n,N)=1$ acting on $S_2(\Gamma_0(N))$.

A newform f gives rise to $\varphi_f : \mathbb{T}_{\mathbb{Z}} \longrightarrow \mathcal{O}_f$, $T_n \longmapsto a_n(f)$

Let $I_f := \operatorname{Ker} \varphi_f$.

Lemma: 1) $\Lambda_{\mathbb{Q}}^{\pm}[I_f]$ (module annihilated by I_f) is a one dimensional K_f-vectorspace.

(note that the action of $\mathbb{T}_{\mathbb{Q}}$ factors through I_f, and $\mathbb{T}_{\mathbb{Q}}/I_f \simeq K_f$).

2) $\Lambda_{\mathbb{Q}}^{\pm}/I_f \simeq K_f$ as a K_f-vectorspace.

3) $\Lambda_{\mathbb{Z}}^{\pm}/I_f \subseteq \Lambda_{\mathbb{Q}}^{\pm}/I_f$ is a $\mathbb{Z}$-lattice (so of rk $= d = [K_f : \mathbb{Q}]$).

$\simeq K_f$

Pf (of Lemma) Use primary decomposition:

$T_{\mathcal{A}} \simeq K_f \oplus T'$. So have an idempotent π_f (corresp to $(1,0)$).

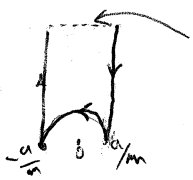
$\Rightarrow \exists\, n_f \in \mathbb{Z}$ s.t $n_f \pi_f \in T_{\mathbb{Z}}$

The next is left to the "reader."

Part (3) of the Lemma $\Rightarrow \exists\, \gamma_0^{\pm} \in \Lambda^{\pm}_{\mathcal{A}}/I_f$ satisfying: $\gamma = n_\gamma \gamma_0^{\pm}$ for some $n_\gamma \in \mathcal{O}_f$ $\left(\forall \gamma \in \Lambda^{\pm}/I_f\right)$.

Now, $\Lambda^-\left(f, \frac{a}{m}, 1\right) = \Lambda\left(f, \frac{a}{m}, 1\right) - \Lambda\left(f, -\frac{a}{m}, 1\right) = \int_{a/m}^{a/m + i\infty} \omega_f - \int_{-a/m}^{-\frac{a}{m} + i\infty} \omega_f =$

$= \int_{a/m}^{-a/m} \omega_f$



goes to 0 as $\to \infty$ (as it is a cusp form).

There is an element $\gamma \in \Gamma_0(N)$ s.t $\gamma \frac{a}{m} = -\frac{a}{m}$.

So the integral is $\int_{a/m}^{\gamma a/m} \omega_f = \varphi_\gamma(\omega_f)$ ← depends only on image of γ modulo I_f.

Write $\gamma = n_\gamma \gamma_0^{+}$, so $\varphi_\gamma(\omega_f) = \varphi_{n_\gamma \gamma_0^-}(\omega_f) = n_\gamma \varphi_{\gamma_0^-}(\omega_f)$.

Then let $\Omega^- := \int_{\gamma_0^-} \omega_f \in i\mathbb{R}$.

For the $+$-part, the argument needs to be modified:

$\Lambda^+\left(f, \frac{a}{m}, 1\right) = \int_{a/m}^{a/m + i\infty} \omega_f + \int_{-a/m}^{-\frac{a}{m} + i\infty} \omega_f = \underbrace{\int_{a/m}^{0} \omega_f + \int_{-a/m}^{0} \omega_f}_{-\Omega^+ \mathcal{O}_f} + 2\int_0^{i\infty} \omega_f$

need to deal with this

where $\Omega^+ := \int_{\gamma_0^+} \omega_f$ as before.

(cont pf)

To control $\int_0^{i\infty} \omega_f$, we use T_p. Take representatives $\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}$ $(j = 0 \dots p-1)$

$$\int_0^{i\infty} \omega_f | T_p = \int_0^{i\infty} \omega_f |_2 \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} + \cdots + \omega_f |_2 \begin{pmatrix} 1 & p-1 \\ 0 & p \end{pmatrix} = 2i \int_0^{i\infty} \omega_f + \int_{1/p}^{1/p + i\infty} \omega_f + \cdots + \int_{\frac{p-1}{p}}^{\frac{p-1}{p} + i\infty} \omega_f =$$

$$= a_p \int_0^{i\infty} \omega_f$$

Consider now $(p+1) \int_0^{i\infty} \omega_f$, and then:

$$\left((p+1) - a_p(f)\right) \int_0^{i\infty} \omega_f = \int_{1/p}^{0} \omega_f + \int_{2/p}^{0} \omega_f + \cdots + \int_{p-1}^{0} \omega_f \in \Omega^+ \cdot \mathcal{O}_f$$

Hence $\int_0^{i\infty} \omega_f \in \frac{\Omega^+}{(p+1-a_p(f))} \mathcal{O}_f$.

Replace now Ω^+ by $\frac{\Omega^+}{p+1-a_p(f)}$ for some p (could vary over all p to get an smaller denominator)

Recall of what we've done so far: $f \in S_2(\Gamma_0(N))$, $\omega_f := 2\pi i f(z)\, dz$.

We showed that $\Lambda_f^+ \subseteq k_f \Omega_+$, $\Omega_+ \in \mathbb{R}$

$\Lambda_f^- \subseteq k_f \Omega_-$, $\Omega_- \in i\mathbb{R}$

(where $\Lambda_f^{\pm} = \left\{ \int_{a/m}^{\gamma_m + i\infty} \omega_f \pm \int_{\gamma_m - a/m}^{-a/m + i\infty} \omega_f \right\} \subseteq \begin{cases} \mathbb{R} & (+) \\ i\mathbb{R} & (-) \end{cases}$).

To do this, we proved that, for $p \nmid N$:

$$(1 + p - a_p)\, \Lambda_f^+ \subseteq \left\{ \int_\gamma \omega_f + \overline{\omega}_f : \gamma \in H_1(X_0(N)(\mathbb{C}), \mathbb{Z}) \right\}$$

$$\Lambda_f^- \subseteq \left\{ \int_\gamma \omega_f - \overline{\omega}_f \right\}$$

Recall also that we defined a map:

$$\mathrm{Int}_f^{+} : \frac{H_1(X_0(N)(\mathbb{C}), \mathbb{Z})^{\pm}}{I_f H_1(X_0(N)(\mathbb{C}), \mathbb{Z})^{\pm}} \longrightarrow \mathbb{C}^{\pm}$$

($\pm$ ← action of c conjugation)

where $I_f = \ker \left\{ \begin{array}{ccc} \mathbb{T} & \longrightarrow & K_f \\ T_n & \longmapsto & a_n \end{array} \right\}$

From this, get that $\dfrac{H_1(X_0(N)(\mathbb{C}), \mathbb{Q})^{\pm}}{I_f} \simeq K_f$ as a K_f-vectorspace

Hence $\exists\, \Omega_{\pm}$ s.t. $\Lambda_f^{\pm} \in K_f \Omega_{\pm}$.

The integrality follows from the fact that $H_1(X_0(N)(\mathbb{C}), \mathbb{Z})$ is finitely-generated as a $\mathbb{Z}$-module.

Corollary:

1) If $\chi(-1) = 1$ (χ is even), then:

$$\Lambda(f, \chi, 1) \in \frac{1}{2} \frac{\tau(\chi)}{m} \Omega_f^{+} \mathcal{O}_f \mathcal{O}_\chi$$

where $\mathcal{O}_\chi = \mathbb{Z}[\chi(2), \chi(3), \ldots, \chi(n-1)]$.

(where m = conductor of χ)

2) If $\chi(-1) = -1$ (χ is odd) then:

$$\Lambda(f, \chi, 1) \in \frac{1}{2} \frac{\tau(\chi)}{m} \Omega_f^{-} \mathcal{O}_f \mathcal{O}_\chi$$

Pf (1) As $\Lambda(f, \chi, 1) = \dfrac{\tau(\chi)}{m} \sum_{a=0}^{m-1} \overline{\chi}(a) \Lambda(f, \frac{a}{m}, 1) \overset{\chi \text{ even}}{=} \dfrac{\tau(\chi)}{2m} \sum_{a=0}^{m-1} \left(\overline{\chi}(a) + \overline{\chi}(-a)\right) \Lambda(f, \frac{a}{m}, 1)$

$$= \frac{1}{2} \frac{\tau(\chi)}{m} \sum_{a=0}^{m-1} \overline{\chi}(a) \Lambda^{+}(f, \tfrac{a}{m}, 1) \in \frac{1}{2} \frac{\tau(\chi)}{m} \Omega_{+} \mathcal{O}_f \mathcal{O}_\chi$$

For (2), the proof is essentially the same.

• Modular Symbols: Let A be an abelian group.

Define: An A-valued modular symbol is a function

$$m : \mathbb{P}_1(\mathbb{Q}) \times \mathbb{P}_1(\mathbb{Q}) \longrightarrow A$$
$$(r, s) \longmapsto m\{r \to s\}$$

satisfying:

1) $m\{r \to s\} = -m\{s \to r\}$
2) $m\{r \to s\} + m\{s \to t\} = m\{r \to t\}$

$\forall\ r, s, t \in \mathbb{P}_1(\mathbb{Q})$.

The group $GL_2(\mathbb{Q})$ acts on $M(A) := \{$(abelian) group of all A-valued modular symbols$\}$ on the right, by the rule:

$$(m \mid \gamma)\{r \to s\} = m\{\gamma r \to \gamma s\}$$

Example: Given a newform f, can define:

- $m_f^+\{r \to s\} := \int_r^s \omega_f + \int_{-r}^{-s} \omega_f$
- $m_f^-\{r \to s\} := \int_r^s \omega_f - \int_{-r}^{-s} \omega_f$

Note that $m_f^{\pm} \in M\left(\Omega_f^{\pm} \mathcal{O}_f\right)$

The modular symbols were introduced because they are computable.

So next we will see an algorithm to compute the $m_f^{\pm}$:

↓

• Algorithm for computing $m_\ell^{\pm}$

Simplifying assumption: assume N is prime.

In this case, $\Gamma_0(N)\backslash P_1(\mathbb{Q}) = \Gamma_0(N)\cdot 0 \sqcup \Gamma_0(N)\cdot\infty$

$\{\frac{a}{b} : N \nmid b\}$ $\qquad$ $\{\frac{a}{b} : N \mid b\}$.

(otherwise, we have more orbits)

(1) $m_\ell^{+}\{0\to\infty\} = 2\Lambda(\ell,1)$ ← has been worked out in the HW #3.

$m_\ell^{-}\{0\to\infty\} = 0$

Def: Two elements $\frac{a}{b}, \frac{c}{d} \in \mathbb{P}^1(\mathbb{Q})$ are adjacent if $ad - bc = \pm 1$

(convention: always represented in lowest terms, and $\infty = \frac{1}{0}$).

(2) Lemma: Any two cusps $\frac{a}{b}, \frac{c}{d}$ can be joined by a succession of paths between adjacent "cusps" elts of $\mathbb{P}^1(\mathbb{Q})$.

pf/ Enough to be able to join $\frac{a}{b}$ to ∞:

$$\{\tfrac{a}{b}\to\infty\} = \{\tfrac{a}{b}\to\tfrac{t}{a'}\} + \{\tfrac{t}{a'}\to\infty\}$$

where $a'a \equiv 1 \pmod b$ and such that $|a'| \le b/2$.

And choose t s.t. $aa' - bt = 1$.

Then $\{\frac{a}{b}\to\frac{t}{a'}\}$ is adjacent, and we are reduced to a problem size, as $|a'| \le \frac{b}{2}$.

It is basically the Euclidean algorithm to compute $\gcd(a,b)$.

(3) $m_f^{\pm}\{\gamma r \to \gamma s\} = m_f^{\pm}\{r \to s\} \quad \forall \gamma \in \Gamma_0(N)$,

because $m_f^{\pm}\{\gamma r \to \gamma s\} = \int_{\gamma r}^{\gamma s} \omega_f^{\pm} = \int_r^s \omega_f^{\pm} | \gamma = \int_r^s \omega_f^{\pm} = m_f^{\pm}\{r \to s\}$

From the remarks (1), (2), (3), we find that $m_f^{\pm}$ is completely determined by its values on

$$\Gamma_0(N) \backslash \left\{ \left(\frac{a}{b}, \frac{c}{d}\right) : ad - bc = 1 \right\} \xrightarrow{\simeq} \mathbb{P}_1\left(\mathbb{Z}/N\mathbb{Z}\right)$$

$$\left(\frac{a}{b}, \frac{c}{d}\right) \longmapsto \; ? \leftarrow \text{exercise.}$$

Hence we just need to compute $N+1$ values of $m_f^{\pm}$:

Corollary: $m_f^{\pm}\{r \to s\}$ is a $\mathbb{Z}$-linear combination of:

$$m_f^{\pm}\{0 \to \infty\},\ m_f^{\pm}\{1 \to 0\},\ m_f^{\pm}\{\tfrac{1}{2} \to 0\},\ \dots,\ m_f^{\pm}\left\{\tfrac{1}{N-1} \to 0\right\}.$$

(4) To compute this finite set of values, one can use analytic techniques.

Also, we can get an algorithm to compute modular forms:

Computation of Modular Forms.

Lemma: The integration map $S_2(\Gamma_0(N), \mathbb{R}) \longrightarrow \mathcal{M}(\mathbb{R})^{\Gamma_0(N)}$

$$f \longmapsto m_f^{+}$$

is an injection and can be made Hecke-equivariant

(after a suitable action of $\mathbb{T}$ on $\mathcal{M}(\mathbb{R})^{\Gamma_0(N)}$).

Def: $m|T_n\{r \to s\} := \sum_{j=1}^{k} m\{\alpha_j r \to \alpha_j s\}$ where $\Gamma_0(N)\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}\Gamma_0(N) = \bigcup_{j=1}^{k} \Gamma_0(N)\alpha_j$

This leads to an efficient procedure for calculating $S_2(\Gamma_0(N))$, by doing linear algebra on $M(R)^{\Gamma_0(N)}$ (diagonalize T there, and will get the eigenvalues of the eigenforms ...).

Another application: p-adic L-functions attached to f.

Fix a conductor m (prime to N, if $f \in S_2(\Gamma_0(N))$).

Let $G_m := (\mathbb{Z}/m\mathbb{Z})^\times$, $\lambda_f^\pm\left(\frac{a}{m}\right) := m_f^\pm \left\{\frac{a}{m} \to \infty\right\} \cdot \frac{1}{\Omega_f^\pm} \in \mathcal{O}_f$

Define $\Theta_m^\pm(f) := \sum_{a=1}^{m-1} \lambda_f^\pm\left(\frac{a}{m}\right) \cdot \sigma_a \in \mathcal{O}_f[G_m]$

where σ_a is the image of $a \in (\mathbb{Z}/m\mathbb{Z})^\times$ (and $\sigma_a = 0$ if $(a,m) \neq 1$)

Note also that if χ is a primitive character of conductor m (we computed this before)

$$\overline{\chi}\left(\Theta_m^\pm(f)\right) = \begin{cases} \frac{1}{\Omega_f^\pm} \Lambda(f,\chi,1) & \text{if parity of } \chi = \pm \\ 0 & \text{if parity of } \chi \neq \pm \end{cases}$$

Fix now a prime $p \nmid N$, and consider the elements:

$$\Theta_p^\pm(f),\ \Theta_{p^2}^\pm(f),\ \ldots,\ \Theta_{p^n}^\pm(f)$$

We have a natural projection:

$$\nu : \mathcal{O}_f[G_{p^{n+1}}] \to \mathcal{O}_f[G_{p^n}]$$

induced by the canonical map $(\mathbb{Z}/p^{n+1}\mathbb{Z})^\times \to (\mathbb{Z}/p^n\mathbb{Z})^\times$.

Q: Do the $\Theta_{p^n}^\pm(f)$ have a compatibility under ν?

That is, what's the relation between $\nu\left(\Theta_{p^{n+1}}^\pm(f)\right)$ and $\Theta_{p^n}^\pm(f)$?

Prop (Quasi-distribution relation): $n \geq 1$, $a \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$. Then:

$$\sum_{j=0}^{p-1} \lambda_f^{\pm}\left(\frac{a+jp^n}{p^{n+1}}\right) = a_p \lambda_f^{\pm}\left(\frac{a}{p^n}\right) - \lambda_f^{\pm}\left(\frac{a}{p^{n-1}}\right)$$

↑ p^{th} Fourier coeff of the modular form f.

Pf/ Recall that $\lambda_f^{\pm}\left(\frac{a}{p^n}\right) = m_f^{\pm}\left\{\frac{a}{p^n} \to \infty\right\} \cdot \frac{1}{\Omega^{\pm}}$

So $m_f^{\pm} \mid T_p \left\{\frac{a}{p^n} \to \infty\right\} = a_p(f)\, \lambda_f^{\pm}\left(\frac{a}{p^n}\right) \Omega^{\pm}$

$$\| $$

$$m_f^{\pm}\left\{\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\left(\frac{a}{p^n}\right) \to \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\infty\right\} + m_f^{\pm}\left\{\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\left(\frac{a}{p^n}\right) \to \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\infty\right\} + \cdots + m_f^{\pm}\left\{\begin{pmatrix} 1 & p-1 \\ 0 & p \end{pmatrix}\left(\frac{a}{p^n}\right) \to (\,)\infty\right\}$$

$$\left(= m_f^{\pm}\left\{\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\left(\frac{a}{p^n}\right) \to \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}\infty\right\} + \sum_{j=0}^{p-1} m_f^{\pm}\left\{\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}\left(\frac{a}{p^n}\right) \to \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}\infty\right\}\right)$$

$$= m_f^{\pm}\left\{\frac{a}{p^{n-1}} \to \infty\right\} + \sum_{j=0}^{p-1} m_f^{\pm}\left\{\frac{a+jp^n}{p^{n+1}} \to \infty\right\}$$

We will then modify the $\lambda_f^{\pm}$ so that they satisfy better compatibility.

Consider the polynomial $X^2 - a_p X + p \in \mathcal{O}_f[X]$.

$X^2 - a_p X + p = (X-\alpha)(X-\beta)$, $\alpha, \beta \in \mathcal{O}_f'$ ← maybe quadratic / $\mathcal{O}_f$.

Define: $\widetilde{\lambda_f^{\pm}}\left(\frac{a}{p^n}\right) := \alpha^{-n}\left(\lambda_f^{\pm}\left(\frac{a}{p^n}\right) - \frac{1}{\alpha}\lambda_f^{\pm}\left(\frac{a}{p^{n-1}}\right)\right) \in K_f'$

Rk: This definition depends on the choice of either α or β, so there are two ways to define them.

Prop (Distribution relation):

$$\sum_{j=0}^{p-1} \tilde{\lambda}_f^{\pm}\left(\frac{a+jp^n}{p^{n+1}}\right) = \tilde{\lambda}_f^{\pm}\left(\frac{a}{p^n}\right) \in \mathcal{O}_f[\alpha^{-1}]$$

Proof:

$$\sum_{j=0}^{p-1} \tilde{\lambda}_f^{\pm}\left(\frac{a+jp^n}{p^{n+1}}\right) = \sum_{j=0}^{p-1} \alpha^{-(n+1)}\left(\lambda_f^{\pm}\left(\frac{a+jp^n}{p^{n+1}}\right) - \frac{1}{\alpha}\lambda_f^{\pm}\left(\frac{a}{p^n}\right)\right) \overset{\text{prev. prop.}}{=}$$

$$= \alpha^{-(n+1)}\left(a_p \lambda_f^{\pm}\left(\frac{a}{p^n}\right) - \lambda_f^{\pm}\left(\frac{a}{p^{n-1}}\right) - \frac{p}{\alpha}\lambda_f^{\pm}\left(\frac{a}{p^n}\right)\right)$$

As $\frac{p}{\alpha} = \beta$ and $a_p = \alpha + \beta$, get:

$$= \alpha^{-(n+1)}\left(\alpha \lambda_f^{\pm}\left(\frac{a}{p^n}\right) - \lambda_f^{\pm}\left(\frac{a}{p^{n-1}}\right)\right) = \tilde{\lambda}_f^{\pm}\left(\frac{a}{p^n}\right)$$

Corollary: Define, for $n \geq 1$, ($a \mapsto$ image of a in $G_n = (\mathbb{Z}/p^n\mathbb{Z})^\times$)

$$\tilde{\Theta}_n^{\pm} := \sum_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \tilde{\lambda}_f^{\pm}\left(\frac{a}{p^n}\right) \cdot \sigma_a \in \underbrace{\mathcal{O}_f[1/\alpha]}_{=:R}[G_n] \quad \text{(group ring)}.$$

Then: $\left(\nu_{n+1,n} : R[G_{n+1}] \to R[G_n]\right)$

$$\boxed{\nu_{n+1,n}\left(\tilde{\Theta}_{n+1}^{\pm}\right) = \tilde{\Theta}_n^{\pm}}$$

$G_\infty := \varprojlim G_n = \mathbb{Z}_p^\times$ (projective limit)

So one can define $\Theta_\infty^{\pm} := \left(\tilde{\Theta}_n^{\pm}\right)_{n \geq 1} \in \varprojlim_{\nu_{n+1,n}} R[G_n] =: R[\![G_\infty]\!]$

Rk: $R[G_\infty] \subseteq R[\![G_\infty]\!]$, but the latter is much nicer.

Def: The ring $R[\![G_\infty]\!]$ is called the <u>completed group ring</u> with coefficients in R, associated to the profinite group G_∞.

• Some (soft) p-adic functional analysis.

Let $\widetilde{\mathcal{F}}_{l.c.}(G_\infty)\left(=\widetilde{\mathcal{F}}_{lc}(\mathbb{Z}_p^\times)\right)$ be the space of locally-constant R-valued functions on G_∞.

That is, because R is endowed —for now— with the discrete topology, being locally-constant is the same as being continuous.

(so $\widetilde{\mathcal{F}}_{lc}(G_\infty)$ is the space of continuous functions $G_\infty \to R$).

Let $\widetilde{\mathcal{F}}_{lc}^{\vee}(G_\infty) := \mathrm{Hom}\left(\widetilde{\mathcal{F}}_{lc}(G_\infty), R\right)$.

Prop: $\widetilde{\mathcal{F}}_{lc}^{\vee}(G_\infty) \overset{\text{natural}}{=} R[\![G_\infty]\!]$

Pf: deferred

~~Lemma: If $h \in \widetilde{\mathcal{F}}_{lc}(G_\infty)$~~

Remark: If $U_{a,n} \subseteq G_\infty$ is an open subset, ~~[illegible]~~ of the form $U_{a,n} = a + p^n\mathbb{Z}_p$, for $a \in \mathbb{Z}_p^\times$, then $U_{a,n}^c = \coprod_{\substack{b \neq a \\ (\mathrm{mod}\ p^n)}} (b + p^n\mathbb{Z}_p)$,

so $U_{a,n}$ is both open and closed.

Hence $\chi_{U_{a,n}}$ (the characteristic function on $U_{a,n}$) is continuous.

Lemma:

1) If $h \in \mathcal{F}_{lc}(G_\infty)$, then h is a finite R-linear combination of $\chi_{U_{a,n}}$'s.

2) Suppose, further, that R contains all $(p-1)p^n$-th roots of 1, and $\frac{1}{p(p-1)}$. Then h is an R-linear combination of finitely many continuous characters $\chi: G_\infty \to R^\times$

Pf (1) For $x \in G_\infty$, $\exists\, U_x \ni x$ s.t. $h|_{U_x}$ is constant.

So write $G_\infty = \bigcup_{x \in G_\infty} U_x$. As G_∞ is compact (profinite!), $G_\infty = U_{x_1} \cup \cdots \cup U_{x_n}$. Then we are done.

(2) By Fourier analysis on the G_n's, one can express any $\chi_{a,n}$ as a linear combination of $\chi: G_\infty \to R^\times$.

Prop (which implies the previously stated one):

The function $\mathcal{F}_{lc}^{\vee}(G_\infty) \to R[\![G_\infty]\!]$ which sends $\mu \mapsto \left(\theta_n := \sum_{a \in (\mathbb{Z}/p^n\mathbb{Z})^\times} \mu(a+p^n\mathbb{Z}_p)\sigma_a^{-1}\right)_n$ is an R-linear isomorphism.

Pf Exercise //

Terminology:

- The elements of $\mathcal{F}_{lc}^{\vee}(G_\infty) = R[\![G_\infty]\!]$ are called "R-valued distributions on G_∞".
- If $h \in \mathcal{F}_{lc}(G_\infty)$, and $\mu \in \mathcal{F}_{lc}^{\vee}(G_\infty)$, then $\mu(h) =: \int_{G_\infty} h\, d\mu$

In particular, to $\tilde{\theta}_n^{\pm} \in R[\![G_\infty]\!]$ we have an associated $\mu_f^{\pm} \in \mathcal{F}_{lc}^{\vee}(G_\infty)$.

→ Interpolation formula :

Let $\chi : \mathbb{Z}_p^\times \to R^\times$ be a finite order continuous character of $\mathbb{Z}_p^\times$.

• If $\chi \neq \chi_{triv}$:

$$\int_{\mathbb{Z}_p^\times} \chi \, d\mu_f^{\pm} = \begin{cases} \dfrac{\alpha^{-n} p^n}{\tau(\chi)} \dfrac{\Lambda(f,\chi,1)}{\Omega_f^{\pm}} & \text{if } \chi(-1) = \pm 1 \\ 0 & \text{if } \chi(-1) = \mp 1 \end{cases}$$

(signs according to $\mu_f^{\pm}$)

• If $\chi = \chi_{triv}$:

$$\int_{\mathbb{Z}_p^\times} d\mu_f^{+} = \left(1 - \frac{1}{\alpha}\right) \frac{\Lambda(f,1)}{\Omega_f^{+}}$$

and $$\int_{\mathbb{Z}_p^\times} d\mu_f^{-} = 0$$

Prove it as an exercise.

We now put a topology on R, and start more serious p-adic analysis.

So let R be endowed with a p-adic topology.

(e.g. R = completion of K_f at a prime above p).

This gives $\mathcal{F}_{lc}(G_\infty)$ a topology (from the sup norm : $\|h\|_{sup} = \sup_{x \in \mathbb{Z}_p^\times} |h(x)|$).

Then $\mathcal{F}_{lc}(G_\infty) \subseteq \mathcal{F}_{cont}(G_\infty)$

Lemma : The completion of $\mathcal{F}_{lc}(G_\infty)$ wrt $\|\cdot\|_{sup}$ is $\mathcal{F}_{cont}(G_\infty)$.

Pf Exercise (use compactness for the density).

Lemma: An R-valued distribution μ is continuous relative to the sup norm on $\mathcal{F}_{lc}(G_\infty)$ iff μ is bounded

(i.e. iff $\{\mu(a+p^n\mathbb{Z}_p)\}_{\substack{n\geq 1 \\ (a,p^n)=1}} \subseteq R$ is a bounded subset) for the p-adic norm.

Pf

$\Leftarrow$] If μ is bounded.

Suppose that $h, g \in \mathcal{F}_{lc}(G_\infty)$ satisfy $\|h-g\| < \varepsilon$.

There exists $n \geq 1$ and $U_1, \dots, U_n$ of open + closed subsets of $\mathbb{Z}_p^\times$

such that $h = \sum_{i=1}^{n} a_i \chi_{U_i}$, $g = \sum_{i=1}^{n} b_i \chi_{U_i}$,

(assume also w.l.o.g. that the U_i's are disjoint).

$\|h-g\| < \varepsilon \Rightarrow |a_i - b_i| < \varepsilon$ for $i = 1 \dots n$.

But $\int h\,d\mu = \sum_{i=1}^{n} a_i \mu(\chi_{U_i})$; $\int g\,d\mu = \sum_{i=1}^{n} b_i \mu(\chi_{U_i})$.

So $|\mu(h) - \mu(g)| = \left| \sum_{i=1}^{n} \overbrace{(a_i - b_i)}^{\leq \varepsilon} \overbrace{\mu(\chi_{U_i})}^{\leq C} \right| < C \cdot \varepsilon$

↑ strong triangle inequality (thanks to non-archimedean)

$\Rightarrow$] Suppose that μ is unbounded. Want to see that μ is discontinuous.

Let $U_1, \dots, U_n, \dots$ be a sequence of open/closed subsets of $\mathbb{Z}_p^\times$ such that $\mu(\chi_{U_j}) \to \infty$.

But $h_j := \dfrac{\chi_{U_j}}{\mu(U_j)} \longrightarrow 0$ uniformly, and $\int h_j\,d\mu = 1 \ \forall j \Rightarrow$ disc.

Lemma: Let $j: K_f \to R$ be the natural embedding of K_f in its completion (that is, $R = K_{f,\mathfrak{p}}$, $\mathfrak{p}|p$).

Then $j_*(\mu_f^{\pm})$ is bounded iff $|j(a_p)| = 1$ (i.e. $j(a_p)$ is a unit).

Def: We say that f is ordinary at $\mathfrak{p} \triangleleft \mathcal{O}_f$ if $p \nmid a_p$. (that is, $\alpha \in \mathcal{O}_K^\times$)

Proof (of lemma):

Recall α is a root of $X^2 - a_p X + p$.

If $\mathfrak{p} \nmid a_p$, then $X^2 - a_p X + p \equiv X(X - a_p) \bmod \mathfrak{p}$ (distinct roots).

So by Hensel's lemma, it has two roots (distinct) $\alpha, \beta \in K_{f,\mathfrak{p}} = R$.

Assume that $\alpha \equiv a_p \bmod \mathfrak{p}$, $\beta \equiv 0 \bmod \mathfrak{p}$.

Then the corresponding $\mu_f^{\pm}$ are bounded, hence continuous.

The converse is left as an exercise.

If f is ordinary, we get elements $\mu_f^{\pm} \in \widetilde{F}_{cts}(K_{f,\mathfrak{p}})^\vee$.

* **Some key functions on $\mathbb{Z}_p^\times$ (continuous).**

$\chi_k : x \mapsto x^k$. These $\chi_k \in \mathrm{Hom}_{cts}(G_\infty, \mathbb{Z}_p^\times)$ (for $k = 1, 2, \dots$ ($\in \mathbb{Z}$), $-1, -2, \dots$).

$\mathbb{Z} \subseteq \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p$. Put on $\mathbb{Z}$ the subspace topology ($\mathbb{Z}/(p-1)\mathbb{Z}$ with discrete top).

Then $k \mapsto \chi_k$ is continuous relative to this topology:

if $(k_1 - k_2) \equiv 0 \bmod (p-1)p^n$, then $x^{k_1} - x^{k_2} \equiv 0 \pmod{p^{n+1}}$ $\forall x \in \mathbb{Z}_p^\times$.

(Pf as an exercise)

Def (The p-adic L-function): ← Mazur-Swinnerton Dyer

Suppose that f is ordinary at p, and let $\mu_f^{\pm}$ be the (bdded) dist on G_{∞}.

Then the p-adic L-function attached to f is the function on $\mathbb{Z}/(p-1)\times\mathbb{Z}_p$

$$L_p^{\pm}(f,s) := \int_{\mathbb{Z}_p^\times} x^{s-1}\, d\mu_f^{\pm}(x) \qquad \text{(the Mazur-Mellin transform)}$$

(where $s \in \mathbb{Z}/(p-1)\times\mathbb{Z}_p$ can be seen as a limit of integers — $\mathbb{Z}$ dense in $\mathbb{Z}/(p-1)\times\mathbb{Z}_p$)

Lemma: If $x \in \mathbb{Z}_p^\times$, then there exists a unique $(p-1)^{st}$-root of 1 in $\mathbb{Z}_p^\times$, say ξ such that $\xi \equiv x \pmod p$.

Pf: Hensel's lemma

Notation: $\omega(x) := \xi$, is called the Teichmüller lift of x.

(Rk: Sometimes ω is defined to be ξ^{-1}!)

Rk: $\omega(x) = \lim_{n\to\infty} x^{p^n}$

Write then $x = \omega(x)\langle x\rangle$, $\langle x\rangle = 1 + p\tilde{x}$, $\tilde{x}\in\mathbb{Z}_p$.

Note then that $(x \bmod p, \tilde{x})$ determine $x \in \mathbb{Z}_p^\times$.

Recall $U_{a,j} := a + p^j\mathbb{Z}_p$ = ball of radius p^{-j} "centered at a".

Define $M_f(a,k) := \int_{U_{a,1}} \tilde{x}^k\, d\mu_f^{\pm}(x) \in$ Bounded subset of K

(this is called the k-th moment of $\mu_f^{\pm}$ on $U_{a,1}$).

• "Taylor expansion" of $L_p^{\pm}(f,s)$

Prop: $$L_p^{\pm}(f,s) = \sum_{a=1}^{p-1} \omega(a)^{s-1} \left(\sum_{k=0}^{\infty} p^k M(a,k) \cdot \binom{s-1}{k} \right)$$

where $\binom{s-1}{k} = \frac{(s-1)(s-2)\cdots(s-k)}{k!}$ $\left(\in \mathbb{Z}_p \text{ if } s \in \mathbb{Z}_p\right)$. $\left(\text{and } \binom{s-1}{0} = 1 \text{ by convention}\right)$

Proof:

$$\int_{\mathbb{Z}_p^\times} x^{s-1} d\mu_f^{\pm}(x) = \sum_{a=1}^{p-1} \int_{U_{a,1}} x^{s-1} d\mu_f^{\pm}(x) = \sum_a \int_{U_{a,1}} \omega(x)^{s-1} \langle x \rangle^{s-1} d\mu_f^{\pm}(x)$$

$$= \sum_a \omega(a)^{s-1} \int_{U_{a,1}} (1+p\tilde{x})^{s-1} d\mu_f^{\pm}(x)$$ and use the binomial thm to expand this. ∎

This is a good way to do computations (the moments are "easy" to compute).

Applications to arithmetic:

Key example: Elliptic Curves.

Let $E/\mathbb{Q}$ be a given elliptic curve.

Theorem (Wiles, ...): There exists a newform $f \in S_2(\Gamma_0(N))$ with integer coefficients such that $L(E,s) = L(f,s)$.

What is shown is that $V_p(E) \simeq V_p(f)$, as representations of $G_{\mathbb{Q}}$.

where $V_p(E) = \left(\varprojlim_n E[p^n]\right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \left(\simeq \mathbb{Q}_p^2\right)$.

and $V_p(f)$ = Galois rep. attached to f, characterised by the Frobenius:

if $\ell \nmid Np$, the char. poly of Frob_ℓ is $X^2 - a_\ell X + \ell$.

↓

Theorem (Eichler-Shimura): If f is a newform in $S_2(\Gamma_0(N))$ with integer coefficients, then there exists an elliptic curve E_f, such that $L(E_f, s) = L(f, s)$.

Rk: Once we have E_f, then define $V_p(f) = V_p(E_f)$.

Construction of E_f: $E_f = \frac{J_0(N)}{I_f}$ where $J_0(N)$ = Jacobian of $X_0(N)$.

What is the relation of E and E_f?

We have that $L(E, s) = L(E_f, s)$ (or equivalently, $V_p(E) \simeq V_p(E_f)$)

Then:

Theorem (Faltings): If E_1, E_2 are elliptic curves over $\mathbb{Q}$ (or two abelian varieties over K a #field), such that $V_p(E_1) \simeq V_p(E_2)$, then $\exists\ \phi : E_1 \to E_2$ an isogeny.

Consequence: there is an (abelian) map, defined over $\mathbb{Q}$, $J_0(N) \twoheadrightarrow E$.

Recall the definition of $\omega_f = 2\pi i f(\tau)\, d\tau$, on $\frac{\mathcal{H}}{\Gamma_1(N)}$, a diff form on $X_0(N)(\mathbb{C})$.

The elliptic curve E has a one-dimensional space of regular differential 1-forms:

$\omega_E = \frac{dx}{y}$ if $E: y^2 = x^3 + ax + b$, $a, b \in \mathbb{Q}$.

Theorem: $\phi^*(\omega_E) = c \cdot \omega_f$, for $c \in \mathbb{Q}^\times$. (and $\phi: J_0(N) \twoheadrightarrow E$ is the $\mathbb{Q}$-map.)

Periods of f:

define $\omega_E^\pm = \omega_E \pm \overline{\omega_E}$

$$m_f^\pm\{r \to s\} = \int_r^s \omega_f^\pm = \int_r^s \omega_f \pm \bar{\omega}_f = \int_r^s c^{-1} \phi^*(\omega_E^\pm) = c^{-1} \int_{\phi[r\to s]} \omega_E^\pm$$

Choose q any prime $q \nmid N$, and then

$$\Rightarrow (q+1-a_q)\, m_f^\pm\{r \to s\} = c^{-1}(q+1-a_p) \int_{\phi([r\to s])} \omega_E^\pm = c^{-1} \int_{\phi[(q+1-T_q)\{r\to s\}]} \omega_E^\pm$$

Note that $\phi\left((q+1-T_q)[r \to s]\right) \in H_1(E(\mathbb{C}), \mathbb{Z})$

Hence $\boxed{m_f^\pm\{r \to s\} \in (q+1-a_q)^{-1} \cdot c^{-1} \cdot \Lambda_E^\pm}$,

where $\Lambda_E^\pm = \left\{ \int_\gamma \omega_E^\pm : \gamma \in H_1(E(\mathbb{C}), \mathbb{Z}) \right\}$.

Then $\Lambda_E^+ = \Omega_E^+ \mathbb{Z}$, $\Lambda_E^- = \Omega_E^- \mathbb{Z}$, for $\Omega_E^\pm \in \mathbb{R}$, $\Omega_E^- \in i\mathbb{R}$.

Birch - Swinnerton Dyer conjecture:

By Mordell-Weil theorem, $E(\mathbb{Q}) \simeq \mathbb{Z}^r \oplus T$, $|T| < \infty$, $r = r_E(\mathbb{Q})$.

Conjecture (BSD): $\operatorname{ord}_{s=1} L(E,s) = r_E(\mathbb{Q})$.

Conjecture (BSD_p): $\operatorname{ord}_{s=1} L_p^+(E,s) = r_E(\mathbb{Q})$ (if $p \nmid N$).

• What's known about BSD?

For the (classical) BSD: If $\operatorname{ord}_{s=1} L(E,s) \leq 1$, then it is true.

For BSD_p, we know a lot more: $\operatorname{ord}_{s=1} L_p^+(E,s) \leq 1$ then true as well, and:

$$\operatorname{ord}_{s=1} L_p^+(E,s) \geq r_E(\mathbb{Q}) \qquad \text{(theorem of Kato)}.$$

The philosophy is that the p-adic L-function is closer to arithmetic than the complex one.

• p-adic Modular Forms.

Preview: The Kubota-Leopoldt p-adic L-function:

Given $\chi : \left(\frac{\mathbb{Z}}{p^n\mathbb{Z}}\right)^\times \to \mathbb{C}^\times$, have defined:

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

Theorem: $L(\chi, 0)$ are rational $\forall \chi$, and moreover there exists a p-adic measure (a bounded p-adic distribution) μ_a such that:

$$\forall \chi \neq 1 \text{ primitive} \qquad \int_{\mathbb{Z}_p^\times} \chi(t)\, d\mu_a(t) = L(\chi,0)\cdot\left(1 - a\chi(a)\right).$$

(for any previously fixed $a \in \mathbb{Z}_p^\times$).

If $\chi = 1$, $\int_{\mathbb{Z}_p^\times} d\mu_a(t) = \left(1 - a\chi(a)\right)\left(1 - \frac{1}{p}\right) \overbrace{L(1,0)}^{\zeta(0)}$

• Kubota-Leopoldt L-function

we define $L_p(s) = \int_{\mathbb{Z}_p^\times} x^{s-1}\, d\mu_a(x)$, $s \in \mathbb{Z}/(p-1) \times \mathbb{Z}_p$

Interesting phenomenon:

$$L_p(k) = (1-a^k)(1-p^{k-1})\,\zeta(1-k) \qquad \forall k>1 \text{ integer}, \; k \equiv 1 \pmod{p-1}.$$

This is how $L_p(s)$ is constructed usually:

One first proves that $\zeta(1-k_1) \equiv \zeta(1-k_2) \bmod p^m$ if $k_1 \equiv k_2 \bmod (p-1)p^{m-1}$ and $k_i \not\equiv 0 \pmod{p-1}$.

(called Kummer-Von Standt congruence).

Question: Can we prove similar congruences, and therefore construct analogous p-adic L-functions by replacing $\zeta(s)$ by the Dedekind Zeta-function of a number field.

Let F be a number field, $\zeta_F(s) = \sum_{\mathfrak{a} \subseteq \mathcal{O}_F} (N\mathfrak{a})^{-s} = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}$

If F is abelian, $\zeta_F(s) = \prod_{\chi \in \widehat{Gal(F/\mathbb{Q})}} L(\chi, s)$ is easier.

But we can do it in general. We will see that $\zeta_F(1-k)$ can be written as constant term of certain modular forms.

Let $f \in M_k := M_k(SL_2(\mathbb{Z}))$, $g \in M_{k'}$.

We want to show that:

$$\begin{cases} a_n(f) \equiv a_n(g) \pmod{p^r} \ \forall n \\ (p-1) \nmid k \end{cases} \Longrightarrow a_0(f) \equiv a_0(g) \pmod{p^r}$$

Recall the Eisenstein series $G_k = \underbrace{\frac{1}{2}\zeta(1-k)}_{-\frac{B_k}{2k}} + \sum_{n \geq 1} \sigma_{k-1}(n) q^n$ $k \geq 2$ even.

and $E_k := \frac{-2k}{B_k} G_k = 1 - \frac{2k}{B_k} \sum_{n \geq 1} \sigma_{k-1}(n) q^n$ $\quad \sigma_{k-1}(n) = \sum_{d \mid n} d^{k-1}$

Define also

$$P := E_2 = 1 - 24 \sum \sigma_1(n) q^n \quad (B_2 = 1/6)$$
$$Q := E_4 = 1 + 240 \sum \sigma_3(n) q^n \quad (B_4 = -1/30)$$
$$R := E_6 = 1 - 504 \sum \sigma_5(n) q^n \quad (B_6 = 1/42)$$

(from Ramanujan)

Rk: it is not true in general that the E_k have integer coefficients!

We will assume $\boxed{p \geq 5}$. For $p = 2, 3$ things can be adapted, but proofs become more cumberson.

Basic properties of the Eisenstein series.

I. For $k \geq 4$, $E_k \in M_k$.

I': $E_2\left(\frac{az+b}{cz+d}\right) = (cz+d)^2 E(z) + \underbrace{\frac{12}{2\pi i} \cdot c \cdot (cz+d)}_{\text{because the series is not absolutely convergent}}$

II. Clausen–Von Staudt congruences:

a) $(p-1) \nmid k$ & $\zeta(1-k)$ is p-integral and, if $k \equiv k' \bmod (p-1)p^{r-1}$, then it follows $\zeta(1-k) \equiv \zeta(1-k') \pmod{p^r}$.

b) $(p-1) \mid k$: then $p \mid \text{denom}(\zeta(1-k))$. More precisely, if $k \equiv 0 \bmod (p-1)p^{r-1}$ then $p^r \mid \text{denom}(\zeta(1-k))$. (and $(p-1)p^{r-1} \| k \Rightarrow p^r \| \text{denom}(\zeta(1-k))$)

The Clausen-Von Staudt congruences will not be proven. But check Cyclotomic Fields (L. Washington).

Proposition: ("Clausen-Von Staudt for Eisenstein series"): all the Fourier coeffs are congruent.

a) If $\begin{cases} k \equiv k' \pmod{(p-1)p^{r-1}}, \text{ and} \\ (p-1) \nmid k \end{cases}$ then $G_k \equiv G_{k'} \pmod{p^r}$

b) If $(p-1)p^{r-1} \mid k$, then $E_k \equiv 1 \pmod{p^r}$.

pf

a) $a_0(G_k) \equiv a_0(G_{k'})$ is a restatement of the C-VStaudt congruences.

$a_n(G_k) \equiv a_n(G_{k'})$ follows from $d^{k-1} \equiv d^{k'-1} \pmod{p^r}$. (if $k \equiv k' \bmod (p-1)p^{r-1}$)

b) Follows from C-VStaudt part (b) - immediately.

(continues basic properties)

III. Write $M = \bigoplus M_k$, the graded of modular forms.

Last semester: $M \cong \mathbb{C}[Q, R]$ with deg $Q = 4$, deg $R = 6$

(↑ as graded rings)

New definitions:

Let $M_k :=$ Modular forms of weight k on $SL_2(\mathbb{Z})$ with Fourier coeffs in $\mathbb{Z}_{(p)}$.

$M := \bigoplus_k M_k$

Lemma: $M \cong \mathbb{Z}_{(p)}[Q,R]$.

Pf There's a natural map $\mathbb{Z}_{(p)}[Q,R] \hookrightarrow M$. Need surjectivity.

We argue by induction on k, by considering the map:

$\mathbb{Z}_{(p)}[Q,R]^{\deg = k} \hookrightarrow M_k$. and showing surjectivity there.

For $k=0$, $M_0 = \mathbb{Z}_{(p)}$ ✓

$k=2$, $M_2 = 0$ ✓

$k=4$, $M_4 = \mathbb{Z}_{(p)} \cdot Q$ because if $f \in M_4$, $f = a_0(f) \cdot Q$, and

$a_0(f) \in \mathbb{Z}_{(p)}$ ✓.

$k=6$; $M_6 = \mathbb{Z}_{(p)} \cdot R$ similarly.

$k=8$, $M_8 = \mathbb{Z}_{(p)} \cdot Q^2$ "

$k=10$, $M_{10} = \mathbb{Z}_{(p)} \cdot QR$

Assume now $k \geq 12$. Let $f \in M_k$. Choose $a, b \in \mathbb{Z}_{\geq 0}$ s.t

$4a + 6b = k$

Let $f_0 = f - a_0(f) Q^a R^b \in S_k \subseteq M_k$ (cusp forms with coeffs in $\mathbb{Z}_{(p)}$)

So $\exists\, g \in M_{k-12} \otimes \mathbb{C}$ s.t $f_0 = g \cdot \Delta$

Claim: $g \in M_{k-12}$.

Pf Note that $g = f_0 \Delta^{-1}$ on $\mathbb{Z}_{(p)}[\![q]\!]$. But $f_0 \Delta^{-1} = f_0 q^{-1} \left(\frac{\Delta}{q}\right)^{-1}$

($\mathbb{Z}_{(p)}[\![q]\!]$ b/c $a_1(\Delta) = 1$)

Now, use induction hypothesis: $g = G(Q,R)$, $G \in \mathbb{Z}_{(p)}[Q,R]$.

Then $f_0 = g \cdot \Delta$. As $\Delta = \frac{Q^3 - R^2}{1728}$, then $f_0 = \frac{Q^3 - R^2}{1728} G(Q,R) \in \mathbb{Z}_{(p)}[Q,R]$

and we are done.

Def: $f \in M_k$, $g \in M_{k'}$ are said to be congruent mod p^r if

$$a_n(f) \equiv a_n(g) \pmod{p^r} \quad \forall n \geq 0.$$

Theorem: If $f \equiv g \pmod{p^r}$ and $p \nmid f$, then $k \equiv k' \pmod{(p-1)p^{r-1}}$ ($r \geq 1$)

↑ avoid getting "stupid extra congruence".

To prove the theorem, consider first the case $r = 1$.

Def: The space of modular forms mod p, denoted $\bar{M}$, is the natural image of $M \otimes \mathbb{F}_p$ in $\mathbb{F}_p[\![q]\!]$

(coming from $M \hookrightarrow \mathbb{Z}_{(p)}[\![q]\!]$, get $M \otimes_{\mathbb{Z}_{(p)}} \mathbb{F}_p \longrightarrow \mathbb{F}_p[\![q]\!]$, not injective anymore!).

- **Structure of $\bar{M}$**:

We need to study the kernel of the surjective map $\pi : M \otimes \mathbb{F}_p \to \mathbb{F}_p[\![q]\!]$.

Recall that (C-VS) $E_{p-1} \equiv 1 \pmod{p}$.

Def The polynomial $A(X, Y) \in \mathbb{F}_p[X, Y]$ of degree $p-1$ satisfying

$$E_{p-1} = A(Q, R)$$

is called the Hasse polynomial, or the Hasse invariant.

Obviously, $A - 1 \in \ker \pi$.

Rk: $A - 1$ is not homogeneous! (b/c of the -1).

We will next show that $\ker \pi = (A - 1)$.

Theorem: $\ker \pi = (A-1)$

Pf

Step 1: It is enough to show that $A-1$ is irreducible, so that $(A-1)$ is prime:

If $(A-1) \subsetneq \ker \pi \triangleleft \mathbb{F}_p[Q,R]$,

as $\mathbb{F}_p[Q,R]$ is 2-dimensional, $\ker \pi$ is maximal.

This would imply that $\bar{M} = \frac{\mathbb{F}_p[Q,R]}{\ker \pi}$ is finite field.

But $\pi|_{M_K \otimes \mathbb{F}_p}$ is injective, hence $\dim_{\mathbb{F}_p} \bar{M} = \infty$. $\Rightarrow$!!

Step 2: It is enough to show that $A(x,y)$ has no multiple factors.

Why: Suppose that $A(x,y)-1$ has a nontrivial irreducible factor, say $G(x,y)$.

Then $\deg G(x,y) < \deg A(x,y) = p-1$

Write $G = G_r(x,y) + (\text{homog. terms of lower degree})$ ← homog. of degree $r < p-1$

For $\lambda \in \mathbb{F}_p^\times$, order of $\lambda = p-1$

$$G(\lambda^4 x, \lambda^6 y) \mid A(\lambda^4 x, \lambda^6 y) - 1 = \lambda^{p-1} A(x,y) - 1 = A(x,y) - 1$$

So we get another divisor of $A(x,y)-1$.

Note that $G(\lambda^4 x, \lambda^6 y) = \underbrace{\lambda^r}_{\neq 1 \text{ b/c } r<p-1} G_r(x,y) + \cdots$

So $G(x,y)$ and $G(\lambda^4 x, \lambda^6 y)$ are <u>different</u>.

Hence $G(x,y)\, G(\lambda^4 x, \lambda^6 y) \mid A(x,y) - 1$.

Looking at the leading terms; get:

$\lambda^r G_r(x,y)^2 \mid A(x,y) \Rightarrow A(x,y)$ has a multiple factor ✓

The fact that $A(x,y)$ has no repeated factors is a classical result. We will see more about it later, but note that, assuming this fact, we have proven:

$$\bar{\pi} \cong \mathbb{F}_p[Q,R]/(A-1)$$

Then $\bar{\pi}$ has a natural grading by $\mathbb{Z}/(p-1)\mathbb{Z}$ (note that $\deg A = p-1 \overset{\deg 1}{\equiv} 0 \ (p-1)$)

So write $\bar{M} = \bigoplus_{j=0}^{p-2} \bar{M}_j$, where $\bar{M}_j$ = image of $\bigoplus_{\substack{k \equiv j \\ (\mathrm{mod}\ p-1)}} M_k \otimes \mathbb{F}_p$ in $\mathbb{F}_p[\![q]\!]$.

Now, suppose that $f \in M_k$, $g \in M_{k'}$.

Write $\bar{f} = F(Q,R)$, $\bar{g} = G(Q,R)$. (Assume $p \nmid f$)

If $f \equiv g \pmod p$, then

$F - G \in \ker \bar{\pi} \Rightarrow \deg F = \deg G \pmod{p-1} \Rightarrow k \equiv k' \pmod{p-1}$.

This is the main theorem, for the case $r = 1$.

Differential operators:

Define $\Theta = \frac{1}{2\pi i} \frac{d}{dz} = q \frac{d}{dq}$.

So $\Theta\left(\sum a_n q^n\right) = \sum n a_n q^n$.

The operator Θ operates nicely on q-expansions, but doesn't preserve M!

Let $f \in M_k$. Then $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$.

Apply Θ to both sides:

$$(cz+d)^{-2} (\Theta f)\left(\frac{az+b}{cz+d}\right) = (cz+d)^k (\Theta f)(z) + k \cdot c \cdot (cz+d)^{k-1} f(z).$$

The computation from the previous page yields:

$$(\Theta f)\left(\frac{az+b}{cz+d}\right) = (cz+d)^{k+2}(\Theta f)(z) + kc(cz+d)^{k+1} f(z)$$

We will now modify Θ so that it preserves M:

Def: $\partial_k := 12\Theta - kP \qquad (P = E_2)$.

Theorem: ∂_k maps M_k to M_{k+2}

Pf $$(P\cdot f)\left(\frac{az+b}{cz+d}\right) = (cz+d)^{k+2}(P\cdot f)(z) + \frac{12c}{2\pi i}(cz+d)^{k+1} f(z)$$

so letting $\partial_k = 12\Theta - kP$, we cancel the "pernicious" term. ∎

Aside: a note about PS 3, Assignment 4.

Thm: Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$.

Let $g = \text{genus}\left(\Gamma\backslash\mathcal{H}^*\right) = \dim S_2(\Gamma)$.

Let $t = \#\text{cusps} = \#\left(\Gamma\backslash\mathbb{P}_1(\mathbb{Q})\right) = \#\left[PSL_2(\mathbb{Z}) : \overline{\Gamma}\right]$.

Then: $\dim_{\mathbb{C}}\left(M^\Gamma\right) = 2g + t - 1$.

Pf (sketch)

Let $\mathcal{F} :=$ space of κ-valued functions on $\mathbb{P}_1(\mathbb{Q})$.

$M :=$ space of κ-valued modular symbols

Then we have an exact sequence:

$$0 \to \kappa \longrightarrow \mathcal{F} \xrightarrow{d} M \longrightarrow 0$$

$$f \longmapsto (df)\{x,y\} = f(y) - f(x)$$

The congruence subgroup Γ acts on these spaces,

Taking the Γ-group cohomology, get:

$$0 \to k \to \mathcal{F}^\Gamma \to M^\Gamma \xrightarrow{\delta} H^1(\Gamma, k) \to H^1(\Gamma, \mathcal{F}) \to H^1(\Gamma, M) \to \cdots$$

Fact: $\dim H^1(\Gamma, k) = 2g + t - 1$.

(it's the abelianization of the fundamental gp of a surface of genus g with t points removed).

Now write $\mathcal{F} = \bigoplus_{x \in \Gamma \backslash \mathcal{F}} \mathrm{Ind}_{\Gamma_x}^{\Gamma} k$. ← stabilizer of x.

By Shapiro's lemma, $H^1(\Gamma, \mathcal{F}) = H^1\left(\Gamma, \bigoplus \mathrm{Ind}_{\Gamma_x}^{\Gamma} k\right) = \bigoplus_{x \in \Gamma \backslash \mathcal{F}} H^1(\Gamma_x, k)$

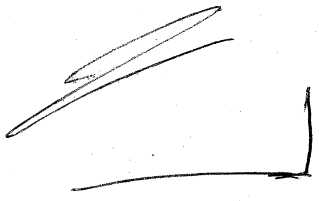
As Γ acts trivially on k,

$$H^1(\Gamma_x, k) = \mathrm{Hom}(\Gamma_x, k) \simeq k .$$

So $\dim_k H^1(\Gamma, \mathcal{F}) = t$

Finally, one needs to analyze the kernel of $H^1(\Gamma, \mathcal{F}) \to H^1(\Gamma, M)$, to show that it's one-dimensional.

Reference: Chapter II of H. Darmon's "Rational Points on Elliptic Curves".



Complementary Proposition:

$12\Theta P - P^2 \in M_4$

Remark: There is no 2 in front of P^2! ($12\Theta f - kPf \dots$).

Proof: exercise! //

Formulae: write $\partial_k := 12\Theta - kP$ (so $\partial_k f = \frac{12}{2\pi i}\frac{\partial f}{\partial \tau} - kPf$)

$12\Theta P - P^2 = -Q$

$\partial_4 Q = 12\Theta Q - 4PQ = -4R$

$\partial_6 R = 12\Theta R - 6PR = -6Q^2$

From this, we get:

$$\Theta P = \frac{P^2 - Q}{12}$$

$$\Theta Q = \frac{PQ - R}{3}$$

$$\Theta R = \frac{PR - Q^2}{2}$$

and so we find that Θ acts as a derivation on $\mathbb{Z}_{(p)}[P, Q, R]$, and on its image in $\mathbb{Z}_{(p)}[\![q]\!]$.

Define $\partial := \bigoplus_{k=0}^{\infty} \partial_k : M \to M$, which is a derivation of weight 2:

$\partial(fg) = (\partial f)\cdot g + f \cdot \partial g$

(that means that, if f has weight k and g has weight ℓ, then

$\partial_{k+\ell}(f \cdot g) = \partial_k f \cdot g + f \cdot \partial_\ell g$.).

• Differential equation satisfied by A.

Let $B(X,Y)$ be the unique homogeneous polynomial of degree $p+1$ such that $B(Q,R) = E_{(p+1)}$ ← not $p-1$!

Recall that $E_{p+1} = E_2^{\equiv p} \pmod p$ [b/c $p+1 \equiv 2 \pmod{p-1}$].

As $M \cong \mathbb{Z}_{(p)}[Q,R]$, ∂ acts also on polynomials:

Def If $F \in \mathbb{Z}_{(p)}[X,Y]$ is homogeneous of degree k,

$\partial F :=$ unique hom poly of deg $k+2$ s.t $(\partial F)(Q,R) = \partial_k(F(Q,R))$.

(so $\partial_4 X = -4Y$, $\partial_6 Y = -6X^2$).

Thm: 1) $\partial A = B$

2) $\partial B = -QA$

Pf 1) $(\partial A)(Q,R) = 12\,\theta E_{p-1} - (p-1)P E_{p-1}$

In $\mathbb{F}_p[\![q]\!]$, this is $\equiv 0 + P \cdot 1 \equiv P \equiv E_{p+1}$.

Hence $\partial A = B$. (b/c $\deg(\partial A) = \deg B$).

2) is done in the same way. (exercise). ∎

This will allow us to prove that $A(X,Y)$ has no multiple factors, and thus give the structure of the modular forms mod p.

Theorem: $A(X,Y)$ has no multiple factors in $\mathbb{F}_p[X,Y]$.

Pf Suppose that $F(X,Y)$ is an irreducible polynomial such that $F^a \| A$, $a > 1$.

As A is homogeneous, F will be as well.

Write $A = F^a \tilde{A}$, $F \nmid \tilde{A}$.

Differentiating, we get:

$$B = \partial A = a F^{a-1}(\partial F)\cdot \tilde{A} + F^a(\partial \tilde{A}).$$

Note that ∂F is not divisible by F (b/c there are no "polynomials" of degree 2 ($M_2 = 0$)).

So $(F, \partial F) = 1$, and

$B = \partial A = F^{a-1}\tilde{B}$, with $(F, \tilde{B}) = 1$.

Differentiating again ($a - 1 > 0$):

$$-QA = \partial^2 A = (a-1) F^{a-2}(\partial F)\tilde{B} + F^{a-1}(\partial \tilde{B}).$$

So $-QA = F^{a-2}\cdot C$, with $\gcd(C, F) = 1$. $\Rightarrow$!!

because $F^a \mid A$!

Rk: a and $a-1$ are nonzero (mod p!), because $\deg A = p \neq 1$, so $a < p-1$.

Remark: We have also shown that $\gcd(A, B) = 1$.

So far, we have the main theorem: ($f \equiv g \bmod p^r \Rightarrow k \equiv k' (p-1)p^{r-1}$ proved for the case $r = 1$).

Remark: $\bar{M} = \dfrac{\mathbb{F}_p[Q,R]}{(A-1)} = \bigoplus_{j=0}^{p-2} \bar{M}_j$ ← grading on $\mathbb{Z}/(p-1)$.

This implies at once our thm (for $r=1$).

Goal: Prove it for any $r > 1$.

For this, we introduce the filtration.

Def: The filtration, or weight of $f \in \bar{M}_j$ is the ~~unique~~ least $\kappa = w(f)$ such that $f = F(Q,R)$ for some polynomial of degree κ.

So $\kappa \equiv j \pmod{p-1}$

Properties: (would have equality if A was irreducible, but it never is!)

- $w(fg) \leq w(f) + w(g)$.
- $w(f+g) \leq \max\{w(f), w(g)\}$. (if $w(f) = w(g)$, $w(f+g)$ may decrease)

Define then $\bar{M}_j^{\kappa} := \{ f \in \bar{M}_j : w(f) \leq \kappa \}$.

Then $\bar{M}_j$ is filtered by these submodules.

$$\bar{M}_j^{j} \subseteq \bar{M}_j^{j+(p-1)} \subseteq \bar{M}_j^{j+2(p-1)} \subseteq \cdots \subseteq \bar{M}_j$$

Crucial remark: Θ preserves $\bar{M}$. More precisely, $\Theta(\bar{M}_j) \subseteq \bar{M}_{j+2}$, for $j \in \mathbb{Z}/(p-1)\mathbb{Z}$

Pf: Just note that the image of $\mathbb{Z}_{(p)}[P,Q,R]$ in $\mathbb{F}_p[[q]]$ equals image of $\mathbb{Z}_{(p)}[E_{p+1}, Q, R] =$ image of $\mathbb{Z}_{(p)}[Q,R] = \bar{M}$.

As Θ preserves $\mathbb{Z}_{(p)}[P,Q,R]$, then it preserves $\bar{M}$.

We want to understand now how Θ interacts with the filtration.

Prop: Let $f \in \bar{M}$.

a) $w(\Theta f) \leq w(f) + (p+1)$

b) $w(\Theta f) = w(f) + (p-1) \iff p \nmid w(f)$

c) If $p \mid w(f)$, then $w(\Theta f) \leq w(f) + 2$.

Pf: Deferred.

Examples of the Hasse invariant

$p=5 \to A(Q,R) = Q$

$p=7 \to A(Q,R) = R$

$p=11 \to A(Q,R) = QR$

$p=13 \to A(Q,R) = \alpha Q^3 + \beta R^2$

Q: What are $\alpha, \beta \in \mathbb{Z}/13\mathbb{Z}$?

Exercise.

We want to see now how this theory helps us on our guiding problem.

Prop: If $f \in M_k(\bar{\mathbb{Q}})$, $f = \sum_{n \geq 0} a_n(f) q^n$, and

a) $(p-1) \nmid k$

b) $a_n(f) \in \mathbb{Z}_{(p)}$ for all $n \geq 1$.

Then: $a_0(f) \in \mathbb{Z}_{(p)}$ as well.

Pf: Assume $p^t \| \text{denom}(a_0(f))$, $t \geq 1$ (to get a contradiction).

Consider $p^t \cdot f \in M_k$, and let $g :=$ image of $p^t f$ in $\bar{M}_k$.

Then $g \equiv c$ in $\mathbb{F}_p[\![q]\!]$, where $c \in \mathbb{F}_p^\times$. Then by the grading, $g \in \bar{M}_0$. But $g \in \bar{M}_k$ as well, contradicting $(p-1) \nmid k$.

Q: What if $(p-1) \mid k$?

The Prop is never true, as $E_{p-1} \equiv 1 \pmod p$. Or, if we want,

$$G_k = \zeta(1-k) + 2\sum \sigma_{k-1}(n)\, q^n$$

By C-VS, $p^t \zeta(1-k) \in \mathbb{Z}_{(p)}$, where $t-1 = v_p(k-1)$.

We will show that this counterexample is, in some sense, as bad as it gets.

Theorem: If $f = \sum a_n(f) q^n \in M_k \otimes \mathbb{Q}$ and $a_n(f) \in \mathbb{Z}_{(p)}$ $\forall n \geq 1$,

and $(p-1) \mid k$, and $t-1 = v_p(k)$, then:

$$p^t a_0(f) \in \mathbb{Z}_{(p)}.$$

Pf: Deferred.

Note that, in the previous easy prop, we used in a crucial way that $1 \notin \overline{M}_k$. We will find a modular form that doesn't belong to $\overline{M}_0$, and use this for our theorem.

Recall the previous unproven Prop:

Prop: Let $f \in \overline{M}$.

a) If $p \nmid w(f)$, then $w(\Theta f) = w(f) + p + 1$

b) If $p \mid w(f)$, then $w(\Theta f) \leq w(f) + 2$

Pf: If $w(f) = k$, then $\exists$ $F \in \mathbb{F}_p[Q, R]$ (of deg k) s.t. $F(Q,R) = f$, and $A \nmid F$.

$12\Theta f = \underbrace{\partial_k f}_{\text{weight } k+2} + kPf$. So define $\partial_k F$ s.t. $(\partial_k F)(Q,R) = \partial_k f$,

so $\partial_k F$ is a hom. poly. of deg $k+2$.

$\downarrow$

(cont pf of prop).

So we get: (we defined it last time. It's the one that represents $P = E_{p+1}$)

$$\underbrace{(\theta_k F)(Q,R)}_{k+2} + k \cdot \underbrace{F(Q,R)}_{\text{wt } k} \cdot \underbrace{B(Q,R)}_{p+1}.$$

Hence:

$$12\theta f = A(Q,R)(\theta_k F)(Q,R) + kB(Q,R)F(Q,R)$$

and RHS = hom. poly of degree $k+(p+1)$. So $w(\theta f) \leq k+(p+1)$.

We proved that $\gcd(A,B)=1$. Hence $A \nmid B(Q,R)F(Q,R)$.

Hence, if $p \nmid k$, $w(\theta f) = w(f) + p + 1$.

But if $p \mid k$, then this gets simplified to:

$$12\theta f = (\theta_k F)(Q,R) \Rightarrow w(\theta f) \leq k+2.$$

Theorem: If $(p-1) \mid k$, then $\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \in \mathbb{F}_p[\![q]\!]$ doesn't belong to $\overline{M}_0$, or even to $\mathrm{Frac}(\overline{M}_0)$.

Remark: if $(p-1) \nmid k$, then $\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$ does belong to $\overline{M}_k$ if $p \mid 5(1-k)$.

(e.g. $\sum_{n=1}^{\infty} \sigma_{11}(n) q^n \in \overline{M}_{12}$. for $p = 691$).

Pf

$$\sigma_{k-1}(n) = \sum_{d \mid n} d^{k-1} \overset{\text{write } n = p^t n',\ p \nmid n'}{\equiv} \sum_{d \mid n'} d^{k-1} \equiv \sum_{d \mid n'} d^{-1}$$

In particular, if $p \nmid n$, then $\sigma_{k-1}(n) \equiv \sigma_{-1}(n) \equiv \sum_{d \mid n} \frac{1}{d}$.

So $n\sigma_{-1}(n) = \sigma_1(n)$ $(\forall p \nmid n)$.

(cont pf of Thm).

Let $\varphi = \sum_{n \geq 1} \sigma_{k-1}(n) q^n$. Then $\Theta\varphi = \sum_{\substack{n \geq 1 \\ p \nmid n}} \sigma_k(n) q^n \overset{\text{why?}}{=} \Theta^{p-1} E_{p+1}$.

$\begin{cases} n^{p-1} \equiv 1 \pmod p & \text{if } p \nmid n \\ d^p \equiv d \pmod p \end{cases}$

Let $\varphi = \sum b(n) q^n$, $\Theta^{p-2} E_{p+1} = \sum c(n) q^n$.

Then, as $\Theta\varphi = \Theta\,\Theta^{p-2} E_{p+1}$, we have

$n\,b(n) = n\,c(n)$ $\forall n$. Hence $b(n) \equiv c(n) \pmod p$ if $p \nmid n$.

What about $b(n'p^t)$? $b(n'p^t) = b(n')$.

On the other side, $c(n'p^t) = 0$.

Consider then $\varphi - \varphi^p$. It has the same Fourier coeffs as $\Theta^{p-2} E_{p+1}$.

So $\varphi - \varphi^p = \Theta^{p-2} E_{p+1}$.

We compute now their weights, to get a contradiction:

$w(\varphi) = k$, and $w(\varphi^p) = p \cdot k$ (if $A \neq F$, then $A \neq F^p$).

To compute $w(\varphi - \varphi^p)$, we need to know:

$\varphi - \varphi^p = F(Q,R) \cdot A^k(Q,R) - F^p(Q,R)$ is not divisible by Δ,

so that $w(\varphi - \varphi^p) = pk$.

On the other hand, $w(E_{p+1}) = p+1$, $w(\Theta E_{p+1}) = 2(p+1)$, ... $w(\Theta^{p-2} E_{p+1}) =$

$w(\Theta^{p-2} E_{p+1}) = (p-1)(p+1) = p^2 - 1$ (by our prev. Prop).

This is a contradiction, as $p^2 - 1 \neq kp$. !!

So $\varphi - \varphi^p \notin \overline{M}_0$. But $\overline{M}_0$ is integrally closed, so $\varphi \notin \overline{M}_0$, or is not a Fourier polynomial.

We now go a little back, to prove:

Thm: If $f = \sum a_n(f) q^n \in M_k \otimes \mathbb{Q}$ and $a_n(f) \in \mathbb{Z}_{(p)}$, $\forall n \geq 1$,

and $(p-1) \mid k$, $t = v_p(k) + 1$.

Then: $p^t a_0(f) \in \mathbb{Z}_{(p)}$.

pf/ Assume that $p^{t_1} \| \text{denom}(a_0(f))$, with $t_1 > t$. want to get a contradict

Consider:

$$p^{t_1}\left(\zeta(1-k)\cdot f - a_0(f)\, G_k\right) =: g.$$

Note that $a_0(g) = 0$, and $a_n(g) \equiv \lambda\, \sigma_{k-1}(n) \pmod{p}$, $\lambda \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$.

But then $\overline{g} = \lambda \varphi$, which contradicts the previous proposition. //

Corollary: If $f \in M_k \otimes \mathbb{Q}$, $g \in M_\ell \otimes \mathbb{Q}$, and $a_n(f), a_n(g) \in \mathbb{Z}_{(p)}$.

Then, if $\begin{cases} a_n(f) \equiv a_n(g) \pmod{p^t} \ \forall n \geq 1 \\ k \equiv \ell \pmod{(p-1)p^{t-1}} \end{cases}$, then:

a) If $(p-1) \nmid k$ (and hence $(p-1) \nmid \ell$), then $a_0(f) \equiv a_0(g) \pmod{p^t}$.

b) If $(p-1) \mid k$ (and hence $(p-1) \mid \ell$), then:

$$p^{t_0} a_0(f) \equiv p^{t_0} a_0(g) \pmod{p^t}, \text{ for } t_0 := v_p(k) + 1$$

Proof:

Apply the previous result to $p^{-t}(f - E_h \cdot g) \in M_k$ (assume wlog $k > \ell$)

$k = \ell + h$, $(p-1) \mid h$.

Then $a_n(h) \in \mathbb{Z}_{(p)}$ for $n \geq 1 \Rightarrow a_0(h) \in \mathbb{Z}_{(p)}$ (part a).

Part (b) is proven similarly. //

Key Applications: Congruences of Clausen-Von Staudt type for totally-real fields.

Let $K/\mathbb{Q}$ be a totally real field.

$$\zeta_K(s) := \sum_{\mathfrak{a} \triangleleft \mathcal{O}_K} (N\mathfrak{a})^{-s} = \prod_{\mathfrak{p} \triangleleft \mathcal{O}_K} \left(1 - (N\mathfrak{p})^{-s}\right)^{-1}$$

($\zeta_K(1-k) \equiv 0$ for $k \geq 2$ if K is not totally real. Hence our assumption)

Denote by $r := [K:\mathbb{Q}]$, and let $\iota_1, \dots, \iota_r : K \hookrightarrow \mathbb{R}$ the distinct embeddings.

If $x \in K$, write $x_j := \iota_j(x) \in \mathbb{R}$.

We get then an embedding $K \hookrightarrow \mathbb{R}^r$. The image of $\mathcal{O}_K$ is a lattice in $\mathbb{R}^r$, of rank r.

Theorem (Hecke, Siegel): The values $\zeta_K(1-k)$, for $k \geq 2$ even are all rational nonzero (and occur as the constant term of a particular modular form of weight $r \cdot k$ on $SL_2(\mathbb{Z})$).

Pf (sketch):

Uses Eisenstein series on the Hilbert Modular group: $SL_2(\mathcal{O}_K)$.

Using $\iota_1, \dots, \iota_r$, can embed $SL_2(\mathcal{O}_K) \hookrightarrow SL_2(\mathbb{R})^r$

Then $SL_2(\mathcal{O}_K)$ acts on $\mathcal{H}^r$ (r copies of the upper half plane), with discrete orbits.

This leads to the notion of Hilbert modular forms:

$f(\tau_1, \dots, \tau_r)$ holomorphic on $\mathcal{H}^r$ which satisfies:

$$f\left(\frac{a_1\tau_1 + b_1}{c_1\tau_1 + d_1}, \frac{a_2\tau_2 + b_2}{c_2\tau_2 + d_2}, \dots, \frac{a_r\tau_r + b_r}{c_r\tau_r + d_r}\right) = (c_1\tau_1 + d_1)^k \cdots (c_r\tau_r + d_r)^k f(\tau_1, \dots, \tau_r)$$

(+ assumption at cusps).

(continues sketch of pf)

Let I be an (integral) ideal of $\mathcal{O}_K$. Define:

$$G_{I,k}^{(\tau_1,\tau_r)} := (2\pi i)^k (NI)^k \cdot \sum'_{(m,n) \in \frac{I^2 \setminus (0,0)}{\mathcal{O}_K^\times}} (m_1\tau_1+n_1)^{-k} \cdots (m_r\tau_r+n_r)^{-k}$$

This definition depends only on the ideal class of I (in $Cl(K)$).

The Eisenstein series for K are then:

$$G_{K,k}(\tau_1,\dots,\tau_r) := \sum_{\bar{I} \in Cl(K)} G_{I,k}$$

Basic properties of $G_{K,k}$:

a) $G_{K,k}(\gamma_1\tau_1,\dots,\gamma_r\tau_r) = (c_1\tau_1+d_1)^k \cdots (c_r\tau_r+d_r)^k G_{K,k}(\tau_1,\dots,\tau_r)$

for all $\gamma \in SL_2(\mathcal{O}_K)$. (even for $k=2$)

b) Fourier expansions:

Let $\delta :=$ different ideal. (dual of $\mathcal{O}_K$ w.r.t $Tr: K\times K \to \mathbb{Q}$).

$$G_{K,k} = \zeta_K(1-k) + 2^r \sum_{\substack{n \in \delta^{-1} \\ n>>0}} \sigma_{k-1}(\delta n)\, e^{2\pi i (n_1\tau_1+\cdots+n_r\tau_r)}$$

where $n>>0$ means that $n_1>0,\dots,n_r>0$.

$\sigma_{k-1}(I) := \sum_{J|I} N(J)^{k-1}$ for I an integral ideal.

The calculation to prove these properties is completely analogous to the one done for the classical Eisenstein series.

(For more reading: Thesis of Pierre Charollois).

(continues the sketch of pf).

Define then:

$$g_k(\tau) := G_{k,x}(\tau, \tau, \dots, \tau)$$

This is a modular form of weight kr on $SL_2(\mathbb{Z})$, with Fourier coeffs in $\mathbb{C}$. (a priori).

$$g_k = \zeta_K(1-k) + 2^r \sum_{n=1}^{\infty} \left(\sum_{\substack{x \in \delta^{-1} \\ x >> 0 \\ \mathrm{Tr}(x) = n}} \sigma_{k-1}(\delta x) \right) e^{2\pi i n \tau}$$

Then, $a_n(g_k) = \sum_{\substack{x \in \delta^{-1} \\ x >> 0 \\ \mathrm{Tr}(x) = n}} \sum_{I \mid \delta x} (NI)^{k-1}$ ← finite sums!

Theorem: Suppose that

a) $k_1 \equiv k_2 \pmod{(p-1)p^{t-1}}$

b) $k_1, k_2 \geq t$

c) $(p-1) \nmid k_1$ (and hence k_2)

Then $\zeta_K(1-k_1) \equiv \zeta_K(1-k_2) \pmod{p^t}$

pf $a_n(g_{k_1}) \equiv a_n(g_{k_2}) \pmod{p^t} \quad \forall n \geq 1$

Also, $k_1 \equiv k_2 \pmod{(p-1)p^{t-1}}$

prev result ⇓ ⇒ $a_0(g_{k_1}) \equiv a_0(g_{k_2}) \pmod{p^t}$

Theorem': Suppose that (a) and (b), but:

c') $(p-1) \mid k_1$ (and hence k_2), and let $t_0 := v_p(k_1)+1 < t$

Then: $p^{t_0} \zeta_K(1-k_1) \equiv p^{t_0} \zeta_K(1-k_2) \pmod{p^t}$.

pf Exercise (analogous).

Def: A p-adic modular form (in the sense of Serre) is a limit, in $\mathbb{Z}_p[\![q]\!]$, of forms $\{f_k\}$ of possibly varying weights k.

Theorem: Suppose that $f \in M_k$, $g \in M_\ell$. Assume that $f \equiv g \pmod{p^t}$. $(t \geq 1)$

Then: $k \equiv \ell \pmod{(p-1)p^{t-1}}$.

Proof: The case $t=1$ was proved in the context of mod-p modular forms. Also, $f \equiv \bar{g}$, so $k \equiv \ell \pmod{p-1}$.
Assume WLOG that $k > \ell$, write $k = \ell + h$.

Consider $f - g \cdot E_h = \underbrace{f-g}_{\text{divisible by } p^t} + g(1 - E_h)$

Let $t_0 := \text{ord}_p(h) + 1$, want to prove that $t_0 \geq t$.

So assume that $t_0 < t$.

Then $M_k \ni \dfrac{f - gE_h}{p^{t_0}} = \dfrac{f-g}{p^{t_0}} + g\left(\dfrac{1-E_h}{p^{t_0}}\right)$.

Reducing, the first summand goes away. So we get:

$$\bar{g} \cdot \varphi \in \overline{M}_0, \text{ where } \varphi = \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

This means that $\varphi \in \text{Frac}(M_0)$ - which is a contradiction, since $(p-1) \nmid k$. //

Corollary: A p-adic modular form $f = \sum_i f_{k_i}$ has a well-defined weight in $\mathbb{Z}/_{p-1} \times \mathbb{Z}_p$, $k(f) = \sum_i k_i$.

We want to extend the results of the previous lectures to the case of a number field, not necessarily totally real.

Exercise: Show that, if F is not totally real, then $\zeta_F(1-n)=0 \quad \forall n>0$.

From now on, we focus on the case $F=$ quadratic imaginary field.

Assume also (although this wouldn't be necessary) that $h(F)=1$ (i.e. $\mathcal{O}_F$ is a PID).

Idea: $\zeta_F(s)=\frac{1}{\#\mathcal{O}_F^\times}\sum_{\alpha\in\mathcal{O}_F\setminus(0)}(\alpha\bar{\alpha})^{-s}$

Choose a complex embedding $K\hookrightarrow\mathbb{C}$ and consider then only the powers of α, instead of their norm:

Def: $\zeta_F(n_1,n_2):=\sum_{\alpha\in\mathcal{O}_F}\alpha^{-n_1}\cdot\bar{\alpha}^{-n_2}$ ("Hurwitz Numbers").

($n_1,n_2\in\mathbb{Z}$ because α is a complex number, so have otherwise problems with the choice of the branch of logarithm).

Basic Properties:

1) Converges (absolutely) if $n_1+n_2>2$.

2) If $n_1\not\equiv n_2 \pmod 2$, then $\zeta_F(n_1,n_2)=0$ ($\because -1\in\mathcal{O}_F^\times$).

3) $\zeta_F(n_1,n_2)=\overline{\zeta_F(n_2,n_1)}$ (Remark: as $\mathcal{O}_F$ is stable under conjugation, $\overline{\zeta_F(n_2,n_1)}=\zeta_F(n_2,n_1)$)

4) $\zeta_F(n,n)=\zeta_F(n)\in$ the usual definition.

Q: What are the critical values (in the sense of Deligne).

• Relation between $\zeta_F(n_1, n_2)$ and special values of Hecke L-series.

Given $r \geq 0$, define $f_r := \sum_{\alpha \in \mathcal{O}_F \setminus \{0\}} \alpha^{*} q^{\alpha\bar{\alpha}}$

Claim: f_r is a modular form of weight $r+1$ on $\Gamma_0(D^5)$, $D = \mathrm{disc}(F)$ with character $\varepsilon_F : G_{\mathbb{Q}} \to \{\pm 1\}$ (action of $G_{\mathbb{Q}}$ on F).

Recall: For any quadratic form Q on Λ (a lattice), then $\Theta_Q = \sum_{v \in \Lambda \setminus \{0\}} q^{Q(v)}$ is a modular form of weight $\frac{1}{2}\mathrm{rank}(\Lambda)$.

More generally, for any P a harmonic polynomial, with $P(0) = 0$

$\Theta_{P,Q} := \sum P(v) q^{Q(v)}$ is also modular form (a cusp form, actually) of weight $\frac{1}{2}\mathrm{rank}(\Lambda) + \deg P$.

In our case, the weight is $r+1$.

Lemma: Suppose that $r := n_2 - n_1 \geq 0$.

Then $\zeta_F(n_1, n_2) = L(f_r, n_2)$

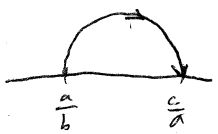
Pf $\zeta_F(n_1, n_2) = \sum_{\alpha \neq 0} \alpha^{-n_1} \bar{\alpha}^{-n_2} = \sum_{\alpha \neq 0} \alpha^{n_2 - n_1} (\alpha\bar{\alpha})^{-n_2}$, $f_r = \sum_{\alpha \neq 0} \alpha^{n_2 - n_1} q^{\alpha\bar{\alpha}}$

On the other hand, $L(f_r, s) = \sum \alpha^{n_2 - n_1} (\alpha\bar{\alpha})^{-s}$

Theorem (Shimura): Let f be a ~~modular form~~ normalized eigenform (cusp) of weight $k \geq 2$.

Then there exist a period Ω_f^+ ~~(Ω_f^-)~~ such that:

$$\mathrm{Re}\left(\int_{a/b}^{c/d} f(\tau) P(\tau) d\tau \right) \in \Omega_f^+ \bar{\mathbb{Q}}.$$



for all $\frac{a}{b}, \frac{c}{d} \in \mathbb{P}_1(\mathbb{Q})$, and for all $P(\tau) \in \bar{\mathbb{Q}}[\tau]^{\deg \leq k-2}$.

(note that $SL_2(\mathbb{Z}) \subseteq \bar{\mathbb{Q}}[\tau]^{\deg \leq k-2}$ by $(P|_k\gamma)(\tau) := P\left(\frac{a\tau+b}{c\tau+d}\right)(c\tau+d)^{k-2}$)

(ommitted proof)

In particular,

$$\mathrm{Re}\left(\int_0^{i\infty} f(\tau) \tau^m d\tau \right) \Big/ \Omega_f^+ \in \bar{\mathbb{Q}} \qquad 0 \leq m \leq k-2.$$

$$\| \\ L(f, m+1)$$

(for m even, If it is odd, then have Ω_f^-, and one takes Im instead of Re).

So there is a critical range (namely $1 \leq m \leq k-1$) for which we expect algebraicity of the special values of $L(f, m)$.

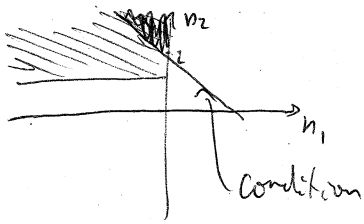
(note: for $k=2$, there is only the "critical point").

Recall now that $\xi_F(n_1, n_2) = L(f_r, n_2)$.

So we will impose $\begin{cases} n_2 - n_1 \geq 0 \\ 1 \leq n_2 \leq n_2 - n_1 = r \end{cases}$;

That is, $n_2 \geq 1$, $n_1 \leq 0$

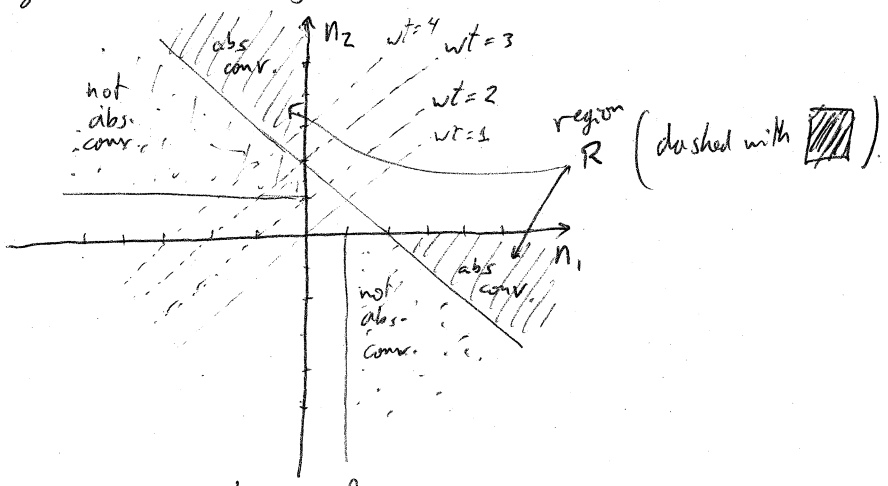
The critical range is then:



← the diagonal is not there!

Also, we must $n_1 \neq n_2$ (2)

Also, n_1 and n_2 can be interchanged (via the functional equation?), so we get the following region (critical range):



• Rationality properties of $\zeta_F(n_1, n_2)$ for $(n_1, n_2) \in R$

We will focus now on the cone in the 4th quadrant.

Key observation: write $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\omega$, $\omega \in \mathcal{H}$ (well defined up to $SL_2(\mathbb{Z})$).

Then $\zeta_F(k,0) = G_k(\omega)$, where $G_k(\tau) = \sum_{(m,n)}{}' (m+n\tau)^{-k}$

(the Eisenstein series of weight k).

Pf: $\zeta_F(k,0) = \sum_{\alpha \in \mathcal{O}_F - \{0\}} \alpha^{-k} = \sum_{(m,n)}{}' (m+n\omega)^{-k}$ //

The function $k \mapsto G_k(\infty)$ has p-adic interpolation. Want to replace ∞ by ω and get a similar statement.

The problem is that the x-axis and the y-axis (together) are not dense in $\mathbb{Z}^2$ (p-adically) and so we don't get good interpolation, we need more points.

Recall the Shimura-Maass operator:

$\delta_k = \left(\frac{d}{d\tau} + \frac{k}{\tau-\bar{\tau}}\right)\cdot\frac{1}{2\pi i} =: \delta_k$. But we'll omit the $\frac{1}{2\pi i}$ for a few lectures!

It is a differential operator that sends: $M_k \longrightarrow M^{nh}_{k+2}$,

where M^{nh}_{k+2} = "nearly holomorphic modular forms of wt $k+2$".

Theorem: $\delta_k G_k(\omega) = \frac{k}{\omega-\bar{\omega}}\,\zeta_F(k+1,-1)$

Pf: $\delta_k (m+n\tau)^{-k} = -kn\,(m+n\tau)^{-k-1} + \frac{k}{\tau-\bar{\tau}}(m+n\tau)^{-k} =$

$$= (m+n\tau)^{-(k+1)}\left(-kn + \frac{k}{\tau-\bar{\tau}}(m+n\tau)\right)$$

$$= (m+n\tau)^{-(k+1)}\,\frac{k(m+n\bar{\tau})}{\tau-\bar{\tau}}$$

So $\delta_k G_k(\tau) = \frac{k}{\tau-\bar{\tau}}\sum_{(m,n)}{}' (m+n\tau)^{-(k+1)}(m+n\bar{\tau})$.

at ω, get $\delta_k G_k(\omega) = \frac{k}{\omega-\bar{\omega}}\sum (m+n\omega)^{-(k+1)}(m+n\bar{\omega}) = \frac{k}{\omega-\bar{\omega}}\zeta_F(k+1,-1)$ //

This gives us a new row of values in the cone we are looking at.

We want to iterate this:

Thm: $(\delta_{k+2}\delta_k G_k)(\omega) = \frac{k(k+1)}{(\omega-\bar{\omega})^2}\,\zeta_F(k+2,-2)$

↓

Proof (this is similar to the general case):

We know $\delta_k (m+n\tau)^{-k} = \frac{k}{\tau-\bar{\tau}} (m+n\tau)^{-(k+1)} (m+n\bar{\tau})$.

$$\delta_{k+2}\,\delta_k (m+n\tau)^{-k} = \frac{-k}{(\tau-\bar{\tau})^2} (m+n\tau)^{-(k+1)} (m+n\bar{\tau}) - \frac{k(k+1)\cdot n}{\tau-\bar{\tau}} (m+n\tau)^{-(k+2)} (m+n\bar{\tau})$$

$$+ \frac{(k+2)\,k}{(\tau-\bar{\tau})^2} (m+n\tau)^{-(k+1)} (m+n\bar{\tau})$$

$$= \frac{k(k+1)}{(\tau-\bar{\tau})^2} (m+n\tau)^{-(k+1)} (m+n\bar{\tau}) - \frac{k(k+1)n}{\tau-\bar{\tau}} (m+n\tau)^{-(k+2)} (m+n\bar{\tau})$$

$$= \frac{k(k+1)}{(\tau-\bar{\tau})^2} (m+n\tau)^{-(k+2)} (m+n\bar{\tau})^2 \left(\underbrace{\frac{(m+n\tau)}{(m+n\bar{\tau})} - \frac{n(\tau-\bar{\tau})}{(m+n\bar{\tau})}}_{=1} \right)$$

and we conclude the proof as before. //

The general theorem is: define first $\delta_k^r := \delta_{k+2(r-1)} \circ \delta_{k+2(r-3)} \circ \cdots \circ \delta_{k+2} \circ \delta_k$

Thm: $\delta_k^r G_k(\omega) = \frac{k(k+1)\cdots(k+r-1)}{(\omega-\bar{\omega})^r} \zeta_F(k+r, -r)$

Pf/ Exercise. ($r=0,1,2$ is already done). //

Theorem (Shimura): There exists a period Ω, depending only on F, such that, for all $f \in M_k$ with Fourier coefficients in $\mathbb{Q}$.

$$\frac{(\delta_k^r f)(\omega)}{\Omega^{k+2r}} \in \overline{\mathbb{Q}}$$

Corollary (to the Thm of Shimura):

$$\frac{\zeta_F(k+r,-r)}{\pi^k \, \Omega^{k+2r}} \in \overline{\mathbb{Q}}$$

(Pf:/ B/C $\frac{G_k}{\pi^{2k}}$ has rational fourier coefficients)

Recall now that there is a bijection:

$$\{\text{lattices}\} \longleftrightarrow \left\{\begin{array}{l}\text{Elliptic curves} \\ \text{together with a} \\ \text{non zero regular diff. on } E\end{array}\right\}$$

$$\Lambda \longmapsto (\mathbb{C}/\Lambda, dz)$$

$$\left\langle \int_\gamma \omega : \gamma \in H_1(E(\mathbb{C}),\mathbb{Z}) \right\rangle \longleftarrow (E,\omega)$$

• Algebraic Modular Forms.

Def: An algebraic modular form of weight k over a ring R_0 is a rule f which, to every pair $(E_{/R}, \omega_{/R})$, where R = an R_0-algebra, associates an element $f(E,\omega) \in R$;

subject to:

A1) If $\varphi: R_1 \to R_2$ is an R_0-algebra homomorphism, then:

$$f\left(\varphi\left(E_{/R_1}, \omega_{/R_1}\right)\right) = \varphi\left(f\left(E_{/R_1}, \omega_{/R_1}\right)\right) \quad \left(\begin{array}{l}\text{compatible} \\ \text{with base change}\end{array}\right)$$

A2) $f\left((E_{/R}, \lambda\omega_{/R})\right) = \lambda^{-k} f\left((E_{/R}, \omega_{/R})\right)$ for all $\lambda \in R^\times$

A3) $f\left(\left(\text{Tate}_q, \frac{dt}{t}\right) \otimes_{\mathbb{Z}} R[\tfrac{1}{6}]((q))\right)$ $\left(\in R[\tfrac{1}{6}]((q))\right)$ belongs to $R[\tfrac{1}{6}][[q]]$

(Tate$_q$: ← we'll define it now.)

(The expression $f((\text{Tate}_q, \frac{dt}{t}) \otimes \dots)$ is called the q-expansion of f.)

An elliptic curve over a ring R is a curve of genus 1 over R, equipped with an R-rational point $\mathcal{O}$, such that, for all $\varphi: R \to K$ (K a field),

$E \underset{\varphi}{\times} \operatorname{Spec} K$ is an elliptic curve over K.

Over K, one can use Riemann-Roch, and will get an equation:

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6 \quad , (\Delta \in R^\times.)$$

(x is defined up to $x \mapsto ax+b$, $a, b \in K$, $a \in K^\times$).

(y is defined up to $y \mapsto a'y + b'x + c'$, $a' \in K^\times$, $b', c' \in K$).

Remark: There are no elliptic curves over $\mathbb{Z}$! But there are plenty of alg. modular forms over $\mathbb{Z}$ ($\mathbb{Z} \to \mathbb{Z}_{(n)}, \dots$).

We also get a representable functor:

$$E : (R\text{-alg}) \longrightarrow (\text{Groups}).$$

$$E(S) = \{(x:y:z) \in \mathbb{P}_2(S) : Y^2 Z + a_1 XYZ + a_3 YZ^2 = X^3 + a_2 X^2 Z + a_4 XZ^2 + a_6 Z^3\}$$

(where $\mathbb{P}_2(S) = \{(x:y:z) \in S^3 \text{ s.t. } (x,y,z) = (1)S\} / S^\times$.

• Differential forms on E - Assume R is a PID, or some other "nice" r.ing.

Let $\mathcal{O}_E$ = sheaf of functions on E (the structure sheaf).

($\mathcal{O}_E(U)$ = { alg. functions which are regular on U }).

Let $\Omega_{E/R}$ = sheaf of regular differentials on E.

Example: Let $U = E - \{\infty\}$. Then:

$$\mathcal{O}_E(U) = R[x,y]/(E) \qquad (E) = \text{eq. of the curve.}$$

$$\Omega_E(U) = \big(R[x,y]\,dx + R[x,y]\,dy\big)/(dE)$$

(dE = eq obtained by applying d to the original eq).

Let D be a divisor on E, $D = \sum n_i P_i$, $n_i \in \mathbb{Z}$, $P_i \in E(R)$ (restricted definition)

$\mathcal{O}_E(D)$ = sheaf defined by $\mathcal{O}_E(D)(U) := \{ f$ such that $\operatorname{ord}_{P_i}(f) \geq -n_i \ \forall P_i \in U \}$

$\Omega_E(D)(U) := \{ \omega \in$ "Ω_E" s.t. $\operatorname{ord}_{P_i}(\omega) \geq -n_i \}$.

↑ meromorphic differentials

Theorem (Riemann-Roch): If X is a smooth curve over R, $H^0(X, \mathcal{O}_X(D))$ and $H^1(X, \Omega_X(D))$ are locally-free R-modules (Λ, R = PID, they are actually free). If $g = \text{genus}(X)$, then:

$$\operatorname{rank} H^0(E, \mathcal{O}_E(D)) - \operatorname{rank} H^0(E, \Omega_E(-D)) = 1 - g + \deg D.$$

If $X=\bar{E}$, $g=1$, then

- Take $D=0$.

  Get $H^0(\bar{E}, \mathcal{O}_{\bar{E}}) = R = R\cdot 1 \Rightarrow H^0(E, \Omega_E) = R\cdot\omega_E$, (on compact $div\,\omega_E = 0$ $(\Rightarrow K = 0)$; ω_E: canonical divisor)

  where ω_E is well-defined up to $\omega_E \mapsto \lambda\omega_E$, $\lambda \in R^\times$.

- Take $D = n\cdot(\infty)$, $n = 1..6$ and get the equation of $\bar{E}$.

Key lemma: Let E/R be an elliptic curve (R a PID). Let ω_E be a regular differential on E. Assume that $6 \in R^\times$. Then there exist unique functions x, y on E ($x, y \in \mathcal{O}_E(E\cdot(\infty))$) such that:

a) x, y satisfy an equation of the form:

$$y^2 = x^3 + g_2 x + g_3 \quad , \; g_2, g_3 \in R.$$

b) $\omega_E = \frac{dx}{y}$.

Proof: exercise //.

Def: Given (E, ω_E), the functions x, y given by the "key lemma" are called the "canonical coordinates" on E, and the equation:

$$\left(y^2 = x^3 + g_2 x + g_3 \;,\; \frac{dx}{y}\right)$$ is called the "canonical equation" for the pair (E, ω_E).

Next we will see some examples of elliptic curves over rings.

Examples:

1) $R=\mathbb{C}$, $E=\mathbb{C}/\langle 1,\tau\rangle$ $\omega_E = dz$. The canonical equation is then:

$$\left(y^2 = 4x^3 + g_2 x + g_3,\ \frac{dx}{y}\right), \text{ where } \begin{cases} g_2 = -60 \sum_{m,n}{}' (m+n\tau)^{-4} \\ g_3 = -140 \sum_{n,n}{}' (m+n\tau)^{-6} \end{cases}$$

1') "The universal elliptic curve over $\mathcal{H}$":

$\left(y^2 = x^3 + g_2(\tau)x + g_3(\tau),\ \frac{dx}{y}\right)$ is an elliptic curve defined over the ring $\mathcal{O}_{\mathcal{H}}$ = ring of holomorphic functions on $\mathcal{H}$.

2) The Tate Curve:

$$\mathbb{C}/\langle 1,\tau\rangle \xrightarrow[\cong]{\varphi: z \mapsto e^{2\pi i z}} \mathbb{C}^\times/q^{\mathbb{Z}}, \quad q = e^{2\pi i \tau}$$

t

Q: What does correspond to dz?

A: Try $\frac{dt}{t}$: $\varphi^*\left(\frac{dt}{t}\right) = \frac{2\pi i\, e^{2\pi i z}}{e^{2\pi i z}} dz = 2\pi i\, dz$.

So dz corresponds to $\frac{1}{2\pi i}\frac{dt}{t}$

The canonical equation for the pair $\left(\mathbb{C}^\times/q^{\mathbb{Z}},\ \frac{dt}{t}\right)$ is of the form:

Tate q_m

$\left(y^2 = x^3 + \tilde{g}_2(q)x + \tilde{g}_3(q),\ \frac{dx}{y}\right)$, where $\tilde{g}_2, \tilde{g}_3$ belong to $\mathbb{Z}\left[\frac{1}{6}\right][\![q]\!]$.

The discriminant is $\Delta = q\prod_{n\geq 1}(1-q^n)^{24} \in \mathbb{Z}\left[\frac{1}{6}\right]((q))^\times$

Laurent series in q

Def: The pair $\left(\mathrm{Tate}_q, \frac{dt}{t}\right)$ is called the Tate curve. It is an elliptic curve over $\mathbb{Z}[\frac{1}{6}]((q))$.

Reference: Silverman's "Advanced Topics in the arithmetic of E.C."

We go back now to algebraic modular forms:

- **From algebraic to "classical" modular forms:**

Let f be an algebraic modular form over $\mathbb{C}$.

Consider the function $\tilde{f}(\tau) := f\left(\left(\mathbb{C}/\langle 1, \tau\rangle, dz\right)\right)$

Claim: $\tilde{f}$ is a modular form of weight k on $SL_2(\mathbb{Z})$.

Pf

- Invariance under $SL_2(\mathbb{Z})$:

$$\tilde{f}(\tau) = f\left(\mathbb{C}/\langle 1, \tau\rangle, dz\right) = f\left(\frac{\mathbb{C}}{\langle c\tau+d,\ a\tau+b\rangle}, dz\right) = f\left(\frac{\mathbb{C}}{\langle 1, \frac{a\tau+b}{c\tau+d}\rangle}, (c\tau+d)dz'\right)$$

$$= (c\tau+d)^{-k} f\left(\frac{\mathbb{C}}{\langle 1, \frac{a\tau+b}{c\tau+d}\rangle}, dz'\right) = (c\tau+d)^{-k}\, \tilde{f}\left(\frac{a\tau+b}{c\tau+d}\right). \quad \checkmark$$

- Holomorphicity:

Note that $\tilde{f}(\tau) = f\left(\underbrace{(y^2 = x^3 + g_2(\tau)x + g_3(\tau))}_{\text{def over } \mathcal{O}_{\mathcal{H}}}, \frac{dx}{y}\right) \in \mathcal{O}_{\mathcal{H}}$.

- Growth at ∞ comes from A3.

• The q-expansion principle.

It says that the map (K ~~field~~ any field $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$)

$$\left\{ \begin{array}{l} \text{algebraic} \\ \text{modular forms} \\ \text{over } K \end{array} \right\} \xrightarrow{q\text{-exp}} K[\![q]\!]$$

is injective, and its image is exactly $M_k(SL_2(\mathbb{Z}); K) \subseteq K[\![q]\!]$

(it's actually a map of K-~~vectorspaces~~ algebras)

Proof:

Injectivity: Suppose that $f(\mathrm{Tate}_q, \frac{dt}{t}) = 0$. We want to see that $f = 0$.

If (E, ω) is any test object defined over $\mathbb{C}$, then

$$f(E,\omega) = f\left(\mathbb{C}/\langle 1, \tau\rangle, \lambda\, dz\right) = 0$$

← value of q-expansion at $q = e^{2\pi i \tau}$.

If now R is any K-algebra, and $K \to \mathbb{C}$ is a homomorphism,

then $\varphi\left(f(E/R, \omega/R)\right) = f\left((E/R, \omega/R) \otimes \mathbb{C}\right) = 0 \Rightarrow f(E/R, \omega/R) = 0$ //

(*) ↑ we'll clarify this later. (on pg 48, back).

Remark: We also have a map

$$\left\{ \begin{array}{l} \text{alg-mod. forms} \\ \text{over } \mathbb{F}_p \end{array} \right\} \longrightarrow \mathbb{F}_p[\![q]\!]$$

but this is not injective, as the image of the Hasse invariant is the same as the element 1.

Surjectivity:

We know $M(SL_2(\mathbb{Z}), K) = \bigoplus_{k \geq 0} M_k(SL_2(\mathbb{Z}), K) = K[E_4, E_6]$. It's enough to show that E_4 and E_6 are algebraic mod. forms of weights 4, 6.

(cont pf of q-expansion ppl):

Given $(E,\omega)/R$ we saw (Kelly Lemma) that there exist unique $X, Y \in H^0(E\setminus O, \mathcal{O}_E)$ and $g_2, g_3 \in R$ such that:

$$y^2 = x^3 + g_2 x + g_3 \quad , \quad \omega = \frac{dx}{y}$$

Define then $E_4(E,\omega) := \alpha \cdot g_2$, $E_6^{(E,\omega)} := \beta g_3$

(where $\alpha, \beta \in \mathbb{Z}[\frac{1}{6}]^\times$ are the appropriate constants)

Proposition: Let $\tau \in \mathcal{H}$, and suppose that $\mathbb{C}/\langle 1,\tau\rangle$ is isomorphic to an elliptic curve defined over a field K.

Then: there is a period $\Omega_\tau \in \mathbb{C}^\times$ such that

$$\frac{f(\tau)}{\Omega_\tau^k} \in K \quad \text{for all } f \in M_k(SL_2(\mathbb{Z}), K)$$

Proof: By hypothesis, there is an isomorphism $\varphi: \mathbb{C}/\langle 1,\tau\rangle \xrightarrow{\sim} E^{alg}$, where E^{alg} is defined over K.

Let ω be a regular differential on E^{alg}/K.

Then $\varphi^*\omega = \Omega_\tau dz$ (Ω_τ is defined to be the constant we get in this expression).

(if ω is changed by $\lambda \in K^\times$, the conclusion of the theorem is not affected!)

$$f(\tau) = f\left(\mathbb{C}/\langle 1,\tau\rangle, dz\right) = f\left(\mathbb{C}/\langle 1,\tau\rangle, \frac{1}{\Omega_\tau}\cdot\varphi^*\omega\right) = \frac{f\left(\mathbb{C}/\langle 1,\tau\rangle, \varphi^*\omega\right)}{\Omega_\tau^k}$$

$$= \Omega_\tau^{-k} f\left(\mathbb{C}/\langle 1,\tau\rangle, \varphi^*\omega\right) = \Omega_\tau^{-k} f\left((E_\tau^{alg},\omega)\otimes_{K,\varphi} \mathbb{C}\right) = \Omega_\tau^{-k} \underbrace{f(E_\tau^{alg},\omega)}_{\in K}$$

Theorem: Let $F \subseteq \mathbb{C}$ be an imaginary quadratic field, and let $\tau \in \mathcal{H} \cap F$. Then $\mathbb{C}/\langle 1, \tau \rangle$ is isomorphic to an elliptic curve defined over $\overline{\mathbb{Q}}$ (more precisely, it's defined over some abelian extension of F).

Pf (sketch):

$$\mathrm{End}_{\mathbb{C}}\left(\mathbb{C}/\langle 1,\tau\rangle\right) \cong \left\{ \alpha \in \mathbb{C} : \begin{cases} \alpha\tau = a\tau + b \\ \alpha \cdot 1 = c\tau + d \end{cases} \text{ for some } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \right\}$$

If τ doesn't satisfy a quadratic equation with coefficients in $\mathbb{Z}$, then $\mathrm{End}_{\mathbb{C}}\left(\mathbb{C}/\langle 1,\tau\rangle\right) \cong \mathbb{Z}$, because only diagonal matrices are there.

If, on the contrary, $\tau \in \mathcal{H} \cap F$, so $\tau^2 + t\tau + p = 0$ for some $t, p \in \mathbb{Q}$, then $\mathrm{End}_{\mathbb{C}}\left(\mathbb{C}/\langle 1,\tau\rangle\right) \cong \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : (c, d-a, -b) \sim (1, t, p) \right\}$.

The ring $\mathrm{End}_{\mathbb{C}}\left(\mathbb{C}/\langle 1,\tau\rangle\right)$ is contained in F, and it is free of rank 2 as a $\mathbb{Z}$-module. Such a ring is called an order in F. It is of the form $\mathcal{O} = \mathbb{Z} + \mathbb{Z}\omega$.

Fix now this order $\mathcal{O}$, and consider the collection of $E/\mathbb{C}$ (modulo isomorphism) satisfying $\mathrm{End}_{\mathbb{C}}(E) \cong \mathcal{O}$.

Lemma: The collection of such isomorphism classes is a finite set, in bijection with the class group of $\mathcal{O}$, $\mathcal{CL}(\mathcal{O})$.

(map $[I] \in \mathcal{CL}(\mathcal{O}) \longmapsto \mathbb{C}/I$)

Let $\{E_1, \dots, E_h\}$ be the collection of representatives for these isom-classes.

Consider the j-invariants $j(E_1), \dots, j(E_h)$.

If $\sigma \in \mathrm{Aut}(\mathbb{C}/\bar{\mathbb{Q}})$, then $j(E_i)^\sigma = j(E_{\sigma(i)})$ for some permutation of the indices.

Therefore, the ~~sets~~ $j(E_i) \in \bar{\mathbb{Q}}$.

References:

- Serre's article in Cassels-Frohlich.
- Chapter in Silverman's A.T. (vol II).

Corollary: If $\tau \in \mathcal{H} \cap F$, then there exists $\Omega_\tau \in \mathbb{C}^\times$ s.t

$$\frac{f(\tau)}{\Omega_\tau^k} \in \bar{\mathbb{Q}} \quad \forall f \in M_k(SL_2(\mathbb{Z}), \bar{\mathbb{Q}}).$$

Pf/ τ corresponds to $\mathbb{C}/\langle 1, \tau \rangle$ which corresponds to an algebraic elliptic curve, so we are done.

Now we want to understand $\delta_k f(\tau)$, $\delta_k^r f(\tau)$.

Theorem: If $\tau \in \mathcal{H} \cap F$, then $\frac{f(\tau)}{\Omega_\tau^k} \in \bar{\mathbb{Q}} \quad \forall f \in M_k(\Gamma, \bar{\mathbb{Q}})$

for any $\Gamma(N) \subseteq \Gamma \subseteq SL_2(\mathbb{Z})$ (congruence subgroup).

$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}$

The idea in the previous theorem is to interpret also

$M_k(\Gamma, \bar{\mathbb{Q}})$ as algebraic modular forms.

So the definition has to be extended:

The "test objects" are now $(E, \omega, \{P_1, P_2\})_{/K}$, where P_1, P_2 are a basis for $E[N]$ (the N-torsion)

To $f(E, \omega, (P_1, P_2))$ we associate $f(\tau) := f\left(\mathbb{C}/\langle 1, \tau\rangle, dz, \left(\frac{1}{N}, \frac{\tau}{N}\right)\right)$

Define now $\tilde{M}_k := \varinjlim_{\Gamma} M_k(\Gamma, \bar{\mathbb{Q}})$ (Γ varying N!) $\circlearrowleft SL_2(\mathbb{Q})$ $(f \mapsto f|_k\gamma)$. ; $\tilde{M} = \bigoplus_{k \geq 0} \tilde{M}_k$

we enlarge it still further by considering the fraction field: $\tilde{M}^+ = \bigoplus_{k \in \mathbb{Z}} \tilde{M}_k^+$

Prop: If $f \in \tilde{M}_k^+$ and f is defined on τ, then

$$\frac{f(\tau)}{\Omega_\tau^k} \in \bar{\mathbb{Q}}$$

← that will be Step 3.

In fact, we prove ~~instead~~ first Step 2:

Thm: $\frac{f(\tau)}{\Omega_\tau^k} \in \bar{\mathbb{Q}}$, for all $f \in M_k(\Gamma, \bar{\mathbb{Q}})$ (Γ a congruence subgroup).

Pf (sketch):

We may assume that $\Gamma = \Gamma(N)$. A modular form f on $\Gamma(N)$ can be interpreted a rule which associates to every triple

$(E, \omega, (P_1, P_2))_{/\mathbb{C}}$ ($E/\mathbb{Q}$ an elliptic curve, $\Omega \in H^0(E, \Omega^1)$, (P_1, P_2) a $\frac{\mathbb{Z}}{N\mathbb{Z}}$-basis for $E[N]$). $f(\tau) = f\left(\mathbb{C}/\langle 1, \tau\rangle, dz, \left(\frac{1}{N}, \frac{\tau}{N}\right)\right)$.

Thus levels, as we saw, to algebraic modular forms, exactly as before.

What about the Tate curve:

The "natural" basis for $E_{Tate}[N]$ would be $(\zeta_N, q^{\frac{1}{N}})$.

So it is defined on $\mathbb{Z}[\zeta_N]((q^{\frac{1}{N}}))$

(the q-expansions at the different cusps are given by evaluating the modular form on E_{Tate}, but with basis $(\zeta_N^a q^{b/N}, \zeta_N^c q^{d/N})$, for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$).

Fact: f is an algebraic modular form over a ring R if, and only if,

$$f\left(\mathrm{Tate}_q, \frac{dt}{t}, (\zeta_N, q^{\frac{1}{N}})\right) \in R[\zeta_N][\![q^{\frac{1}{N}}]\!]$$

← Called the q-expansion principle.

(so only need to check at one cusp).

Now, we can write:

$$f(\tau) = f\left(\mathbb{C}/\langle 1, \tau\rangle, dz, \left(\tfrac{1}{N}, \tfrac{\tau}{N}\right)\right) = f\left(A_\tau, \Omega_\tau^{-1}\frac{dx}{y}, (P_1, P_2)\right) =$$

(where P_1, P_2 are defined over F^{ab} $\quad (F = \mathbb{Q}(\tau))$.)

$$= \Omega_\tau^{+k} f\left(A_\tau, \frac{dx}{y}, (P_1, P_2)\right).$$

By the q-expansion principle, any classical modular form on $M_k(\Gamma, \bar{\mathbb{Q}})$ is algebraic, and so we are done.

Recall the definition one gave:

$$\widetilde{M}_k := \varinjlim_{\Gamma(N) \subseteq \Gamma \subseteq SL_2(\mathbb{Z})} M_k(\Gamma, \bar{\mathbb{Q}}) \quad , \quad \widetilde{M} := \bigoplus_{k \geq 0} \widetilde{M}_k$$

and the fraction field, $\widetilde{M}^+ = \mathrm{Frac}(\widetilde{M})$ ($\widetilde{M}$ is an integral domain)

(so $\widetilde{M}^+ = \bigoplus_{k \in \mathbb{Z}} \widetilde{M}_k^+$, where $\widetilde{M}_k^+$ is generated by $\frac{f}{g}$, $f \in \widetilde{M}_{k+\ell}$, $g \in \widetilde{M}_\ell$)

Next step (3): $r = 0$, but $f \in \widetilde{M}_k^+$

Pf $f(\tau)$ is in this case a $\bar{\mathbb{Q}}$-linear combination of expressions of the form

$\frac{g}{h}$, $g \in \widetilde{M}_{k+\ell}$, $h \in \widetilde{M}_\ell$, so it follows immediately. //

Step 4: $r = 1$, $k = 0$:

Theorem: For all $f \in \widetilde{M}_0^+$, we have:

$$\frac{(\delta_0 f)(\tau)}{\Omega_\tau^2} \in \bar{\mathbb{Q}}$$

Pf Enough to prove this if $f = \frac{g}{h}$, $g, h \in \widetilde{M}_k$ (in general, it would be a linear combination of those).

$$\delta_0(f) = \delta_0\left(\frac{g}{h}\right) = \frac{(\delta_0 g)h - g\,\delta_0 h}{h^2} = \frac{1}{2\pi i}\left(\frac{g'h - gh'}{h^2}\right)$$

Exercise: if $g, h \in \widetilde{M}_k$, then $[g,h] := \frac{1}{2\pi i}(g'h - gh')$ is in $\widetilde{M}_{2k+2}$. (cf assignment #10).

So $\delta_0 f \in \widetilde{M}_2^+$ $\Rightarrow$ We are done, by the previous step. //

Next, Step 5: $r=1$, k general:

Thm: $\dfrac{(\delta_k f)(\tau)}{\Omega_\tau^{k+2}} \in \bar{\mathbb{Q}} \quad \forall f \in \widetilde{M}_k$.

Pf Choose a matrix $M=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Q})$ such that $M\cdot\tau=\tau$

That is, $\begin{cases} a\tau+b=\alpha\tau \\ c\tau+d=\alpha \end{cases}$, where $\alpha \in F^\times = \bar{\mathbb{Q}}^\times$.

(we can do this because τ is quadratic imaginary, $\mathbb{Q}(\tau)=F$).

(just impose $c\neq 0$).

Apply now the slash operator:

$$(f|_k M)(\tau) = (c\tau+d)^{-k} f(M\tau) = (c\tau+d)^{-k} f(\tau)$$

Remark: $f|_k M \in \widetilde{M}_k$.

So $f|_k M = f\cdot h$ (*), $h \in \widetilde{M}_0^\times$ $\left(h(\tau)=(c\tau+d)^{-k}\right)$.

So $h(\tau)=(c\tau+d)^{-k}=\alpha^{-k} \in F^\times$.

We apply δ_k to both sides of (*):

$$\delta_k(f|_k M) = \delta_k(fh) \overset{\text{assign. \#9}}{=} (\delta_k f)h + f\cdot(\delta_0 h) \quad \text{(Leibniz formula)}$$

$\|$ ← ass #9

$(\delta_k f)|_{k+2} M$

Evaluating the resulting identity at τ, yields:

$$\left((\delta_k f)|_{k+2} M\right)(\tau) = (\delta_k f)(\tau)\, h(\tau) + f(\tau)(\delta_0 h)(\tau)$$

$(c\tau+d)^{-k-2}\cdot(\delta_k f)(\tau)$ (by ...)

2

(cont pf)

we get:

$$\alpha^{-k-2}(\delta_k f)(\tau) = (\delta_k f)(\tau)\cdot\alpha^{-k} + f(\tau)\cdot(\delta_0 h)(\tau).$$

So:

$$(\alpha^{-k-2} - \alpha^{-k})(\delta_k f)(\tau) = f(\tau)\cdot(\delta_0 h)(\tau)$$

Hence:

$$(\delta_k f)(\tau) = \overbrace{\alpha^k(\alpha^{-2}-1)^{-1}}^{F^k} f(\tau)(\delta_0 h)(\tau)$$

By Step 1, $\dfrac{f(\tau)}{\Omega_\tau^k} \in \overline{\mathcal{A}}$ $\Rightarrow$ ✓.

By Step 4, $\dfrac{(\delta_0 h)(\tau)}{\Omega_\tau^2} \in \overline{\mathcal{A}}$.

Last Step: General r, k.

we just use the general Leibniz rule (Assy. #9):

$$\delta_k^r(f\cdot h) = \sum_{j=0}^{r} \binom{r}{j} (\delta_k^j f)(\delta_0^{r-j} h).$$

Theorem: $\dfrac{(\delta_k^r f)(\tau)}{\Omega_\tau^{k+2r}} \in \overline{\mathcal{A}}$, $\forall f \in \widetilde{M}_k^+$. $(\forall r \geq 0)$

pf Again, take the equation $(*)$: $f|_k M = f\cdot h$, and apply δ_k^r to both sides:

$$\delta_k^r(f|_k M) = \sum_{j=0}^{r}\binom{r}{j}(\delta_k^j f)(\delta_0^{r-j} h) = \delta_k^r f\cdot h + \sum_{j=0}^{r-1}\binom{r}{j}(\delta_k^j f)(\delta_0^{r-j} h)$$

$$\| \quad (\delta_k^r f)|_{k+2r} M$$

Again as before, we get the desired result: ∎

$$\alpha^{-k-2r}(\delta_k^r f)(\tau) = (\delta_k^r g)(\tau) \cdot \alpha^{-k} + \sum_{j=0}^{r-1} \binom{r}{j} (\delta_k^j g)(\tau)(\delta_0^{r-j} h)(\tau)$$

Hence:

$$(\delta_k^r f)(\tau) \cdot \alpha^{-k}(\alpha^{-2r}-1) = \sum_{j=0}^{r-1} \binom{r}{j} (\delta_k^j f)(\tau)(\delta_0^{r-j} h)(\tau)$$

Proceed by induction on r (has been done before for $r=0,1$).

$$\frac{(\delta_k^j g)(\tau)}{\Omega_\tau^{k+2j}} \in \bar{\mathbb{Q}}, \qquad \frac{(\delta_0^{r-j} h)(\tau)}{\Omega_\tau^{2r-2j}} \in \bar{\mathbb{Q}}$$

Also, $\delta_0^{r-j} h = \delta_z^{r-j-1}(\delta_0 h)$, so we can apply ind. hyp here as well, to get $\frac{\delta_0^{r-j} h}{\Omega_\tau^{2r-2j}} \in \bar{\mathbb{Q}}$, and hence we are done.

Some remark about the universal elliptic curve:

Prop: There exists a universal pair $(E^{univ}, \omega^{univ})/R^{univ}$, where R^{univ} is a $\mathbb{Z}[\frac{1}{6}]$-algebra, such that: if $(E,\omega)/R$ is any pair, with R a $\mathbb{Z}[\frac{1}{6}]$-algebra, then there is a unique

$$\lambda_{(E,\omega)} : R^{univ} \to R, \text{ a hom. of } \mathbb{Z}[\tfrac{1}{6}]\text{-algebras},$$

such that $(E,\omega)/R = (E^{univ}, \omega^{univ}) \otimes_{\lambda_{(E,\omega)}} R$

So we get a functor $\mathcal{F}: \mathbb{Z}[\frac{1}{6}]\text{-alg.} \to \text{Sets}$ which associates to R the set of all R-iso classes of $(E,\omega)/R$.

Actually, R^{univ} is defined to be:

$$\left(y^2 = x^3 + ax + b,\ \frac{dx}{y}\right) \Big/ \mathbb{Z}\left[\tfrac{1}{6}, a, b, \tfrac{1}{\Delta(a,b)}\right].$$

Now, let f be an algebraic modular form, and suppose that

$f\left((E,\omega)_{/\mathbb{C}}\right) = 0 \quad \forall\ (E,\omega)$ pair defined over $\mathbb{C}$.

Consider then $F(a,b) := f\left(\left(E^{univ}, \omega^{univ}\right)_{/\mathbb{Z}\left[\frac{1}{6}, a, b, \frac{1}{\Delta}\right]}\right) \in \mathbb{Z}\left[\tfrac{1}{6}, a, b, \tfrac{1}{\Delta}\right]$.

By compatibility with base change,

$$F(a,b) = 0 \quad \forall (a,b) \in \mathbb{C}^2 - (\text{zero locus of } \Delta).$$

$$\Rightarrow F \equiv 0 \ \text{(as a polynomial)}.$$

Remark: $F(a,b)$ is actually the expression of f as a homogeneous polynomial in (a,b) of weight $4, 6$, respectively.

$$M_k^{alg}(R) \xrightarrow{\text{Evaluation at } (E^{univ}, R^{univ})} R[a,b]^{hom-k}$$

Recall the theorem we just proved in last lecture:

Thm: If $\tau \in \mathcal{H} \cap F$, F a quadratic imaginary # field, then there exists $\Omega_\tau \in \mathbb{C}^\times$ s.t., $\forall f \in M_k^{alg}(\overline{\mathbb{Q}})$,

$$\frac{(\delta_k^r f)(\tau)}{\Omega_\tau^{k+2r}} \in \overline{\mathbb{Q}}.$$

Recall that we had defined:

$$\zeta_F(n_1,n_2) := \sum_{\alpha \in \mathcal{O}_F} \alpha^{-n_1} \bar{\alpha}^{-n_2}$$

If $\mathcal{O}_F = \mathbb{Z} + \mathbb{Z}\omega$, $\omega \in \mathcal{H}$, then we had seen that:

$$\frac{k(k+1)\cdots(k+r-1)}{(\omega-\bar{\omega})^r} \frac{\zeta_F(k+r,-r)}{\pi^k \Omega_F^{k+2r}} = \frac{\delta_k^r \tilde{G}_k(\omega)}{\Omega_F^{k+2r}} \in \bar{\mathbb{Q}} \qquad \begin{matrix} k \geq 2 \\ r \geq 0 \end{matrix}$$

(from the Thm)

Q: Can we interpolate ζ_F (or rather this algebraic multiple) to extend it to a p-adically continuous function on $\left(\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p\right)^2$?

Rk: The range $k \geq 2$, $r \geq 0$ gives $\{(k+r,-r)\}$ $\to$ a cone that we drew before, which has dense image in $\left(\mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}_p\right)^2$, so such an extension would be unique.

More general question: Let $M := \bigoplus_{k \geq 0} M_k$, $M_k = M_k(SL_2(\mathbb{Z}); \mathbb{Z})$.

Suppose that $f_1, f_2 \in M$.

Suppose that $f_1 \equiv f_2 \pmod{p^n}$, and that $p \nmid f_1$.

We know that $k_1 \equiv k_2 \pmod{(p-1)p^{n-1}}$. ($k_i$ = weight (f_i)).

Is it true that

a) $\dfrac{f_1(\omega)}{\Omega_{t\omega}^{k_1}} \equiv \dfrac{f_2(\omega)}{\Omega_{t\omega}^{k_2}} \pmod{p^n}$?

← needs to be refined, as at least we need p-integrality.

b) If $r_1 \equiv r_2 \pmod{(p-1)p^{n-1}}$, does that imply that ($f \in M_k$)

$$\frac{(\delta_k^{r_1} f)(\omega)}{\Omega^{k+2r_1}} \equiv \frac{(\delta_k^{r_2} f)(\omega)}{\Omega^{k+2r_2}} \quad ?$$

Consider now the rings:

- $M \otimes \mathbb{Z}_p$
- $M \otimes \mathbb{F}_p = \frac{M}{pM}$ $\leftarrow$ an $\mathbb{F}_p$-algebra.
- $\overline{M}$:= ring of modular forms mod p = image of M in $\mathbb{F}_p[\![q]\!]$,

$$\overline{M} = \frac{M \otimes \mathbb{F}_p}{(1 - E_{p-1})} \qquad E_{p-1} = \text{normalized Eisenstein series of wt } p-1.$$

$$\left(\overline{M} = \bigoplus_{j=0}^{p-2} \overline{M}_j \right).$$

We want to give a geometric interpretation of $\overline{M}$ and of $\overline{M}_0$.

Note first that $M \otimes \mathbb{Z}_p = M_K^{alg}(\mathbb{Z}_p)$

Likewise, $M_K \otimes \mathbb{F}_p = M_K^{alg}(\mathbb{F}_p)$

Note that any element of $\overline{M}_0$ can be written in the form $\frac{F}{A^r}$, for some r, where $F \in M_{r(p-1)} \otimes \mathbb{F}_p$

Hence, any $f \in \overline{M}_0$ gives rise to a function $(E, \omega) \mapsto f(E, \omega)$, provided that we restrict ourselves to pairs $(E, \omega)_{/R}$ for which $A(E, \omega) \in R^\times$

Def: A <u>modular form mod p</u> is a rule to which every $(E, \omega)_{/R}$, R an $\mathbb{F}_p$-algebra such that $A(E, \omega) \in R^\times$, associates some $f(E, \omega) \in R$.

Def: An elliptic curve E defined over $\overline{\mathbb{F}_p}$ satisfying $A(E,\omega)=0$ (for one, and hence all invariant differentials ω on E) is called **supersingular**.

Rk: There are finitely-many $E/\overline{\mathbb{F}_p}$ supersingular curves (in fact, there are roughly $\frac{p}{12}$).

- **Modular definition of the Hasse invariant.**

Define $\tilde{A}$ as an algebraic modular form (over R_0, an $\mathbb{F}_p$-algebra.)

The Frobenius endomorphism is $F: R \to R$, $x \mapsto x^p$

If $(E,\omega)_{/R}$ is a test object, we get a new test object $(E^{(p)},\omega^{(p)})$, which is $(E^{(p)},\omega^{(p)}) := (E,\omega)\otimes_F R$.

(ie if $(E,\omega) = \left(y^2 = x^3+ax+b, \frac{dx}{y}\right)$, then $(E^{(p)},\omega^{(p)}) = \left(y^2 = x^3+a^p x+b^p, \frac{dx}{y}\right)$.

Consider also the "geometric Frobenius map", which is an isogeny:

$$F: E_{/R} \longrightarrow E^{(p)}_{/R}$$ ← purely inseparable

which sends $(x,y) \longmapsto (x^p, y^p)$.

The degree of F is p, so $\ker F \subseteq E[p]_{/R}$

Def The dual isogeny to F is called the Verschiebung, and denoted V.

$\left(V: E^{(p)} \longrightarrow E, \text{ and } V\circ F = [p]_E,\ F\circ V = [p]_{E^{(p)}}.\right)$

Also, it is a fact that $\ker F$ is a connected group scheme.

$\left(\Leftrightarrow (\ker F)(\overline{\mathbb{F}_p}) = 0\right)$

Q: Is V separable?

Consider $V^*(\omega) = \tilde{A}(E,\omega)\cdot\omega^{(p)}$ $\quad(\tilde{A}(E,\omega)\in R)$.

This is how we define $\tilde{A}$:

To (E,ω), we compare $V^*\omega$ with $\omega^{(p)}$, and the ratio is called $\tilde{A}(E,\omega)$.

Theorem: $A(E,\omega) = \tilde{A}(E,\omega)$.

Pf: We will show that they have the same weight and the same q-expansion. (mod p!).

(1) weight $= p-1$

(2) $A\left(\mathrm{Tate}_q, \frac{dt}{t}\right) = 1 = \tilde{A}\left(\mathrm{Tate}_q, \frac{dt}{t}\right)$

(1) The weight of $\tilde{A}$:

$\tilde{A}\left((E,\lambda\omega)_{/R}\right)$?

$V^*(\lambda\omega) = \lambda\cdot V^*(\omega) = \lambda\cdot\tilde{A}(E,\omega)\cdot\omega^{(p)}$

Note now $(\lambda\omega)^{(p)} = \lambda^p\omega^{(p)}$. So $V^*(\lambda\omega) = \lambda^{1-p}\tilde{A}(E,\omega)\cdot(\lambda\omega)^{(p)}$

$\Rightarrow \tilde{A}(E,\lambda\omega) = \lambda^{1-p}\tilde{A}(E,\omega)$ $\to$ weight $p-1$. ✓

(2) $\left(\mathrm{Tate}_q, \omega_q\right) = \left(y^2 = x^3 + a(q)x + b(q), \frac{dx}{y}\right) = \left(\frac{\mathbb{G}_m}{q^{\mathbb{Z}}}, \frac{dt}{t}\right)$

$a(q), b(q) \in \mathbb{F}_p[\![q]\!]$

$$\left(\mathrm{Tate}_q^{(p)}, \omega_q^{(p)}\right) = \left(y^2 = x^3 + a(q^p)x + b(q^p), \frac{dx}{y}\right) = \left(\frac{\mathbb{G}_m}{q^{p\mathbb{Z}}}, \frac{dt}{t}\right)$$

The Frobenius morphism is induced by $\mathbb{G}_m \to \mathbb{G}_m$, $t \mapsto t^p$, $F: \mathbb{G}_m/q^{\mathbb{Z}} \to \mathbb{G}_m/q^{p\mathbb{Z}}$, $t \mapsto t^p$

(and $\ker F = \mu_p$).

From this, $V: \mathbb{G}_m/q^{p\mathbb{Z}} \longrightarrow \mathbb{G}_m/q^{\mathbb{Z}}$ sends $t \mapsto t$

Then $\ker V = \langle q \rangle$ (cyclic of order p).

From the expression for V, $V^* \frac{dt}{t} = \frac{dt}{t} = \left(\frac{dt}{t}\right)^{(p)} \Rightarrow \widetilde{A}(\mathrm{Tate}_q, \omega_q) = 1$

as we wanted.

Theorem: Let $E/\overline{\mathbb{F}}_p$ be an elliptic curve. Then the following are equivalent:

1) $A(E,\omega) = 0$ for one (and hence all) ω.

2) The morphism $V: E^{(p)} \to E$ is (purely) inseparable.

3) The morphism $[p]: E \to E$ is purely inseparable.

4) There is no p-torsion: $E(\overline{\mathbb{F}}_p)[p] = \{0\}$.

(In other words, if E is defined over $\mathbb{F}_q$, then $\#E(\mathbb{F}_{q^t}) = q^t + 1 - \alpha^t - \bar{\alpha}^t$, and we ask that $\alpha + \bar{\alpha} \equiv 0 \pmod p$).

5) $\mathrm{End}(E)$ is an order in a quaternion algebra.

In this case, we say that E is **supersingular**.

Pf

(1) $\Leftrightarrow$ (2) follows from the differential criterion for separability.

(2) $\Rightarrow$ (3) follows because F is inseparable.

(3) $\Rightarrow$ (4) and (4) $\Rightarrow$ (5) can be found on Silverman's 1st book.

Algebraic, mod p and p-adic modular forms.

• Algebraic modular forms:

Fix $\mathcal{Z}$ a base ring.

Eg:

a) $\mathcal{Z}$ = field $(\mathbb{Q}, \bar{\mathbb{Q}}, \mathbb{C}, \mathbb{F}_p, \bar{\mathbb{F}}_p, \mathbb{Q}_p, K((q)))$.

b) $\mathcal{Z}$ = local ring $(\mathbb{Z}_{(p)}, \mathbb{Z}_p)$

c) $\mathcal{Z}$ = PID $(\mathbb{Z})$.

Let E be an elliptic curve over R (smooth curve of genus 1, with a section).

For all hom. $\varphi: R \to K$, we have $E \otimes_R K$ an elliptic curve over K. (where K is a field).

• Modular forms over $\mathcal{Z}$.

a) Naive definition:

$$M_k(SL_2(\mathbb{Z}), \mathcal{Z}) := M_k(SL_2(\mathbb{Z}), \mathbb{Z}) \otimes \mathcal{Z}$$

(if $G \subset \mathcal{Z}^K$, this is $\cong$ to $\mathcal{Z}[Q, R]^{\deg = K}$)

b) Katz's definition

Def: A test object over $\mathcal{Z}$ is a triple $(E, \omega)_{/R}$ where:

- R is a $\mathcal{Z}$-algebra.
- E is an elliptic curve over R. locally free R-module of rank 1.
- $\omega \neq 0 \in H^0(E, \Omega^1_{E/R})$ (in particular, the image of ω in $H^0(E, \Omega^1_{E/K})$ $\Rightarrow$ nonzero for all $\varphi: R \to K$).

We identify $(E, \omega)_{/R} \sim (E', \omega')_{/R}$ iff $\exists\, \varphi: E \to E'$ such that $\varphi^*(\omega') = \omega$.

We have a <u>base change</u> for test objects: if $\varphi: R \to R'$ is a $\mathbb{Z}$-algebra homomorphism, then

$$(E,\omega)_{/R} \underset{\varphi}{\otimes} R' := \left(E \otimes R', \omega \otimes R'\right)_{/R'}.$$

<u>Def</u>: An <u>algebraic modular form</u> over $\mathbb{Z}$ is a rule which, to any test object $(E,\omega)_{/R}$ with R a $\mathbb{Z}$-algebra, it associates

$f\left((E,\omega)_{/R}\right) \in R$ such that:

1) Compatible with base change.

2) <u>wt k</u>: $f\left((E,\lambda\omega)_{/R}\right) = \lambda^{-k} f\left((E,\omega)_{/R}\right) \quad \forall \lambda \in R^\times$.

3) $f\left(\left(\mathrm{Tate}_q, \omega_{can}\right)_{/\mathbb{Z}((q))}\right) \in \mathbb{Z}[\![q]\!]$.

<u>Normal Form Theorem</u>: Assume that $6 \in \mathbb{Z}^\times$.

Thm/ If $(E,\omega)_{/R}$ is a test object, then $\exists!\ x, y \in H^0(E - \{0\}, \mathcal{O}_E)$ satisfying, for some elements $a, b \in R$:

a) $y^2 = 4x^3 + ax + b$

b) $\omega = \frac{dx}{y}$.

From this, we get that:

$$\left\{\begin{array}{l}\text{test objects} \\ \text{defined over } R\end{array}\right\} \longleftrightarrow \mathrm{Hom}_{\mathbb{Z}}\left(R^{univ}, R\right)$$

where $R^{univ} = M_{\mathbb{Z}} = \mathbb{Z}[a,R] = M_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{Z}$

• Modular forms over $\mathbb{F}_p$ $(p \geq 5)$.

Take in the previous discussion $\mathcal{Z} := \mathbb{F}_p$.

$$M_{\mathbb{F}_p} := M \otimes \mathbb{F}_p .$$

The space $M_{\mathbb{F}_p}$ contains a distinguished form of ~~degree~~ weight $p-1$, called the Hasse invariant $A(Q,R)$ such that:

$$A(Q,R) \equiv E_{p-1} \equiv 1 \text{ in } \mathbb{F}_p[\![q]\!]. \qquad \text{(Naive definition of } A\text{)}.$$

→ Modular definition of ~~A~~

We saw how to define it on $(E,\omega)_{/R}$.

Let $F: R \to R$ the Frobenius (R of char p).

Then $(E^{(p)}, \omega^{(p)})_R := (E,\omega)_{/R} \underset{F}{\otimes} R$.

Concretely, if $E \equiv y^2 = x^3 + ax + b$, $a, b \in R$, then $\left(\omega = dx/y\right)$

$$E^{(p)} \equiv y^2 = x^3 + a^p x + b^p \quad , \omega^{(p)} = dx/y$$

we get an isogeny also $F: E \to E^{(p)}$ which sends $(x,y) \mapsto (x^{(p)}, y^{(p)})$.

$\deg F = p$, and so if we define $V := F^\vee$, then $\deg V = p$, and

$$V \circ F = [p]_E, \qquad F \circ V = [p]_{E^{(p)}} .$$

The Frobenius F is always (purely) inseparable. But V is not, in general:

Theorem:
$$V^*\left(\omega^{(p)}\right) = A(E,\omega) \cdot \omega .$$

↓

Pf we saw last time that $wt(A) = p-1$. We want to see as well that its q-expansion is $\equiv 1 \pmod p$ (continues Pf later)

- Some things about the Tate curve.

a) For $\tau \in \mathcal{H}$, we have a "natural" test object:

$$\left(\mathbb{C}/\langle 1, \tau\rangle, dz\right)/\mathbb{C}$$

By the Normal Form Theorem, this equals:

$$\left(y^2 = 4x^3 - g_2(\tau)x - g_3(x),\ \frac{dx}{y}\right)$$

where $g_2(\tau) = \frac{(2\pi i)^4}{12}\left(1 + 240\, S_3(q)\right)$

$g_3(\tau) = \frac{(2\pi i)^6}{2^3 3^3}\left(-1 + 504\, S_5(q)\right)$ $\qquad q = e^{2\pi i \tau}$

(and $S_k(q) = \sum_{n \geq 1} \sigma_k(n) q^n = \sum_{n \geq 1} \frac{n^k q^n}{1-q^n} \in \mathbb{Z}[[q]]$).

Moreover, the functions x and y are given by $(u := e^{2\pi i z})$

$$x = \wp_\tau(z) = (2\pi i)^2\left(\sum_{n \in \mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} + \frac{1}{12} - 2\, S_1(q)\right)$$

$$y = \wp'_\tau(z) = (2\pi i)^3\left(\sum_{n \in \mathbb{Z}} \frac{q^n u(1+q^n u)}{(1-q^n u)^3}\right)$$

b) Tate curve over $\mathbb{C}$, but in terms of q:

Make a change of variables $z \longmapsto u = e^{2\pi i z}$

$$\varphi: \mathbb{C}/\langle 1, \tau\rangle \longrightarrow \mathbb{C}^\times/q^{\mathbb{Z}}$$

But $\varphi^*\left(\frac{du}{u}\right) = 2\pi i\, dz$

We change then the original test object, to get:

$$\left(\mathbb{C}/\langle 1,\tau\rangle,\ 2\pi i\,dz\right)/\mathbb{Z} \cong \left(\mathbb{C}^\times/q^{\mathbb{Z}},\ \frac{du}{u}\right).$$

$$\left(y^2 = 4x^3 - \tilde{g}_2(q)x - \tilde{g}_3(q),\ \frac{dx}{y}\right)/\mathbb{Z}((q)) \qquad \text{need } 6\in\mathbb{Z}^\times !$$

where $\tilde{g}_2(q) = \frac{1}{12}\left(1 + 240\, S_3(q)\right) \left(\in \mathbb{Z}[\![q]\!]\right) = \frac{1}{12}\,Q$

$\tilde{g}_3(q) = \frac{1}{6^3}\left(-1 + 504\, S_5(q)\right) \left(\in \mathbb{Z}[\![q]\!]\right) = \frac{-1}{6^3}\,R$

Moreover, the new functions are:

$$X(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u}{(1-q^n u)^2} + \frac{1}{12} - 2S_1(q) \in \mathbb{Z}\left[u, \tfrac{1}{u}\right][\![q]\!]$$

$$Y(u,q) = \sum_{n\in\mathbb{Z}} \frac{q^n u(1+q^n u)}{(1-q^n u)^3} \in \mathbb{Z}\left[u, \tfrac{1}{u}\right][\![q]\!].$$

c) The Tate curve over a complete local ring.

Let K be a local field (quotient field of a complete local ring).

Assume furthermore that $\mathcal{O}_K$ is a DVR.

Let $q \in K^\times$ be such that $|q| < 1$.

Also, suppose that K is a $\mathbb{Z}$-algebra (eg take $\mathbb{Z} = \mathbb{Z}[\frac{1}{6}]$).

We have an "evaluation map" $\mathbb{Z}((q)) \to K$.

Also, we have, for all $u_1, u_2 \in \mathbb{C}^\times$,

$$\left(X(u_1,u_2,q),\ Y(u_1,u_2,q)\right) = \left(X(u_1,q),\ Y(u_1,q)\right) +_E \left(X(u_2,q),\ Y(u_2,q)\right).$$

Def: The Tate curve is then defined to be:

$$\left(\mathrm{Tate}(q), \omega_{can}\right)_{/K} := \left(y^2 = 4x^3 - \widetilde{g}_2(q)x - \widetilde{g}_3(q), \frac{dx}{y}\right)_{/K}.$$

Note that $(\mathrm{Tate}(q))(K) \cong K^\times / q^{\mathbb{Z}}$ is an analytic isomorphism.

$$(X(u,q), Y(u,q)) \longleftrightarrow u$$

(not algebraic!)

u in $\mathbb{Z}[u, \frac{1}{u}][\![q]\!]$

→ Explicit descriptions of F and V on $\left(\mathrm{Tate}(q), \omega_{can}\right)_{/\mathbb{F}_p((q))}$:

Again, $\left(\mathrm{Tate}(q) \equiv y^2 = 4x^3 - \widetilde{g}_2(q)x - \widetilde{g}_3(q), \frac{dx}{y}\right)$.

$F: \mathbb{F}_p((q)) \longrightarrow \mathbb{F}_p((q))$ sends $\sum a_n q^n \mapsto \sum a_n^p q^{pn}$.

So:

$\mathrm{Tate}(q)^{(p)} \equiv y^2 = 4x^3 - \widetilde{g}_2(q^p)x - \widetilde{g}_3(q^p)$ and $\frac{dx}{y}$ stays the same.

So $F: (x,y) \longmapsto (x^p, y^p) = \left(X(u^p, q^p), Y(u^p, q^p)\right)$.

Claim $V: \mathrm{Tate}(q^p) \longrightarrow \mathrm{Tate}(q)$

$$\left(X(u,q^p), Y(u,q^p)\right) \mapsto \left(X(u,q), Y(u,q)\right)$$

Pf Exercise. (check that $V \circ F = [p]$).

Now we compute:

$$V^*\left(\frac{dX(u,q^p)}{Y(u,q^p)}\right) = \frac{d\left(X(u,q^p)\right)}{Y(u,q^p)} = \omega^{(p)}$$

Hence $V^*\omega = \omega^{(p)}$.

So the Hasse invariant A, evaluated at $\left(\mathrm{Tate}(q), \omega_{can}\right)_{/\mathbb{F}_p((q))}$ is 1.

(In particular, lies on $\mathbb{F}_p[\![q]\!]$, which we didn't know a priori!)

Geometric Interpretation of Modular forms mod p

Let $f \in \bar{M}_0 = M_{\mathbb{F}_p}/(A-1)$. $\left(M_{\mathbb{F}_p} = M_K \otimes \mathbb{F}_p\right)$

We want to define $f((E,\omega)_R)$, where R is an $\mathbb{F}_p$-algebra.

$\exists$ $f_k \in M_k \otimes \mathbb{F}_p$ such that $f_k \equiv f$ in $\mathbb{F}_p[[q]]$. (note that $p-1 \mid k$)

So we can define:

$$f((E,\omega)) := \frac{f_k(E,\omega)}{A(E,\omega)^{\frac{k}{p-1}}}$$

We need to check that this is well-defined:

If $f_{k'} \equiv f_k \pmod p$, then $k' = k + \nu(p-1)$ (wlog assume $\nu > 0$)

Then $f_{k'} = f_k \cdot A^{\frac{k'-k}{p-1}}$, so when we divide by the appropriate power, we get the same value.

The only problem we have then is that A is nonzero.

Hence we stay away from supersingular elliptic curves.

We have so far written $\frac{S_F(k,0)}{\Omega_\tau^k} = \frac{E_k}{\Omega_\tau^k} = E_k(A_\tau, \omega)$

where A_τ is an elliptic curve defined over H = Hilbert class field of F, and ω is a regular differential on A_τ/H.

We want to study the assignment:

$$k \longmapsto E_k((A_\tau,\omega)/H).$$

Let $\mathfrak{P}$ be a prime of H above the prime p, and let

$\mathcal{O}$ = ring of integers of $H_{\mathfrak{P}}$ ← completion of H at $\mathfrak{P}$.

Def: A_τ has <u>good reduction</u> at $\mathfrak{P}$ if there exists $\widetilde{A}_\tau / \mathcal{O}$

such that $\widetilde{A}_\tau \otimes_{\mathcal{O}} H \simeq A_\tau$.

Such an $\widetilde{A}_\tau$ is called an <u>integral model</u> (at $\mathfrak{P}$) of A_τ over $\mathcal{O}$.

Def: We say that A_τ has <u>good ordinary reduction</u> if $\widetilde{A}_\tau \otimes_{\mathcal{O}} (\mathcal{O}/\mathfrak{P})$ is ordinary

(i.e. not supersingular).

<u>Theorem</u>: The elliptic curve A_τ has good ordinary reduction at $\mathfrak{P}$ if and only if, p (← small p!) splits in F.

Pf We prove only the $\Leftarrow$ implication. Write $p = \pi\bar{\pi}$, where

$\pi, \bar{\pi}$ are ideals of $\mathcal{O}_F$.

If h = class number of $\mathcal{O}_F$ (or simply the order of π in $Cl(\mathcal{O}_F)$),

then $p^h = \alpha_p \cdot \bar{\alpha}_p$, where $\alpha_p, \bar{\alpha}_p \in \mathcal{O}_F \simeq End_H(A_\tau)$

Consider the endomorphisms on $\widetilde{A}_\tau$ (defined over $\mathcal{O}$) given by α_p and $\bar{\alpha}_p$.

(Let $\widetilde{A}_\tau$ be an integral model of A_τ over $\mathcal{O}$ (over F, all elliptic curves have good reduction! In general, they have bad reduction only on a finite set of primes).)

↓

(cont pf of thm).

We want to see whether $\alpha_p, \overline{\alpha_p}$ are separable. So let $\omega \in \Omega^1_{\widehat{A_\tau}/(\mathcal{O}/\mathfrak{P})}$

$$\alpha_p^*(\omega) = \alpha_p \cdot \omega \quad , \quad \overline{\alpha_p}^*(\omega) = \overline{\alpha_p}\,\omega$$

(choose the isomorphism $\mathcal{O}_F \cong \mathrm{End}(A_\tau)$ so that this happens).

There is exactly one of $\alpha_p, \overline{\alpha_p}$ whose image in $\mathcal{O}/\mathfrak{P}$ is nonzero.

(otherwise, we'd have $\mathfrak{P}$ and $\overline{\mathfrak{P}}$ divide α_p (and $\overline{\alpha_p}$) $\Rightarrow p \mid \alpha_p \Rightarrow !!$)

This implies that exactly one of the isogenies α_p, $\overline{\alpha_p}$ is separable.

Hence $p^h = \alpha_p \overline{\alpha_p}$ is <u>not</u> purely inseparable. $\Rightarrow$ p is not purely inseparable.

Hence $A_\tau/\mathcal{O}$ is <u>not</u> supersingular. Therefore, it's ordinary.

From now on, assume that $(A_\tau, \omega)/\mathcal{O}$ is a test object defined over $\mathcal{O}$, and Ω_τ is chosen such that $\Omega_\tau \cdot (2\pi i\, d\mathbf{z}) = \omega$.

<u>Theorem</u>: Let f_1, f_2 be classical modular forms in $M_{k_1} \otimes \mathbb{Z}_p$ and $M_{k_2} \otimes \mathbb{Z}_p$ (resp).

Assume that $f_1 \equiv f_2 \pmod{p^n}$, and that $p \nmid f_1$.

<u>Then</u>: a) $k_2 \equiv k_1 \mod\left((p-1)p^{n-1}\right)$

b) If $k_2 = k_1 + (p-1)\nu$, <u>then</u>:

~~$E_{p-1}(A_\tau)^\nu f_1(A_\tau,\omega) \equiv f_2(A_\tau,\omega) \pmod{\mathfrak{P}^n\mathcal{O}}$~~

$$\left(E_{p-1}(A_\tau,\omega)\right)^\nu f_1(A_\tau,\omega) \equiv f_2(A_\tau,\omega) \mod \mathfrak{P}^n\mathcal{O}.$$

Pf (of thm):

Assume WLOG that $\nu \neq 0$ (part (a) has been proved previously).

To prove part (b):

Then $E_{p-1}^{\nu} \equiv 1 \pmod{p^n}$.

Therefore, $E_{p-1}^{\nu} f_1 \equiv f_2 \pmod{p^n}$. (mod forms on $M_{k_2} \otimes \mathbb{Z}_p$).

Hence we can write $E_{p-1}^{\nu} f_1 = f_2 + p^n \cdot h$, $h \in M_{k_2} \otimes \mathbb{Z}_p$.

Evaluating at $(E_\tau, \omega)/_{\mathcal{O}}$, yields the result, as $h(E_\tau, \omega) \in \mathcal{O}$.

Remark: Let f be a p-adic modular form of weight $k_0 \in \mathbb{Z}$, with coefficients in $\mathbb{Z}_p$. Then f can be written as $f = \lim_{\nu} f_{k_0 + (p-1)\nu}$

where $f_{k_0+(p-1)\nu}$ is a classical modular form (in $M_{k_0+(p-1)\nu} \otimes \mathbb{Z}_p$).

The sequence: $\dfrac{f_{k_0+(p-1)\nu}\left((A_\tau, \omega)/_{\mathcal{O}}\right)}{E_{p-1}^{\nu}\left((A_\tau, \omega)/_{\mathcal{O}}\right)} \in \mathcal{O}$ converges in $\mathcal{O}$.

(in $\mathcal{O}^\times$)

So we can define $f\left((A_\tau, \omega)/_{\mathcal{O}}\right)$ ← of weight k_0 as well.

(we need that $\mathcal{O}$ is a p-adic ring, that is that

$\mathcal{O} \cong \varprojlim (\mathcal{O}/p^n\mathcal{O})$.)

Theorem: There exists a period $\Omega_{F,p} \in \tilde{\mathcal{O}}^\times$ ($\tilde{\mathcal{O}}$ a finite extension of $\mathcal{O}$) such that the function:

$$k \longmapsto \frac{\zeta_F(k,0)}{\pi^k \Omega_\tau^k} \cdot \Omega_{F,p}^k$$

extends to a continuous (in fact analytic) function of $k \in \frac{\mathbb{Z}}{(p-1)\mathbb{Z}} \times \mathbb{Z}_p$.

Pf

$$\frac{\zeta_F(k,0)}{\pi^k} = \tilde{G}_k(A_\tau, \omega) \cdot \Omega_\tau^k$$

Let then $\Omega_{F,p}$ be a $(p-1)^{st}$ root of $E_{p-1}(A_\tau,\omega)^{-1} \in \mathcal{O}^\times$.

So $\Omega_{F,p} = E_{p-1}(A,\omega)^{\frac{-1}{p-1}} \in \tilde{\mathcal{O}}^\times$

Then $\frac{\zeta_F(k,0)}{\pi^k \Omega_\tau^k} = \tilde{G}_k(A_\tau,\omega) \Rightarrow \frac{\zeta_F(k,0)}{\pi^k \Omega_\tau^k} \Omega_{F,p}^k = \frac{\tilde{G}_k(A_\tau,\omega)}{(E_{p-1}(A_\tau,\omega))^{\frac{k}{p-1}}}$

And apply the previous result.

We need still to interpolate $\zeta_F(k+r,-r)$. (which involves the δ_k^r's).

Recall that $\zeta_F(k+r,-r) \longleftrightarrow \delta_k^r E_k(A_\tau,\omega)$

Our next goal is to prove the following:

Theorem: Let f be a classical modular form in $M_k(\mathbb{Z})$. Let $(A,\omega)/\mathcal{O}$ be an ordinary test object such that $\mathrm{End}(A) \cong \mathcal{O}_F$.

Then: $(\delta_k^r f)(A,\omega) = (d^r f)(A,\omega)$

($\delta_k^r f$: function on lattices; $d^r f$: p-adic modular forms)

where d is the operator $M_k^\dagger \longrightarrow M_k^\dagger$ is the operator $q\frac{d}{dq}$.

The derivative of a modular forms.

First, an alternate description of modular forms:

Def: A modular form of weight k over $\mathbb{Z}$ (a ring) is a rule which associates to any E/R (R a $\mathbb{Z}$-algebra) an element $f(E/R) \in \left(\Omega^1_{E/R}\right)^{\otimes k}$

(given an algebraic modular form, then

$$f(E/R) := f((E,\omega)/R)\cdot \omega^{\otimes k}$$

which is independent of the choice of ω).

Let $X = \lambda$-line (the parameter space for elliptic curves). Then the space of relative differentials $\left(\Omega^1_{E^{univ}/X}\right)^{\otimes k}$ is a line bundle on X,

and a modular form is just a global section of this line bundle.

Problem: Suppose that $(E_\lambda, \omega_\lambda)$ is an algebraic family of elliptic curves and differential forms ω_λ on E_λ.

We'd like to define the "derivative wrt λ" of ω_λ, as an element of $\Omega^1_{E_\lambda}$

This is **not** possible:

Example: Sps $(E_\lambda, \omega_\lambda)$ is the family $\left(y^2 = x(x-1)(x-\lambda), \frac{dx}{y}\right)$

Then $\frac{dx}{y} = \frac{dx}{\sqrt{x(x-1)(x-\lambda)}}$. But $\frac{d}{d\lambda}\left(\frac{dx}{\sqrt{x(x-1)(x-\lambda)}}\right) = \frac{-dx}{x(x-1)(x-\lambda)^{3/2}} =$

$= \frac{-dx}{y(x-\lambda)}$ has a pole at $x=\lambda$.

• deRham cohomology (algebraic) (only for curves).

Let X be a nonsingular projective curve over a field k.

Def: A closed point on X is an element of $X(\bar{k})$. If $P \in X(\bar{k})$ has residue field $k(P) = k_P$.

~~We have a map $k(X) \to k_P((x_P))$.~~

A function $x \in k(X)$ is called a local parameter for X at P if it vanishes at P to order 1. Choosing a local parameter x_P, we get an evaluation map: (function field)

$$ev_P : k(X) \longrightarrow k_P((x_P))$$

Differential 1-forms on X.

Def: A differential form ω on X is called regular if $ev_P(\omega) \in k_P[\![x_P]\!]\,dx_P \subseteq \Omega^1_{k_P((x_P))/k_P}$

(note that ev_P extends to $ev_P : \Omega^1 k(X)/k \longrightarrow \Omega^1 k_P((x_P))/k_P = k_P((x_P))\,dx_P$)

Def: The residue of ω at the point P is the element of k_P appearing as the coefficient of x_P^{-1} in $ev_P(\omega) = \sum_{-M}^{\infty} a_n(P) x_P^n\,dx_P$.

Fact: doesn't depend on the choice of local parameter.

Def: A differential form $\omega \in \Omega^1 k(X)/k$ is said to be

- of the first kind if it is regular at P, $\forall P \in X(\bar{k})$
- of the second kind if $res_P(\omega) = 0 \quad \forall P \in X(\bar{k})$.

We have:

$$\left\{\begin{array}{l}\text{diff. forms}\\ \text{of the 1st kind}\end{array}\right\} \subsetneq \left\{\begin{array}{l}\text{diff forms}\\ \text{of the 2nd kind}\end{array}\right\}$$

(small ← left; huge space → right)

Remark: If $\operatorname{res}_p(\omega)=0$, then $ev_p(\omega) =: \omega_p \in \Omega_{K_p((x_p))/k_p}$ is exact (can integrate termwise). Conversely, exact $\Rightarrow$ res $=0$. (in the local ring).
This doesn't mean that one can ~~locally~~ integrate globally!

Remark: If $k=\mathbb{C}$ and $\gamma \in H_1(X(\mathbb{C}), \mathbb{Z})$, then:

$\int_\gamma \eta$ makes sense for any η of the second kind.

Def: The first deRham cohomology of X/k is the quotient:

$$H^1_{dR}(X/k) := \left\{\begin{array}{l}\text{differential 1-forms}\\ \text{of the second kind on } X/k\end{array}\right\} \Big/ \left\{\begin{array}{l}\text{exact forms}\\ df,\ f\in K(X)\end{array}\right\}$$

Key properties: (1) There is a natural map: $\Omega^1_{X/k} \longrightarrow H^1_{dR}(X/k)$
($\Omega^1_{X/k}$ ← regular (i.e. first kind).)

given by $\omega \longmapsto [\omega]$.

which is injective:

$[\omega]=0 \Rightarrow \omega = df$. As ω is regular, f is regular everywhere, so $f=ct$.

$\Rightarrow \omega = 0$. ✓

② If $\omega \in H^1_{dR}(X/k)$, then there exists a covering $X = \bigcup X_i$ by open subsets (in the Zariski Topology) s.t.

$$\omega|_{X_i} = \omega_i + df_i$$

where $\omega_i \in \Omega^1_{X_i}$ and $f_i \in k(X_i)$

Define then $f_{ij} := f_i - f_i \in \mathcal{O}_{X_i \cap X_j}(X_i \cap X_j)$

Then $\{f_{ij}\}_{i,j}$ is a 1-cocycle (i.e. in $H^1(X, \mathcal{O}_X)$).

(i.e $f_{ij} + f_{jk} + f_{ki} = 0$)

To $\omega \in H^1_{dR}(X/k)$ we can thus associate a the data:

$$(\omega_i, f_{ij}) \text{ s.t } df_{ij} = \omega_j - \omega_i.$$

Def: A collection of $\omega_i \in \Omega^1_{X_i}$ and $f_{ij} \in \mathcal{O}_{X_i \cap X_j}(X_i \cap X_j)$ satisfying

1) $df_{ij} = \omega_j - \omega_i$

2) $f_{ij} + f_{jk} + f_{ki} = 0$

is called a <u>deRham hypercocycle</u>.

Claim:
The map $\omega \mapsto \{f_{ij}\}_{i,j}$ from $H^1_{dR}(X/k) \to H^1(X, \mathcal{O}_X)$ is surjective, and has kernel $= \Omega^1_{X/k}$.

Pf/ omitted //

(but it's clear that $\Omega^1_{X/k} \subseteq$ kernel).

We get in this way an exact sequence:

$$0 \to \Omega^1_{X/k} \longrightarrow H^1_{dR}(X/k) \longrightarrow H^1(X, \mathcal{O}_X) \to 0$$

(3) Duality: Given $[\omega], [\eta] \in H^1_{dR}(X/k)$ (viewed as differentials of the second kind), we can write:

$$\omega_p = d F_p \,, \quad F_p \in K_p((x_p)) \qquad (F_p \text{ is sometimes called a local primitive for } \omega \text{ at } p).$$

Assume that ω, η have no common singularities (one can modify one of them by an exact form so that this is true).

$$\langle [\omega], [\eta] \rangle := \sum_{p \in X(\bar{k})} \operatorname{res}_p(F_p \cdot \eta_p)$$

Claim: This pairing is well-defined.

1) Doesn't depend on the choice of the F_p:

$\left(\operatorname{res}_p((F_p + c)\eta_p) = \operatorname{res}(F_p \eta_p) + \operatorname{res}_p(\underbrace{c \cdot \eta_p}_{0 \text{ as } c \eta_p \text{ is of the 2nd kind}}) \right)$.

2) Doesn't depend on the class representatives:

- of ω:

if $\omega' = \omega + dg$, then can take $F_p' = F_p + g$.

Then $\sum_p \operatorname{res}_p(F_p' \eta) = \sum_p \operatorname{res}_p(F_p \eta) + \underbrace{\sum_p \operatorname{res}_p(g \cdot \eta)}_{= 0 \text{ by the residue theorem.}}$ (global meromorphic function!)

- of η: write $\eta' = \eta + dg$.

Then $\sum_p \operatorname{res}_p(F_p \eta') = \sum_p \operatorname{res}_p(F_p \eta) + \sum_p \operatorname{res}_p(F_p\, dg)$

Note that $\operatorname{res}(F_p\, dg) = -\operatorname{res}((dF_p) \cdot g) = -\operatorname{res}(\omega \cdot g)$ so again can apply the residue theorem.

Properties of $\langle \cdot, \cdot \rangle$: (assume K is perfect) — but don't need it.

1) Bilinear and alternating ($\langle \omega, \eta \rangle = -\langle \eta, \omega \rangle$).

2) It takes values in K. (although $\mathrm{res}_p(F_p, h_p) \in k_p$, but it's stable under G_K)

3) (Non-formal property) $\Omega^1_{X/K}$ is a maximal isotropic subspace for $\langle \cdot, \cdot \rangle$.

(so that it induces a ~~pairing~~ perfect K-linear pairing:

$$\Omega^1_{X/K} \times H^1(X, \mathcal{O}_X) \longrightarrow K$$

(Serre duality).

4) **Periods**: Suppose now $K = \mathbb{C}$. Then $X(K)$ is a Riemann surface, say of genus g. ($2g = \mathrm{rk}_{\mathbb{Z}}(H_1(X(\mathbb{C}), \mathbb{Z}))$).

This gives an integration map (called the period map)

$$\mathrm{per}: H^1_{dR}(X/\mathbb{C}) \longrightarrow H_1(X(\mathbb{C}), \mathbb{C})^\vee$$

which is an isomorphism. (note that $\dim_{\mathbb{C}} = 2g$ for each of them).

We have also $H^1_{dR,an}(X(\mathbb{C}), \mathbb{C}) = \{$closed smooth $\mathbb{C}$-valued differential forms on $X(\mathbb{C})\}$ / $\{$exact forms$\}$.

Thm (deRham): $H^1_{dR,an}(X(\mathbb{C}), \mathbb{C}) \simeq H_1(X(\mathbb{C}), \mathbb{C})^\vee$.

In this way, we get a map:

$$H^1_{dR}(X/\mathbb{C}) \xrightarrow{\simeq} H^1_{dR,an}(X(\mathbb{C}), \mathbb{C})$$

$$[\omega] \longmapsto [\omega^{an}]$$

where ω^{an} is smooth on $X(\mathbb{C})$ and closed, and $\int_\gamma \omega = \int_\gamma \omega^{an}$ $\forall \gamma \in H_1(X(\mathbb{C}), \mathbb{C})$.

Theorem: Given $\omega_1, \omega_2 \in H^1_{dR}(X/\mathbb{C})$, then

$$\langle \omega_1, \omega_2 \rangle = \frac{1}{2\pi i} \int_{X(\mathbb{C})} \omega_1^{an} \wedge \omega_2^{an}$$

the pairing on analytic de Rham cohomology (topological). (cf Poincaré duality)

Key example: $X = E$ is an elliptic curve over K, equipped with $\omega \in \Omega^1_{E/K}$. Assume also $6 \in K^\times$.

So $(E, \omega) \rightsquigarrow \left(y^2 = 4x^3 - g_2 x - g_3, \frac{dx}{y}\right)$, where $g_2, g_3 \in K$.

Define then $\eta := x \frac{dx}{y}$ (note that η has a double pole at ∞)

Prop: The form η is a differential form of the second kind on E/K, and the classes $[\omega], [\eta]$ give a basis for $H^1_{dR}(E/K)$

Pf/ We will prove the first part using analytic techniques ($K = \mathbb{C}$), although by choosing a parameter at ∞ one can do it algebraically.

Note that under the identification $(E, \omega) \rightsquigarrow (\mathbb{C}/\langle 1, \tau \rangle, dz)$, then $x \leftrightarrow \wp(z)$, $y \leftrightarrow \wp'(z)$.

So $\frac{dx}{y} \leftrightarrow dz$, and $x \frac{dx}{y} \leftrightarrow \wp(z)\, dz$.

At $z = 0$, $\wp(z) = \frac{1}{z^2} + g(z)$, $g \in \mathbb{C}[[z]]$. So it has no term in $\frac{1}{z}$, as we wanted.

As $\dim_K H^1_{dR}(E/K) = 2g = 2$, we just need to prove linear independence. Note that if $[\eta] = \lambda \cdot [\omega]$, then $\langle \omega, \eta \rangle = 0$. So need to show $\langle \omega, \eta \rangle \neq 0$.

$$\langle \omega, \eta \rangle = \operatorname{res}_0 \left(z \cdot \left(\frac{1}{z^2} + g(z) \right) dz \right) = \operatorname{res}_0 \left(\left(\frac{1}{z} + z g(z) \right) dz \right) = 1 \neq 0.$$

Remark: All the previous definitions (in the key example of an elliptic curve) work for E defined over any ring R with $6 \in R^\times$.

So if $(E,\omega)_{/R}$ is a test object, then

$$H^1_{dR}(E_{/R}) = R\cdot\left[\frac{dx}{y}\right] + R\left[x\frac{dx}{y}\right].$$

This gives a canonical splitting of the Hodge filtration:

$$0 \to \Omega^1_{E/R} \to H^1_{dR}(E/R) \to H^1(E,\mathcal{O}_E) \to 0$$
$$\omega \qquad\qquad \eta \dashrightarrow \overline{\eta}$$

The Gauss-Manin connection

Let E be an elliptic curve defined over $K(\lambda)$ ($K(\lambda)$: field of rational functions on λ (an indeterminate)).

Let $\omega \in \Omega^1_{E/K(\lambda)}$. We get then $\left(y^2 = 4x^3 - g_2(\lambda)x - g_3(\lambda),\ \frac{dx}{y}\right)$,

where $g_2, g_3 \in K(\lambda)$, and $\Delta_E \in K(\lambda)^\times$.

Let $P_1,\dots,P_s$ be the set of poles of $g_2(\lambda), g_3(\lambda)\} \cup \{$set of zeros & poles of $\Delta(\lambda)\}$ (a subset of $\overline{K}$).

Let R be the ring of functions which are regular outside $\{P_1,\dots,P_s\}$.

So E gives an ell. curve defined over R. (base extension)

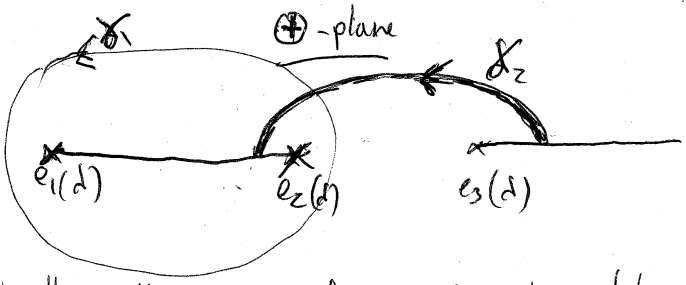
We view $E_{/R}$ as giving an algebraic family $(E_\lambda, \omega_\lambda)$, varying with the parameter λ.

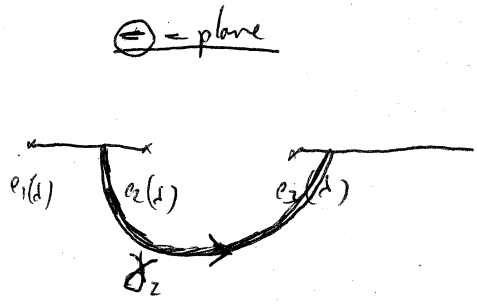
The goal: to "differentiate" ω_λ w.r.t. λ.

To define $\frac{d}{d\lambda}\omega_\lambda$, we should be able to "compare" $\omega_{\lambda+\varepsilon}$ with ω_λ, but they belong to different spaces!.. We need to "identify" $\Omega^1_{E_\lambda} \simeq \Omega^1_{E_{\lambda+\varepsilon}}$.

We get the idea from the analytic/topology setting: So assume $K = \mathbb{C}$.

$$E_\lambda : \; y^2 = 4x^3 - g_2(\lambda)x - g_3(\lambda) = 4\big(x - e_1(\lambda)\big)\big(x - e_2(\lambda)\big)\big(x - e_3(\lambda)\big).$$





and glue together the two planes, along the slits.

The paths γ_1, γ_2 are generators for the homology $\big(H_1(E_\lambda(\mathbb{C}), \mathbb{Z})\big)$

Note that these two paths still make sense if $e_i(\lambda)$ move very little, so in some neighborhood of λ.

So choose a basis γ_1, γ_2 for $H_1\big(E_\lambda(\mathbb{C}), \mathbb{Z}\big)$, and this determines a basis (noted again γ_1, γ_2) for $H_1\big(E_{\lambda+\varepsilon}(\mathbb{C}), \mathbb{Z}\big)$, for ε sufficiently small.

As the deRham cohomology is the dual of the homology, we get a canonical identification (aka the period map).

$$H^1_{dR}\big(E_{\lambda/\mathbb{C}}\big) \simeq H^1_{dR}\big(E_{\lambda+\varepsilon/\mathbb{C}}\big).$$

Theorem ($k = \mathbb{C}$): Let $\omega_\lambda \in H^1_{dR}(E/R)$. Then, there exists a unique form $\omega'_\lambda \in H^1_{dR}(E/R)$ such that:

$$(*) \qquad \int_{\gamma_1} \omega'_\lambda = \frac{d}{d\lambda} \int_{\gamma_1} \omega_\lambda \quad \text{and} \quad \int_{\gamma_2} \omega'_\lambda = \frac{d}{d\lambda} \int_{\gamma_2} \omega_\lambda$$

Proof:

For each $\lambda \in \mathbb{C} - \{P_1, \dots, P_8\}$, the equations $(*)$ determine ω'_λ as an element in $H^1_{dR}(E_\lambda/\mathbb{C})$. The problem is to show that $\{\omega'_\lambda\}_{\lambda \in \mathbb{C} - \{P_1, \dots, P_8\}}$ comes from a differential of the second kind in $H^1_{dR}(E/R)$.

Write $\omega_\lambda = A(\lambda)\frac{dx}{y} + B(\lambda)x\frac{dx}{y}$ $\quad (A(\lambda), B(\lambda) \in R)$.

$$= \frac{A(\lambda) + xB(\lambda)}{\sqrt{4x^3 - g_2(\lambda)x - g_3(\lambda)}}\, dx.$$

Now, $\frac{d}{d\lambda}\int_{\gamma_1} \omega_\lambda = \int_{\gamma_1} \frac{d}{d\lambda}\omega_\lambda = \int_{\gamma_1} \frac{(A'(\lambda) + B'(\lambda)\cdot x)\sqrt{4x^3 - g_2(\lambda)x - g_3(\lambda)} + \frac{1}{2}(\sqrt{\ })^{-1}}{4x^3 - g_2(\lambda)x - g_3(\lambda)}\, dx$

(γ_1 doesn't depend on λ!)

$$= \int_{\gamma_1} \frac{(A'(\lambda) + B'(\lambda)x)\cdot y + \frac{1}{2}y^{-1}\cdot(g_2'(\lambda)x + g_3'(\lambda))(A(\lambda) + xB(\lambda))}{y^2}\, dx$$

$$= \int_{\gamma_1} \omega'_\lambda \qquad \text{where } \omega'_\lambda \text{ is an algebraic differential form on } E/R.$$

To see that it's of the second kind, we need to compute:

$$\frac{1}{2\pi i}\oint_{\textcircled{6}} \omega'_\lambda = \frac{1}{2\pi i}\frac{d}{d\lambda}\Big(\oint_{\textcircled{5}} \omega_\lambda\Big) = 0 \text{ identically} = 0.$$

This will allow us to define the Gauss-Manin connection.

Remark: we can replace now $\mathbb{C}[\lambda]\left[\frac{1}{(\lambda-\beta_1)\cdots(\lambda-\beta_s)}\right]$ with

$$k[\lambda]\left[\frac{1}{(\lambda-\beta_1)\cdots(\lambda-\beta_s)}\right]$$

Def: The form ω_λ' is called the derivative of ω_λ with respect to λ, for the Gauss-Manin connection.

We write $\omega_\lambda' =: \nabla_\lambda \omega_\lambda$

We want to eliminate the dependence on λ. We define thus ∇ as an R-linear map:

$$\nabla : H^1_{dR}(E/R) \longrightarrow H^1_{dR}(E/R) \otimes \Omega^1_{R/k} \qquad \left(\text{Gauss-Manin connection}\right)$$

such that: $\nabla(\omega)\left(\frac{d}{d\lambda}\right) = \nabla_\lambda \omega$

Properties: (recall $d: R \to \Omega^1_{R/k}$).

-Leibniz rule: $\nabla(\lambda \cdot \omega) = d\lambda \otimes \omega + \lambda \cdot \nabla(\omega)$

(HW).

Relation to Modular Forms

If f is a modular form of weight k, it gives rise to an element of $\Omega^{1\otimes k}_{E/k}$ (the k^{th} symmetric power of $\Omega^1_{E/k}$), by considering:

$$f(E,\omega)\,\omega^k \in \mathrm{Sym}^k_R \Omega^1(E/k) \hookrightarrow \mathrm{Sym}^k H^1_{dR}(E/k)$$

We will get $\nabla : H^1_{dR}(E/R)^{\otimes k} \to H^1_{dR}(E/R)^{\otimes k} \otimes \Omega^1_{R/k} \xrightarrow{\text{we'll find a map here.}} \Omega^1(E/k)^{\otimes k} \otimes \Omega^{1\otimes 2}_{E/k}$

At the end, we will get a map $\Omega^{1\otimes k}_{E/R} \to \Omega^{1\otimes k}_{E/k} \otimes \Omega^{1\otimes 2}_{E/k}$

• Algebraic description of the Gauss-Manin connection

Let R be a k-algebra, (e.g. $R = k[\lambda]$). Let E/R be an elliptic curve. Let $d\lambda$ be an R-module generator for $\Omega^1_{R/k}$ (assume here $\dim \Omega^1 = 1$).

Then a form $\omega \in H^1_{dR}(E/R)$ can be viewed as an algebraic family $\{\omega_\lambda\}_{\lambda \in \operatorname{Spec} R}$ of differentials of the second kind on $\{E_\lambda\}$

Define then:

$$\nabla(\omega) := \left(\frac{d}{d\lambda}\omega_\lambda\right) \otimes d\lambda$$

• Analytic description: if $k = \mathbb{C}$ (or $k \subseteq \mathbb{C}$), let $\{\gamma_1, \gamma_2\}$ = basis for $H_1(E_\lambda(\mathbb{C}), \mathbb{Z})$

Then γ_1, γ_2 are also a basis for $H_1(E_{\lambda'}(\mathbb{C}), \mathbb{Z})$ for λ' close to λ.

To ω_λ, one can associate $(\omega_1(\lambda), \omega_2(\lambda))$, where $\omega_i(\lambda) = \int_{\gamma_i} \omega_\lambda$.

Then $\frac{d}{d\lambda}\omega_\lambda$ ($= \omega'_\lambda$) is, by definition, the diff. of second kind on E_λ satisfying:

$$\int_{\gamma_i} \omega'_\lambda = \frac{d}{d\lambda}\omega_i(\lambda)$$

• Some sheaves and isomorphisms

a) $\omega_{E/R}$:= sheaf of regular differentials on E/R

$$\omega_{E/R}(U) := \Omega^1_{E/\mathcal{O}_U}$$

← locally free of rk 1. (U = affine open)

b) $\mathcal{H}^1_{dR}(E/R)$ = relative deRham cohomology sheaf.

$$\mathcal{H}^1_{dR}(U) := H^1_{dR}(E/\mathcal{O}_U)$$

c) $\Omega^1_{R/k}$:= sheaf of differentials on R/k

$$\Omega^1_{R/k}(U) = \Omega^1_{\mathcal{O}_U/k}$$

We also define their k^{th} Symmetric powers:

d) $\omega^{k}_{E/R} := Sym^{k}(\omega_{E/R})$

$\omega^{-k}_{E/R} := Sym^{k}(\omega^{-1}_{E/R})$, where $\omega^{-1}_{E/R} = Hom(\omega_{E/R}, \mathcal{O}_R)$

e) $\mathcal{H}'_{dR}(E/R)^{k}$ will be of rank $k+1$.

Theorem: Suppose that $(E,\omega)_{/R}$ is a test object, and that $6 \in R^{\times}$.

Then:

① $\mathcal{H}^{1}_{dR}(E/R) = \omega_{E/R} \oplus \omega^{-1}_{E/R}$

② $\mathcal{H}'_{dR}(E/R)^{k} = \omega^{k}_{E/R} \oplus \omega^{k-2}_{E/R} \oplus \cdots \oplus \omega^{-k}_{E/R}$

Pf/ For all affine $U \subseteq Spec\ R$, we have:

①
$$\mathcal{H}'_{dR}(E/R)(U) = H'_{dR}(E/\mathcal{O}_U) = \mathcal{O}_U \frac{dx}{y} \oplus \mathcal{O}_U\, x\frac{dx}{y} = \omega'_{E/R}(U) \oplus \omega^{-1}_{E/R}(U)$$

Remark: this decomposition is not functorial.

$\left(\varphi^{*}\left(\frac{dx}{y}\right) = \alpha \cdot \frac{dx}{y}, \text{ but } \varphi^{*}\left(x\frac{dx}{y}\right) \neq \beta \cdot x\frac{dx}{y}\right)$ $\left(\varphi: E_1 \to E_2 \text{ an isogeny}\right)$

For ②, this is just formal.

Theorem: There is a canonical map of sheaves of rank 1.

$$KS : \omega^{\otimes 2}_{E/R} \longrightarrow \Omega^1_{R/k} \qquad (KS = \text{Kodaira-Spencer map}).$$

If $R = k[j]_{\left[\frac{1}{j(j-1728)}\right]}$ and E/R is the "universal" elliptic curve, then KS is an isomorphism.

Pf (only of the first part).

To define KS, we need to define what it is:

$$KS(\omega_1 \otimes \omega_2) := \langle \nabla(\omega_1), \omega_2 \rangle$$

Note that $\nabla(\omega_1) \in H^1_{dR}(E/R) \otimes \Omega^1_{R/k}$, and $\omega_2 \in H^1_{dR}(E/R)$.

Then $\langle \nabla(\omega_1), \omega_2 \rangle \in R \otimes_R \Omega^1_{R/k} = \Omega^1_{R/k}$.

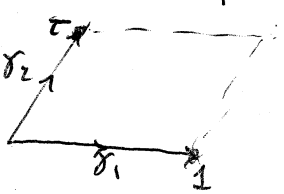
Example: Consider $(E, \omega) = \left(\mathbb{C}/\langle 1, \tau \rangle , dz \right)$.

Instead of working with the algebraic decomposition $\left(dz, P_z(z)dz\right)$, we work with the Hodge decomposition:

Define $\eta = d\bar{z}$ $\left(\omega = dz\right)$. $\left(\begin{cases} dz = dx + i dy \\ d\bar{z} = dx - i dy \end{cases} \right)$

Prop: $\{ [dz], [d\bar{z}] \}$ generate $H^1_{dR}(E/\mathbb{C})$.

Pf Consider their periods:



$\int_{\gamma_1} dz = 1$, $\int_{\gamma_2} dz = \tau$. So the "period vector" of dz is $(1, \tau)$

The period vector of $d\bar{z}$ is then $(1, \bar{\tau})$. These two vectors are l.i because $\operatorname{Im}(\tau) \neq 0$.

(continues example)

The Hodge decomposition in this case is:

$$H^1_{dR}(E/\mathbb{C}) = H^{1,0}(E/\mathbb{C}) \oplus H^{0,1}(E/\mathbb{C})$$

$$\nabla(dz) = \nabla_\tau(dz) \otimes d\tau$$

To compute $\nabla_\tau(dz)$, we use the period description:

the periods of $\nabla_\tau(dz)$ are $\frac{d}{d\tau}(1,\tau) = (0,1)$,

So $\nabla_\tau(dz) = \frac{dz - d\bar{z}}{\tau - \bar{\tau}}$

Hence $\nabla(dz) = \frac{dz - d\bar{z}}{\tau - \bar{\tau}} \otimes d\tau$ ← This doesn't depend on the choice of τ! (inv under $SL_2(\mathbb{R})$)

Also, in the same way we find $\nabla(d\bar{z}) = 0$

Note that in our setting, $\omega^2_{E/\mathbb{C}} = (\mathbb{C}\cdot dz)^2$.

$$\boxed{KS(dz^2)} = \langle \nabla(dz), dz \rangle = \left\langle \frac{dz - d\bar{z}}{\tau - \bar{\tau}}, dz \right\rangle \cdot d\tau =$$

$$= \frac{1}{2\pi i} \int_{E(\mathbb{C})} \frac{dz \wedge d\bar{z}}{\tau - \bar{\tau}} \cdot d\tau = \boxed{-\frac{d\tau}{2\pi i}}$$

Let now $s: H^1_{dR}(E/R) \to \Omega^1_{E/R}$ be an algebraic splitting of the Hodge filtration. Or, more generally, let $s: H^1_{dR}(E_\lambda/\mathbb{C}) \to \Omega^1_{E_\lambda/\mathbb{C}}$ be a splitting (need not be algebraic or holomorphic), which is smooth relative to u, v if $\lambda = u + iv$.

We want to define an operation:

$$D_s : \left\{ \begin{array}{c} \text{Mod. forms of} \\ \text{weight } k \\ \text{(algebraic)} \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{Mod. forms of} \\ \text{weight } k+2 \\ \text{(maybe not} \\ \text{algebraic!)} \end{array} \right\}$$

Recall that we had an identification:

$$M_k(SL_2(\mathbb{Z})) \longrightarrow (\Omega^1_{E/R})^k$$
$$f \longmapsto f(E,\omega)\cdot\omega^k$$

Next, note that $\Omega^1_{E/R}{}^k \hookrightarrow H^1_{dR}(E/R)^k$.

Lastly, ~~project, using the splitting s,~~ to $\Omega^1(E/R)^k$.

Next, apply $\nabla : H^1_{dR}(E/R)^k \longrightarrow H^1_{dR}(E/R)^k \otimes \Omega^1_{R/k}$.

Apply then the splitting s to $H^1_{dR}(E/R)$, to land in:

$$\Omega^1(E_{\mathbb{C}}^{(a)}/\mathbb{C})^k \otimes_{\mathbb{C}} \Omega^1_{R/k}$$

Lastly, apply the Kodaira-Spencer map (the inverse of what we have seen) to identify $\Omega^1_{R/k} \simeq \left(\Omega^1(E_{\mathbb{C}}^{(a)})\right)^2$

So the composition of all these maps gives:

$$D_s : M_k(SL_2(\mathbb{Z})) \longrightarrow M^{\text{maybe not algebraic anymore, depends on } s!}_{k+2}(SL_2(\mathbb{Z}))$$

Example: the case where S = Hodge splitting.

We have $S(a\,dz + b\,d\bar{z}) := a\,dz \qquad (a,b \in \mathbb{C})$.

Start with $f \in M_k(SL_2(\mathbb{Z}))$.

It gives us $f(\tau)\,dz^k \in (\Omega^1_{\mathcal{E}/R})^k$.

Apply ∇: $\nabla(f(\tau)(dz)^k) = df(\tau)\,dz^k + f(\tau)\,\nabla(dz^k) =$

$$= f'(\tau)\,dz^k\,d\tau + f(\tau)\,k\cdot\nabla(dz)\cdot(dz)^{k-1}$$

$$= f'(\tau)dz^k\,d\tau + k f(\tau)\frac{dz - d\bar{z}}{z-\bar{z}}(dz)^{k-1}d\tau$$

So $\nabla\left(f(\tau)(dz)^k\right) = \left(f'(\tau) + \frac{k f(\tau)}{\tau-\bar{\tau}}\right) dz^k d\tau \; - \; \frac{k\,f(\tau)}{\tau-\bar{\tau}}\,d\bar{z}(dz)^{k-1}d\tau$

Note that this last expression is invariant under $\tau \mapsto \frac{a\tau+b}{c\tau+d}$!

Applying now S, gives us:

$$\left(f'(\tau) + k\frac{f(\tau)}{\tau-\bar{\tau}}\right) dz^k d\tau$$

The κs-map is $dz^2 = -\frac{d\tau}{2\pi i}$, so we get:

$$-2\pi i\left(f'(\tau) + k\frac{f(\tau)}{\tau-\bar{\tau}}\right) dz^{k+2} \;=\; \left(\delta_k f\right)(\tau)\,dz^{k+2}$$

We now do a similar computation, but algebraically

Let f be a modular form of weight k.

$$f(q) = f(\mathrm{Tate}_q) = f\left(\mathbb{C}^\times/q^{\mathbb{Z}}, \frac{dt}{t}\right).$$

If $q = e^{2\pi i \tau}$, $t = e^{2\pi i z}$, then this is the same as

$$f\left(\mathbb{C}/\langle 1, \tau\rangle, 2\pi i\, dz\right) = f(\tau).$$

Now,

$$f(E,\omega)\omega^k = f\left(\mathbb{C}/\langle 1,\tau\rangle, 2\pi i dz\right)(2\pi i dz)^k = f(\tau)(2\pi i dz)^k.$$

We have previously computed:

$$\nabla\left(f(\tau)(2\pi i dz)^k\right) = \left[f'(\tau) + \frac{k f(\tau)}{\tau-\bar\tau}\right](2\pi i dz)^k d\tau + \xi\cdot(2\pi i dz)^{k-1} 2\pi i d\bar z d\tau$$

The Hodge splitting induces also:

$$s_{\mathrm{Hodge}} : \Omega^1_{\mathrm{dR}}(E/\mathbb{C})^k \to (\Omega^1_{E/\mathbb{C}})^k$$
$$a dz^k + b dz^{k-1} d\bar z \longmapsto a\, dz^k$$

So applying s_{Hodge} to $\left(\nabla(f(\tau)(2\pi i dz)^k)\right)$ yields:

$$s\left(\nabla(f(\tau)(2\pi i dz)^k)\right) = \left[f'(\tau) + \frac{k f(\tau)}{\tau-\bar\tau}\right](2\pi i dz)^k.$$

Last time we saw that $\kappa_s\left((2\pi i dz)^2\right) = 2\pi i d\tau$

So $\kappa_s^{-1}\left(s_{\mathrm{Hodge}}(\nabla(-))\right) = \frac{1}{2\pi i}\left(f'(\tau) + \frac{k f(\tau)}{\tau-\bar\tau}\right)(2\pi i dz)^{k+2} = \delta_k f(\tau)(2\pi i dz)^{k+2}$

↓

The function $\delta_k f$ can be thought of as a function on lattices (even if it's not holomorphic), as $\delta_k f(\tau) = (\delta_k f)\left(\mathbb{C}/\langle 1,\tau\rangle, 2\pi i dz\right)$.

So our computation yields:

$$\left(ks^{-1} \circ s_{Hodge} \circ \nabla\right)\left(f(E,\omega)\,\omega^k\right) = \left(\delta_k f\right)(E,\omega)\cdot \omega^{k+2}$$

Now we use an algebraic splitting.

Let E be an elliptic curve over $R = \mathbb{C}[j]\left[\frac{1}{j(j-1728)}\right]$.

(the universal elliptic curve, i.e. whose j-invariant is exactly j).

Then E can be viewed as a curve $A(\mathcal{H})$ (ring of hol functions on $\mathcal{H}$).

In this identification, let E_τ the curve corresponding to $\tau \in \mathcal{H}$.

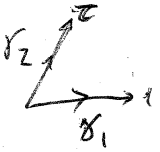
Consider the basis:

$$\left\{ \omega = 2\pi i \frac{dx}{y}\,,\ \eta = \frac{1}{2\pi i} x \frac{dx}{y} \right\} \quad \text{of } H^1_{dR}(E)$$

where we take $E = \left(\mathbb{C}/\langle 1,\tau\rangle, 2\pi i dz\right)$. In this case, the equation of E is $y^2 = 4x^3 + g_2 x + g_3$, where g_2, g_3 have rational coefficients.

We want to compute now $\nabla\omega$.

We'll work analytically, so we first compute the periods of ω, η.



$$\text{per}: H^1_{dR}(E_\tau(\mathbb{C})) \longrightarrow \mathbb{C}^2$$
$$\alpha \longmapsto (\alpha_1, \alpha_2)$$

where $\alpha_j = \int_{\gamma_j} \alpha$

We get (note that $\omega = 2\pi i \frac{dx}{y} = 2\pi i \frac{d(\mathcal{P}(\tau))}{\mathcal{P}'(\tau)} = 2\pi i\, d\tau$.):

$$\begin{cases} \omega = 2\pi i\, d\tau \\ \eta = \frac{1}{2\pi i}\mathcal{P}(\tau)\, d\tau \end{cases}$$

$\mathrm{per}(\omega) = (\omega_1, \omega_2) = (2\pi i, 2\pi i \tau)$

$\mathrm{Per}(\eta) = ?$

Note that $\mathcal{P}(\tau)$ has no residue, so the periods make sense.

Fact 1: $\eta_1 = \frac{2\pi i}{12}\mathbb{P}(\tau) = \frac{2\pi i}{12} E_2(\tau)$ ← $1 + \dots$

Proof: $\eta_1 = \int_{\tau_0}^{\tau_0+1} \frac{1}{2\pi i}\mathcal{P}_\tau(z)\, dz = \dots$ (it's a classical computation, see Appendix to Katz's paper)

↖ can't take $\tau_0 = 0$ because it doesn't converge there.

Fact 2:

$$\omega_1\eta_2 - \omega_2\eta_1 = 2\pi i$$

Pf: We know that $\langle \omega, \eta \rangle = 1$ ✓ (algebraic pairing.)

It's an alternating bilinear pairing, which induces one on $\mathbb{C}^2$. So it's a multiple of the determinant.

Hence $\exists \lambda \in \mathbb{C}^\times$ s.t. $\forall \omega, \eta \in H^1_{dR}(E_\tau)$,

$$\langle \omega, \eta \rangle = \lambda(\omega_1\eta_2 - \omega_2\eta_1).$$

To compute λ, take $\omega = d\tau$, $\eta = d\bar{\tau}$. Then $\langle d\tau, d\bar{\tau} \rangle = \frac{1}{2\pi i}\int_{\mathbb{C}/\langle 1,\tau\rangle} d\tau d\bar{\tau} =$

$$= \frac{1}{2\pi i}(\tau - \bar{\tau})$$

and $\omega_1\eta_2 - \omega_2\eta_1 = \tau - \bar{\tau}$

From the two previous facts, we get:

$(\omega_1, \omega_2) = (2\pi i, 2\pi i \tau)$ ← derivative $= (0, 2\pi i)$

$(\eta_1, \eta_2) = \left(\frac{2\pi i}{12} P(\tau), \frac{2\pi i}{12} \tau P(\tau) + 1\right)$

Next, we need to compute $\nabla_\tau \omega$ = the unique class whose periods are $(0, 2\pi i)$

So $\nabla_\tau \omega = -2\pi i \left(\frac{P(\tau)}{12} \omega - \eta\right)$.

$$\nabla\left(f(\tau)\omega^k\right) = f'(\tau)\omega^k d\tau + f(\tau)\nabla(\omega^k) = f'(\tau)\omega^k d\tau + k f(\tau)\nabla(\omega)\omega^{k-1} =$$

$$= \frac{1}{2\pi i} f'(\tau)\omega^k (2\pi i\, d\tau) + k f(\tau)\, 2\pi i \left(\frac{P(\tau)}{12}\omega - \eta\right)\omega^{k-1} d\tau$$

$$= \left[\frac{1}{2\pi i} f'(\tau) - k f(\tau)\frac{P(\tau)}{12}\right]\omega^k\, 2\pi i\, d\tau + \underline{k f(\tau)\, 2\pi i\, \eta\, \omega^{k-1} d\tau}$$

The algebraic splitting consists on keeping only ω^k. We also take KS^{-1}, and get

$$\left(KS^{-1} \circ S_{alg} \circ \nabla\right)\left(f(\tau)\omega^k\right) = \left[\frac{1}{2\pi i} f'(\tau) - k f(\tau)\frac{P(\tau)}{12}\right]\omega^{k+2} =$$

$$= \left[q\frac{df}{dq}(q) - \frac{k f(q) P(q)}{12}\right]\left(\frac{dt}{t}\right)^{k+2} \leftarrow \text{Serre's operator!}$$

We want to understand the relation between ($\tau \in \mathcal{H} \cap F$ a CM point)

$$\delta_k f(\tau) \longleftrightarrow d^r f(A_\tau, \omega) \qquad \left(d = q\frac{d}{dq}\right)$$

The p-adic picture:

Let now $\bar{E}$ be an ordinary e.c over a p-adic ring R.

(think R = ring of integers of a finite unramified extension of $\mathbb{Q}_p$).

(then $R = W(\mathbb{F}_q)$, where $q = p^{[\mathrm{Frac}(R):\mathbb{Q}_p]}$)

↑ Witt-vectors

Note also that $R/p = \mathbb{F}_q$. Let $\bar{E}$ be the special fiber over $\mathbb{F}_q$.

We have the isogeny $F : \bar{E}_{/\mathbb{F}_q} \longrightarrow \bar{E}^{(p)}_{/\mathbb{F}_q}$ (Frobenius).

This induces a map:

$$\tilde{F} : H^1_{dR}\left(\bar{E}^{(p)}_{/\mathbb{F}_q}\right) \longrightarrow H^1_{dR}\left(\bar{E}_{/\mathbb{F}_q}\right)$$

which is $\mathbb{F}_q$-linear.

We can identify $H^1_{dR}\left(\bar{E}_{/\mathbb{F}_q}\right) \simeq H^1_{dR}\left(\bar{E}^{(p)}_{/\mathbb{F}_q}\right)$, which is not $\mathbb{F}_q$-linear, but φ-linear (φ the Frobenius on $\mathbb{F}_q$).

By composition, we get:

$$F : H^1_{dR}\left(\bar{E}_{/\mathbb{F}_q}\right) \longrightarrow H^1_{dR}\left(\bar{E}_{/\mathbb{F}_q}\right)$$

which is φ-semilinear:

$$F(\lambda\omega) = \lambda^p F(\omega) = \varphi(\lambda) F(\omega).$$

↓

Important Fact: The Frobenius F lifts canonically to $H^1_{dR}(E/R)$ giving a φ-semilinear operation on it.

If E is ordinary, then there exists $\eta \in H^1_{dR}(E/R)$ such that

$$\langle F(\eta) \rangle = R \cdot \eta \quad \text{(as } R\text{-modules)}.$$

(it's like saying that η is an eigenvector of "eigenvalue" a unit, but eigenvalues are not well-defined in semilinear maps).

Fact: ω and η generate $H^1_{dR}(E/R)$. We choose η such that $\langle \omega, \eta \rangle = 1$.

This gives us the unit-root splitting.

We need a formula for η on $\left(\text{Tate}_q, \left(\frac{dt}{t}\right)^{\omega}\right)_{/\mathbb{Z}_p[\![q]\!]}$:

Fact: $\eta = \nabla\left(q\frac{d}{dq}\right)\omega = \nabla_q \omega$

(in other words, $\nabla(\omega) = \eta \frac{dq}{q}$).

Let $S_{\text{unit root}}(a\omega + b\eta) = a\omega$. Then we compute: $\left(d = \theta = q\frac{d}{dq}\right)$

$$\nabla\left(f(q)\left(\frac{dt}{t}\right)^k\right) = \theta f(q)\left(\frac{dt}{t}\right)^k \frac{dq}{q} + f(q)\nabla\left(\left(\frac{dt}{t}\right)^k\right)$$

After $S_{\text{unit root}}$, get:

$$\left(S_{\text{unit root}} \circ \nabla\right)\left(f(q)\omega^k\right) = \left(\theta f(q)\right)\omega^k \frac{dq}{k}$$

$$\left(k S^{-1} \circ S_{\text{unit root}} \circ \nabla\right)(\quad) = (\theta f)(q)\omega^{k+2}$$

So the θ-operator on p-adic modular forms also arises from this setting.

Key Fact: Unlike the algebraic splittings, the Hodge and unit-root splittings are functorial:

If $\alpha: E \to E'$ is an isogeny, that is, $\alpha^*(\eta') \in \langle \eta \rangle$

In particular, if $E/\mathcal{O}_H$ is a CM-elliptic curve (F/Q quadratic im, H an ab. ext of F), and we fix $i_\infty: \mathcal{O}_H \hookrightarrow \mathbb{C}$, $i_p: \mathcal{O}_H \hookrightarrow R$ two embeddings (complex and p-adic resp.)

Then there is a decomposition:

$$H^1_{dR}(E/H) = H\omega \oplus H\eta$$

in such a way that: $\lambda d\bar{z}$, $\lambda \in \mathbb{C}^*$; λ' unit-root class

$$H^1_{dR}(E/\mathbb{C}) = \mathbb{C}\omega \oplus \mathbb{C}\eta'' \qquad H^1_{dR}(E/R) = R\omega \oplus R\eta'' = \lambda'$$

Let $\alpha \in \mathcal{O}_F$. Think of α as an isogeny $E \xrightarrow{\alpha} E$, such that

$$\alpha^*(\omega) = \alpha \cdot \omega \quad \text{(the usual normalization)}$$

Then $\alpha^*(d\bar{z}) = \bar{\alpha}\, d\bar{z}$

$$\alpha^*(\eta_{\text{unitroot}}) = \bar{\alpha}\, \eta_{\text{unitroot}}$$

So the two splittings (Hodge and unit-root) are the same there.

It follows that:

$$\delta_k^r E_k(A,\omega) = d^r E_k(A,\omega)$$

The LHS is related to $\zeta_F(k+r,-r)$

The RHS has Fourier coefficients $n^r \sigma_{k-1}(n)$ as long as $p \nmid n$.

So as long as $p \nmid n$, the function $(r,k) \mapsto n^r \sigma_{k-1}(n)$ is analytic on $\left(\mathbb{Z}_{p-1} \times \mathbb{Z}_p\right)^2$, so it provides an interpolation to $\zeta_F(k_1,k_2)$.

E.O.C.