NCMW - Modular Forms and Galois Representations

IISER Tirupati, Dec. 11-17, 2019

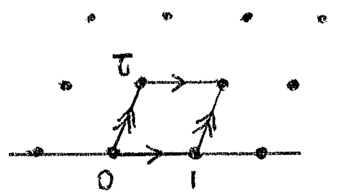
L-values and congruences of modular forms

Neil Dummigan

University of Sheffield

$\mathfrak{h} = \{\tau \in \mathbb{C} : \operatorname{Im}(\tau) > 0\}$ upper half-plane

Given $\tau \in \mathfrak{h}$, lattice $\Lambda_\tau = \langle 1, \tau \rangle_{\mathbb{Z}} = \mathbb{Z} \oplus \mathbb{Z}\tau$



Complex torus $\mathbb{C}/\Lambda_\tau$, a compact connected Riemann surface of genus one.

$H_1(\mathbb{C}/\Lambda_\tau) \simeq \Lambda_\tau$

Space of holomorphic differentials on $\mathbb{C}/\Lambda_\tau$ is $\langle dz \rangle_{\mathbb{C}}$
dimension = genus = 1.

If $\alpha \in \mathbb{C} \setminus \{0\}$,

$$\mathbb{C}/\Lambda_\tau \xrightarrow{\sim} \mathbb{C}/\alpha\Lambda_\tau \qquad \text{(Isomorphism of Riemann surfaces.)}$$
$$[z] \longmapsto [\alpha z]$$

Suppose $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, so $a, b, c, d \in \mathbb{Z}$ and $\det(\gamma) = 1$.

$\Lambda_\tau = \langle 1, \tau \rangle_{\mathbb{Z}} = \langle c\tau + d, a\tau + b \rangle_{\mathbb{Z}}$

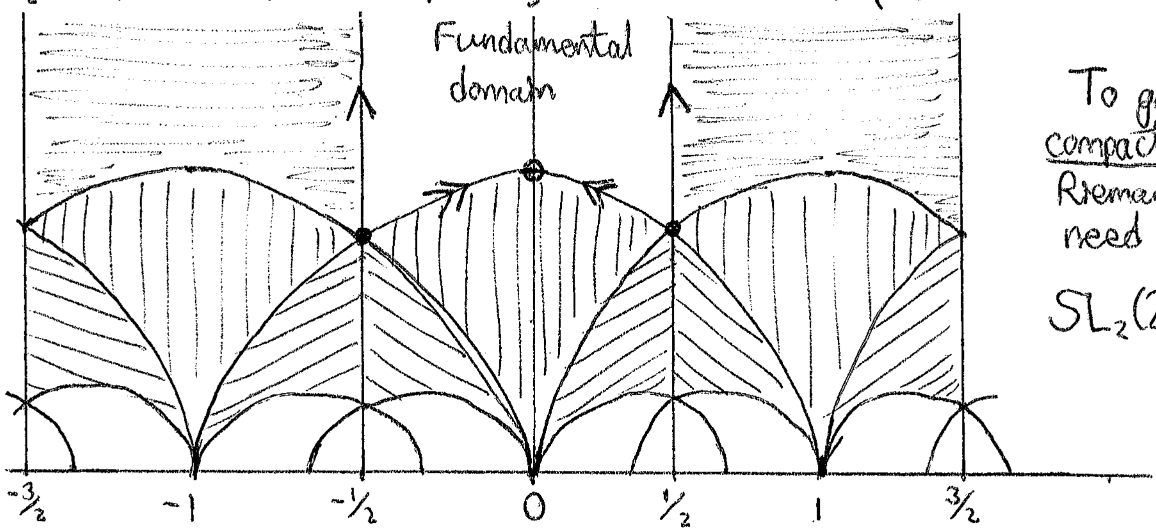
Letting $\alpha = (c\tau + d)^{-1}$, $\alpha \Lambda_\tau = \langle 1, \frac{a\tau+b}{c\tau+d} \rangle$
$\uparrow \in \mathfrak{h}$, since $\det(\gamma) = +1$.

so $\mathbb{C}/\Lambda_\tau \simeq \mathbb{C}/\Lambda_{\frac{a\tau+b}{c\tau+d}} =: \mathbb{C}/\Lambda_{\gamma(\tau)}$

Group action of $SL_2(\mathbb{Z})$ on $\mathfrak{h}$.

Natural bijection of sets

$\{\text{Complex tori up to isomorphism}\} \xrightarrow{\sim} SL_2(\mathbb{Z}) \backslash \mathfrak{h}$



To get a <u>compact</u> connected Riemann surface, need

$SL_2(\mathbb{Z}) \backslash \mathfrak{h}^*$

$\mathfrak{h}^* = \mathfrak{h} \cup \mathbb{P}^1(\mathbb{Q}) = \mathfrak{h} \cup \mathbb{Q} \cup \{\infty\}$

Given a positive integer N,

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

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ : \ \begin{matrix} c \equiv 0 \pmod N \\ d \equiv 1 \pmod N \end{matrix} \right\}$$

$$\{\text{Complex tori up to isomorphism}\} \xrightarrow{\sim} SL_2(\mathbb{Z}) \backslash \mathfrak{h}$$

$$\mathbb{C}/\Lambda_\tau \longmapsto [\tau] = SL_2(\mathbb{Z})\tau$$

extends to

$$\{(\text{Complex torus, Point of order } N)\} \xrightarrow{\sim} \Gamma_1(N) \backslash \mathfrak{h}$$

$$(\mathbb{C}/\Lambda_\tau, 1/N) \longmapsto \Gamma_1(N)\tau$$

and

$$\{(\text{Complex torus, Cyclic subgroup of order } N)\} \xrightarrow{\sim} \Gamma_0(N) \backslash \mathfrak{h}$$

$$(\mathbb{C}/\Lambda_\tau, \langle 1/N \rangle) \longmapsto \Gamma_0(N)\tau$$

How does this work?

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

$$(\mathbb{C}/\Lambda_\tau, 1/N) \xrightarrow{\sim} \left(\mathbb{C}/\Lambda_{\frac{a\tau+b}{c\tau+d}}, \frac{1}{N(c\tau+d)}\right)$$

$$\left(z \longmapsto \frac{z}{c\tau+d}\right)$$

$$\simeq \left(\mathbb{C}/\Lambda_{\frac{a\tau+b}{c\tau+d}}, \frac{a}{N} - \frac{c}{N}\frac{a\tau+b}{c\tau+d}\right)$$

$$\simeq \left(\mathbb{C}/\Lambda_{\frac{a\tau+b}{c\tau+d}}, \frac{1}{N}\right) \iff \frac{c}{N} \in \mathbb{Z} \text{ and } a \equiv 1 \pmod N$$

$$\iff \gamma \in \Gamma_1(N)$$

Similarly $(\mathbb{C}/\Lambda_\tau, \langle 1/N \rangle) \simeq \left(\mathbb{C}/\Lambda_{\frac{a\tau+b}{c\tau+d}}, \langle 1/N \rangle\right)$

$$\iff \frac{c}{N} \in \mathbb{Z} \iff \gamma \in \Gamma_0(N).$$

$$Y_0(N) := \Gamma_0(N) \backslash \mathfrak{h}$$

$$X_0(N) := \Gamma_0(N) \backslash \mathfrak{h}^*$$ Compact, connected Riemann surface, genus g

Let $\{\omega_1, \ldots, \omega_g\}$ be a basis for the space of holomorphic differentials on $X_0(N)$.

Define $i : X_0(N) \longrightarrow \mathbb{C}^g$

$$P \longmapsto \left(\int_\infty^P \omega_1, \ldots, \int_\infty^P \omega_g\right)$$

Path from ∞ to P is only defined up to loops $c \in H_1(X_0(N)) \simeq \mathbb{Z}^{2g}$ so we really only have a well-defined map

$$i : X_0(N) \longrightarrow \mathbb{C}^g/\Gamma, \quad \text{where } \Gamma \text{ is a rank } 2g \text{ lattice } \left\{ \left(\int_c \omega_1, \ldots, \int_c \omega_g \right) : c \in H_1(X_0(N)) \right\}$$

$$\mathbb{C}^g/\Gamma = J_0(N)$$

~~generated by~~

More generally, given a divisor $D = \sum_{P \in X_0(N)} n_P (P)$, a formal finite $\mathbb{Z}$-linear combination of points,

$$i(D) := \sum n_P \, i(P)$$

$$i : \mathrm{Div}(X_0(N)) \longrightarrow J_0(N)$$

Restrict to subgroup $\mathrm{Div}^0(X_0(N))$ of degree-zero divisors $(\sum n_P = 0)$

<u>Abel's Theorem</u>

$$\ker i = \{ \mathrm{div}(f) : f \text{ non-zero meromorphic function on } X_0(N) \} =: \mathrm{Pr}(X_0(N))$$

where $\mathrm{div}(f) := \sum_{P \in X_0(N)} \mathrm{ord}_P(f)(P)$

Let $\mathrm{Pic}^0(X_0(N)) := \mathrm{Div}^0(X_0(N)) / \mathrm{Pr}(X_0(N))$.

Then $i : \mathrm{Pic}^0(X_0(N)) \xrightarrow{\sim} J_0(N)$.

Fixing a prime number $p \nmid N$, we have a holomorphic map

$$\pi_1 : X_0(Np) \longrightarrow X_0(N)$$

$$\Gamma_0(Np)\tau \longmapsto \Gamma_0(N)\tau \qquad \text{Well-defined since } \Gamma_0(Np) \leq \Gamma_0(N).$$

Degree $[\Gamma_0(N) : \Gamma_0(Np)] = p+1$.

There is another map, also of degree $p+1$,

$$\pi_2 : X_0(Np) \longrightarrow X_0(N)$$

$$\Gamma_0(Np)\tau \longmapsto \Gamma_0(N)p\tau$$

Well-defined since if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(Np)$ then $p\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{a(p\tau)+pb}{(c/p)(p\tau)+d}$

and $\begin{pmatrix} a & pb \\ c/p & d \end{pmatrix} \in \Gamma_0(N)$.

Hecke correspondence $T_p = (\pi_2)_* \pi_1^* : J_0(N) \longrightarrow J_0(N)$

($(\pi_2)_*$: push-forward of divisor classes; π_1^*: pullback of divisor classes)

Let $\omega = f(\tau)\,d\tau$ be a holomorphic differential on $Y_0(N) = \Gamma_0(N)\backslash\mathfrak{h}$ (or perhaps its pullback to $\mathfrak{h}$).

ω must be invariant under $\Gamma_0(N)$, so given any $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$,

$$f(\tau)\,d\tau = f\left(\frac{a\tau+b}{c\tau+d}\right) d\left(\frac{a\tau+b}{c\tau+d}\right)$$

Now $d\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{(c\tau+d)a-(a\tau+b)c}{(c\tau+d)^2}\,d\tau = \frac{d\tau}{(c\tau+d)^2}$ since $ad-bc=1$.

Hence $$\boxed{f\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^2 f(\tau)} \quad *$$

Putting $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $f(\tau+1) = f(\tau)$ so f has a Fourier series

$$f(\tau) = \sum_{n\in\mathbb{Z}} a_n q^n \quad \text{where } q = e^{2\pi i\tau}$$

$dq = 2\pi i\, e^{2\pi i \tau}\,d\tau$

so $\frac{dq}{q} = 2\pi i\,d\tau$

Hence for $f(\tau)\,d\tau = \frac{1}{2\pi i}\sum_{n\in\mathbb{Z}} a_n q^n \frac{dq}{q}$ to be holomorphic at $\tau = i\infty$ $(q=0)$

must be $f(\tau) = \sum_{n\geq 1} a_n q^n$.

In other words, f vanishes at the cusp $i\infty$.

To extend to a holomorphic differential on $X_0(N)$, similarly f vanishes at all the cusps $\Gamma_0(N)\backslash\mathbb{P}^1(\mathbb{Q})$.

Holomorphic f satisfying $*$ (for all $\gamma \in \Gamma_0(N)$) and holomorphic at the cusps ~~and vanishing at all the cusps~~ is called a <u>modular form of weight 2 for $\Gamma_0(N)$</u> ($f \in M_2(\Gamma_0(N))$).

If f <u>vanishes</u> at the cusps it is called a <u>cusp form</u> ($f \in S_2(\Gamma_0(N))$).

$$S_2(\Gamma_0(N)) \xrightarrow{\sim} \{\text{Hol. diffs. on } X_0(N)\}$$
$$f \longmapsto f(\tau)\,d\tau$$

T_p naturally acts on $S_2(\Gamma_0(N))$:

$$T_p(f)(\tau) = p\,f(p\tau) + \frac{1}{p}\sum_{b=0}^{p-1} f\left(\frac{\tau+b}{p}\right)$$

If $f(\tau) = \sum_{n=1}^{\infty} a_n q^n$ then $(T_p f)(\tau) = \sum_{n=1}^{\infty} b_n q^n$

where $b_n = \begin{cases} a_{np} & \text{if } p \nmid n; \\ a_{np} + p\,a_{n/p} & \text{if } p \mid n. \end{cases}$ $**$

In fact there are Hecke operators T_n for all $n \geq 1$, all commuting with each other. The T_p for p prime generate all the others.

Petersson inner product on $S_2(\Gamma_0(N))$

$$\langle f, g\rangle = \int_{\Gamma_0(N)\backslash \mathfrak{h}} f(\tau)\overline{g(\tau)}\, dx\,dy \qquad \text{where } \tau = x+iy.$$

If $\gcd(n,N)=1$ then T_n is self-adjoint with respect to $\langle , \rangle$:
$\langle T_n f, g\rangle = \langle f, T_n g\rangle$

Since the T_n commute with each other, $S_2(\Gamma_0(N))$ has a basis of simultaneous eigenforms for all the T_n with $\gcd(n,N)=1$.

Let $S_2(\Gamma_0(N))^{old}$ be the subspace generated by elements of the form $f(\tau) = g(d\tau)$ where $g \in S_2(\Gamma_0(M))$ with $M \mid N$ $(M<N)$ and $d \mid (N/M)$.

Let $S_2(\Gamma_0(N))^{new}$ be the orthogonal complement of $S_2(\Gamma_0(N))^{old}$ with respect to $\langle , \rangle$.

<u>Fact</u> $S_2(\Gamma_0(N))^{new}$ has a basis of simultaneous eigenforms for <u>all</u> T_n.
Such a "newform" $f = \sum_{n=1}^{\infty} a_n q^n$ can be scaled so that $a_1 = 1$ (normalised)
and then formulas such as ** show that $\boxed{T_n f = a_n f}$

i.e. the Fourier coefficients are the Hecke eigenvalues.

The T_n act naturally on the $\mathbb{Z}$-module $H_1(X_0(N))$.
It follows that the eigenvalues a_n are algebraic integers.
For a given f they generate a finite extension $K_f : \mathbb{Q}$.

Special case: $K_f = \mathbb{Q}$, the a_n are rational integers.

<u>Example</u> $\dim S_2(\Gamma_0(11)) = 1$. For $X_0(11)$, $g=1$. $i : X_0(11) \xrightarrow{\sim} J_0(11)$.

$S_2(\Gamma_0(11))$ spanned by a normalised newform $f = q\prod_{n=1}^{\infty}\left[(1-q^n)^2(1-q^{11n})^2\right]$

$$= q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} \cdots$$

What is the meaning of these coefficients?

Up to now, we have looked at $\mathbb{C}/\Lambda_\tau$ and $X_0(N) = \Gamma_0(N)\backslash \mathfrak{h}^*$ purely as Riemann surfaces.
Henceforth, we need to look at them as algebraic curves.

Given $\Lambda_\tau = \langle 1, \tau\rangle_{\mathbb{Z}}$ define the Weierstrass $\wp$-function

$$\wp_{\Lambda_\tau}(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda_\tau \setminus \{0\}} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2}\right)$$

This is doubly periodic: $\wp_{\Lambda_\tau}(z) = \wp_{\Lambda_\tau}(z+\omega) \quad \forall \omega \in \Lambda_\tau$

It has a double pole at each lattice point and is holomorphic elsewhere on $\mathbb{C}$.

It satisfies the identity

$$\wp'(z)^2 = 4\wp(z)^3 - g_2(\Lambda_\tau)\wp(z) - g_3(\Lambda_\tau),$$

where $g_2(\Lambda_\tau) = 60\,G_4(\tau)$

$g_3(\Lambda_\tau) = 140\,G_6(\tau)$

and for even $k>2$ the Eisenstein series $G_k(\tau) = \sum_{\substack{\omega\in\Lambda_\tau \\ \omega\neq 0}} \frac{1}{\omega^k} = \sum_{\substack{(m,n) \\ \in \mathbb{Z}^2\setminus\{(0,0)\}}} \frac{1}{(m\tau+n)^k}$

Since, for any $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $\Lambda_{\frac{a\tau+b}{c\tau+d}} = (c\tau+d)^{-1}\Lambda_\tau$,

$G_k\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau+d)^k G_k(\tau)$.

Also, $\lim_{\tau\to i\infty} \sum_{n\in\mathbb{Z}} \frac{1}{n^k} = 2\zeta(k)$ is finite, so $G_k \in M_k(SL_2(\mathbb{Z}))$.

Let E_τ be the algebraic curve $y^2 = 4x^3 - g_2(\Lambda_\tau)x - g_3(\Lambda_\tau)$

$\left(Y^2 Z = 4X^3 - g_2 XZ^2 - g_3 Z^3 \text{ as a projective curve}\right)$

Then we have an isomorphism of Riemann surfaces

$$\mathbb{C}/\Lambda_\tau \xrightarrow{\sim} E_\tau(\mathbb{C})$$

$$z+\Lambda_\tau \longmapsto \begin{cases} (x,y) = (\wp_{\Lambda_\tau}(z), \wp'_{\Lambda_\tau}(z)) & z\notin\Lambda_\tau \\ O = \text{“}\infty\text{”} & z\in\Lambda_\tau \end{cases}$$

i.e. $z+\Lambda_\tau \longmapsto [X,Y,Z] = \begin{cases} [\wp_{\Lambda_\tau}(z), \wp'_{\Lambda_\tau}(z), 1] & z\notin\Lambda_\tau \\ [0, 1, 0] & z\in\Lambda_\tau \end{cases}$

Inverse map $E_\tau(\mathbb{C}) \xrightarrow{\sim} \mathbb{C}/\Lambda_\tau$

$$P = (x,y) \longmapsto \int_O^P \frac{dx}{y} \quad \text{modulo } \Lambda_\tau$$

Note that $\frac{dx}{y} = \frac{d\wp(z)}{\wp'(z)} = \frac{\wp'(z)\,dz}{\wp'(z)} = dz$, so the integral of $\frac{dx}{y}$ around a loop on $E_\tau(\mathbb{C})$ is $\int_0^\omega dz = \omega$ for some $\omega\in\Lambda_\tau$.

Since $\mathbb{C}/\Lambda_\tau$ is an abelian group under addition,

$E_\tau(\mathbb{C})$ has the structure of an abelian group, neutral element O (at infinity).

$E_\tau(\mathbb{C}) \simeq \mathrm{Pic}^0(E_\tau(\mathbb{C}))$ Group isomorphism

$P \longmapsto [(P)-(O)]$.

Geometrically, the three intersection points of $E_\tau(\mathbb{C})$ with a (projective) line (counted with multiplicity) add up to O.

If $(x_1,y_1)+(x_2,y_2) = (x_3,y_3)$ then

$x_3, y_3 \in \mathbb{Q}(x_1,y_1,x_2,y_2,g_2,g_3)$

$(*)$ $\left[\begin{array}{l} y^2+xy = x^3 - \frac{36}{j-1728}x - \frac{1}{j-1728} \\ \text{has } j\text{-invariant } j. \end{array} \right.$

E_τ is an algebraic group (elliptic curve) defined over the field $\mathbb{Q}(g_2,g_3)$.

$g_2^3,\ g_3^2 \in M_{12}(SL_2(\mathbb{Z}))$, in fact

$\Delta := g_2^3 - 27g_3^2 \in S_{12}(SL_2(\mathbb{Z}))$.

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

($\tau(n)$: Ramanujan tau function.)

$j := \dfrac{1728\, g_2^3}{\Delta} = q^{-1} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \dots$

$j\left(\frac{a\tau+b}{c\tau+d}\right) = j(\tau) \quad \forall \begin{pmatrix} a & b \\ c & d\end{pmatrix} \in SL_2(\mathbb{Z}),\ \tau\in\mathfrak{h}$. (A modular <u>function</u>.)

$j : SL_2(\mathbb{Z})\backslash\mathfrak{h}^* \xrightarrow{\sim} \mathbb{C}\cup\{\infty\} = \mathbb{P}^1(\mathbb{C})$, isomorphism of Riemann surfaces.

So now we see $X_0(1)$ as the set of $\mathbb{C}$-points of an algebraic curve $\mathbb{P}^1$ defined over $\mathbb{Q}$.

From now on we write $X_0(1)(\mathbb{C})$ instead of $X_0(1)$ for $SL_2(\mathbb{Z})\backslash\mathfrak{h}^*$, and write $X_0(1)$ for the algebraic curve

Similarly we write $X_0(N)(\mathbb{C})$ for $\Gamma_0(N)\backslash\mathfrak{h}^*$

$X_1(N)(\mathbb{C})$ for $\Gamma_1(N)\backslash\mathfrak{h}^*$

and $X_0(N)$, $X_1(N)$ are algebraic curves defined over $\mathbb{Q}$.

(This follows from $(*)$) [This is technically not quite the true story, but is intended to give a rough idea: 3 variables x,y,j, two equations: that of E, and from (x,y) being an N-torsion pt.]

<u>Example</u> $X_0(11)$ is the elliptic curve $E: y^2+y = x^3-x^2-10x-20$

The group $E(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$, generated by the point $P=(5,5)$.

(In general Mordell's Thm $\Rightarrow$ $E(\mathbb{Q})$ finitely generated.)

$[5]P = O$ ($[5]$: multiplication by 5 map.)

In fact, on $X_0(11)$, P is the cusp $0 \longmapsto [(0)-(\infty)]$ in $\mathrm{Pic}^0(X_0(11)) = J_0(11)$.

Given elliptic curves E_1, E_2 and an isogeny $\psi : E_1 \to E_2$
(a non-constant morphism of curves, taking O_1 to O_2,
necessarily a group homomorphism),

$\psi : \mathrm{Pic}^0(E_1) \longrightarrow \mathrm{Pic}^0(E_2)$ is ψ_*, push-forward of divisor classes.

Pull-back $\psi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)$
comes from a <u>dual</u> isogeny $\hat{\psi} : E_2 \to E_1$.

$\hat{\psi} \circ \psi : E_1 \to E_1$ (i.e. $\psi^* \psi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_1)$)

is $[\deg \psi]$, multiplication by the degree.

For each prime $p \neq 11$, $E = X_0(11)$ has <u>good reduction</u> at p :

$\tilde{E}/\mathbb{F}_p$ is nonsingular, an elliptic curve in characteristic p.
$\tilde{E} : y^2 + y = x^3 - x^2 - 10x - 20$

May count the points in the finite set $\tilde{E}(\mathbb{F}_p)$.

e.g. $\tilde{E}(\mathbb{F}_2) = \{O, (0,0), (0,1), (1,0), (1,1)\}$ $\quad \# \tilde{E}(\mathbb{F}_2) = 5$

$\tilde{E}(\mathbb{F}_3) = \{O, (1,0), (1,2), (2,0), (2,2)\}$ $\quad \# \tilde{E}(\mathbb{F}_3) = 5$

In general, Frobenius map $\varphi_p : \tilde{E}(\overline{\mathbb{F}}_p) \to \tilde{E}(\overline{\mathbb{F}}_p)$

$(x, y) \mapsto (x^p, y^p)$

This is a purely inseparable isogeny of degree p.
$\ker \varphi_p = \varphi_p^{-1}\{O\} = \{O\}$ has size 1, not $\deg \varphi_p = p$.

$$\tilde{E}(\mathbb{F}_p) = \{ Q \in \tilde{E}(\overline{\mathbb{F}}_p) : \varphi_p(Q) = Q \}$$

$$= \ker(\underbrace{1 - \varphi_p}_{\text{separable isogeny}})$$

$$[\# \tilde{E}(\mathbb{F}_p)] = [\deg(1 - \varphi_p)] = \widehat{(1 - \varphi_p)} \circ (1 - \varphi_p)$$

$$= 1 - (\hat{\varphi}_p + \varphi_p) + \hat{\varphi}_p \circ \varphi_p$$

$$= 1 + p - (\varphi_p + \hat{\varphi}_p)$$

<u>Eichler-Shimura Congruence Relation</u>

Viewing E ~~and~~ as $X_0(11) \simeq J_0(11)$,

$\tilde{T}_p = \varphi_p + \hat{\varphi}_p$ in $\mathrm{End}(\tilde{J}_0(11))$

Hence $\boxed{\# \tilde{E}(\mathbb{F}_p) = 1 + p - a_p}$ $\quad (\Rightarrow |a_p| < 2\sqrt{p})$

p	a_p	$\#\tilde{E}(\mathbb{F}_p) = 1+p-a_p$
2	-2	5
3	-1	5
5	1	5
7	-2	10
[11	1	11]
13	4	10
17	-2	20

Notice always $5 \mid \#\tilde{E}(\mathbb{F}_p)$ (for $p \neq 11$)

This is because the reduction of $P = (5,5)$ gives an element of order 5.

In other words $\boxed{a_p \equiv 1+p \pmod 5 \quad \forall \text{ primes } p \neq 11.}$

The Dirichlet series

$$L_f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \frac{1}{(1-11^{-s})} \prod_{p \neq 11} \frac{1}{1-a_p p^{-s} + p^{1-2s}}$$

is also $L_E(s)$.

As $L_E(s)$, it converges for $\mathrm{Re}(s) > 3/2$ (since $|a_p| < 2p^{1/2}$)

But as $L_f(s)$,

$$\int_0^{\infty} f(iy) y^s \frac{dy}{y} = (2\pi)^{-s} \Gamma(s) L_f(s)$$

Using this, may show that (i) $L_f(s)$ is analytic on $\mathbb{C}$

(ii) $\xi(s) = \pm \xi(2-s)$

where $\xi(s) = 11^{s/2} (2\pi)^{-s} \Gamma(s) L_f(s)$.

Central point $s=1$.

__Birch and Swinnerton-Dyer Conjecture__

$$\mathrm{Rank}\, E(\mathbb{Q}) = \operatorname*{ord}_{s=1} L_E(s).$$

Known by theorem of Kolyvagin, Gross, Zagier when RHS $\leq$ 1.

In this example $L_E(1) \neq 0$ and $E(\mathbb{Q})$ is finite.

Refined conjecture

$$L_E(1) = \frac{c_{11} \cdot \# Ш}{(\# E(\mathbb{Q}))^2} \int_{E(\mathbb{R})} \omega$$

$\omega = \dfrac{dx}{2y+1}$ where $y^2 + y = x^3 - x^2 - 10x - 20$ Global minimal Weierstrass equation

$\Delta = -11^5$.

$c_{11} = 5$, $\# Ш = 1$, $\# E(\mathbb{Q}) = 5$.

$$\int_{E(\mathbb{R})} \omega \approx 1.26920930428$$

$$L_E(1) \approx 0.253841860856$$

As a holomorphic differential on $X_0(11)(\mathbb{C}) = \Gamma_0(11)\backslash\mathfrak{h}^*$, ω must be some multiple of $f(\tau)d\tau$

Recall that $f(\tau)\,d\tau = \frac{1}{2\pi i}\left(\sum_{n=1}^{\infty} a_n q^n\right)\frac{dq}{q}$ $\quad q = e^{2\pi i \tau}$

In fact, since ω is defined over $\mathbb{Q}$, must have $\omega = c\, 2\pi i f(\tau)\,d\tau$ for some $c \in \mathbb{Q}^\times$ (Manin constant)

Conjecturally $c = 1$ (certainly true in this example).

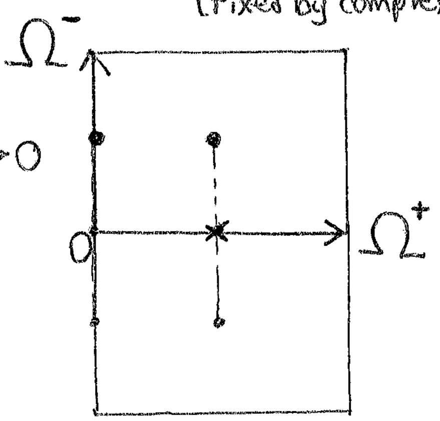
We have the Riemann surface $X_0(11)(\mathbb{C})$ as $\Gamma_0(11)\backslash\mathfrak{h}^*$ but as $E(\mathbb{C})$ it is $\mathbb{C}/\Lambda$ for some lattice Λ.

What does Λ look like?

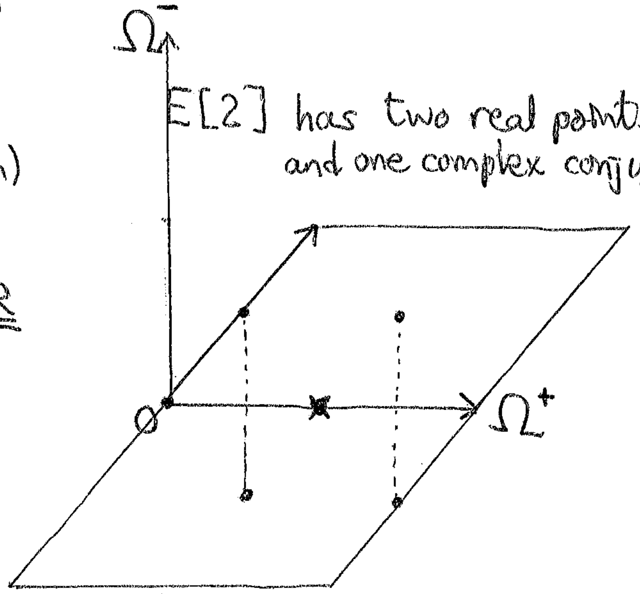
$\underbrace{E[2]}_{\text{2-torsion points}} \subseteq E(\mathbb{R})$ (fixed by complex conjugation)

$E[2]$ has two real points and one complex conjugate pair

$\Delta > 0$

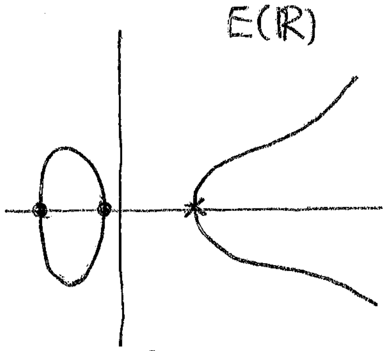


OR



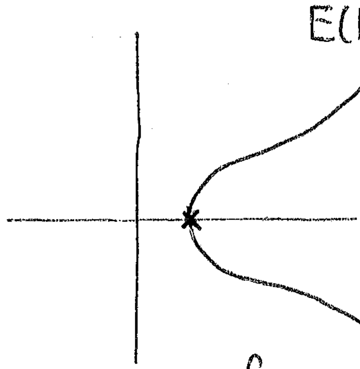
$\Delta < 0$

E(ℝ)



$\int_{E(\mathbb{R})} \omega = 2\Omega^+$

E(ℝ)



$\int_{E(\mathbb{R})} \omega = \Omega^+$

[$E = X_0(11)$ is this case.]

$$\int_{E(\mathbb{C})} \omega\wedge\overline{\omega} = \int_{\mathbb{C}/\Lambda} dz\wedge d\bar{z} = 2i\int_{\mathbb{C}/\Lambda} dx\,dy = \Omega^+\Omega^-$$

But $\omega = 2\pi i f(\tau)\,d\tau \Rightarrow \int_{E(\mathbb{C})} \omega\wedge\overline{\omega} = \int_{X_0(11)(\mathbb{C})} (2\pi)^2 |f(\tau)|^2\, d\tau\wedge d\bar{\tau} = 2i(2\pi)^2\langle f,f\rangle$

Hence $\boxed{\Omega^+\Omega^- = 2i\,(2\pi)^2\langle f,f\rangle}$ (Would be $i(2\pi)^2\langle f,f\rangle$ in other case.)

Another example

$\dim(S_2(\Gamma_0(37))) = 2$, spanned by normalised newforms

$$f = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 6q^9 + 4q^{10} - 5q^{11} - 6q^{12} - 2q^{13} \dots$$

$$g = q + q^3 - 2q^4 - q^7 - 2q^9 + 3q^{11} - 2q^{12} - 4q^{13} \dots$$

$X_0(37)$ has genus 2 so is not an elliptic curve.

Neither is $J_0(37)$, which is a 2-dimensional abelian variety $/\mathbb{Q}$.

All the Hecke correspondences $T_n \in \mathrm{End}(J_0(14))$ are defined over $\mathbb{Q}$. Let $\mathbb{T}$ be the ring they generate, over $\mathbb{Z}$.

We have a homomorphism $\theta_f : \mathbb{T} \to \mathbb{Z}$, $T_n \mapsto a_n(f)$

Let $I_f = \ker \theta_f$

Then $E_f := J_0(37) / I_f J_0(37)$ is an elliptic curve $/\mathbb{Q}$, on which T_n acts as $[a_n]$. (Eichler-Shimura construction.)

For primes $p \nmid 14$, E_f has good reduction at p, and
$$\#\tilde{E}_f(\mathbb{F}_p) = 1 + p - a_p(f).$$

$$X_0(37) \xrightarrow{i} J_0(37) \xrightarrow{\psi_f} E_f$$

$\psi_f : J_0(37) \to E_f$ is $(\pi_f)_* : \mathrm{Pic}^0(X_0(37)) \to \mathrm{Pic}^0(E_f)$

Also have $\widehat{\psi_f} : E_f \to J_0(37)$ which is $(\pi_f)^* : \mathrm{Pic}^0(E) \to \mathrm{Pic}^0(X_0(37))$.

$\psi_f \circ \widehat{\psi_f} : E_f \to E_f$ is $[\deg \pi_f]$

↑ "modular degree" m_{E_f}

$E_f : y^2 + y = x^3 - x$ $\qquad E_f(\mathbb{Q}) \simeq \mathbb{Z}$, generated by $P = (0,0)$

Similarly have $E_g : y^2 + y = x^3 + x^2 - 23x - 50$

$E_g(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, generated by $P = (8,18)$

In fact
$$0 \to E_g \xrightarrow{\widehat{\psi_g}} J_0(37) \xrightarrow{\psi_f} E_f \to 0$$
$$0 \to E_f \xrightarrow{\widehat{\psi_f}} J_0(37) \xrightarrow{\psi_g} E_g \to 0$$
and $\deg \pi_f = \deg \pi_g = 2$.

Inside $J_0(37)$, $E_f \cap E_g$ (i.e. $\hat{\psi}_f(E_f) \cap \hat{\psi}_g(E_g)$) is $E_f[2] = E_g[2]$, since $E_f[2] = E_f[\psi_f \circ \hat{\psi}_f] \simeq \hat{\psi}_f(E_f) \cap \ker \psi_f = \hat{\psi}_f(E_f) \cap \hat{\psi}_g(E_g)$.

Since T_n acts as $a_n(f)$ on E_f
$a_n(g)$ on E_g

$E_f[2] = E_g[2]$ inside $J_0(37)$ $\Rightarrow$ $\boxed{a_n(f) \equiv a_n(g) \pmod 2 \quad \forall n \geq 1}$

In general we have $\pi_f : X_0(N) \longrightarrow E_f$
(where $f \in S_2(\Gamma_0(N))$ is a normalised newform with rational integer coefficents).

If $E_f : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ global minimal Weierstrass equation

$$\omega = \frac{dx}{2y + a_1 x + a_3}$$

$\pi_f^*(\omega) = c \, 2\pi i \, f(\tau) \, d\tau$ for $c \in \mathbb{Q}^\times$ (conjecturally $c = 1$)

$$\int_{X_0(N)} \pi_f^*(\omega \wedge \bar{\omega}) = \deg \pi_f \int_{E(\mathbb{C})} \omega \wedge \bar{\omega}$$

$$\Rightarrow \boxed{\frac{4i}{\#E(\mathbb{R})[2]} (2\pi)^2 \langle f, f \rangle = (\deg \pi_f) \, \Omega^+ \Omega^-}$$

Yet another example

$1058 = 2 \cdot 23^2$ $\qquad \dim(S_2(\Gamma_0(1058))) = 115$

Among the normalised newforms are

$$f = q - q^2 - 2q^3 + q^4 - 3q^5 + 2q^6 - 2q^7 - q^8 + q^9 + 3q^{10} - 6q^{11} - 2q^{12} - q^{13} + 2q^{14} \ldots$$

$$g = q - q^2 + 3q^3 + q^4 + 2q^5 - 3q^6 - 2q^7 - q^8 + 6q^9 - 2q^{10} + 4q^{11} + 3q^{12} + 4q^{13} + 2q^{14} \ldots$$

LMFDB
1058.a2 $E_f : y^2 + xy + y = x^3 + 2$ $\qquad \deg \pi_f = 2^4 \cdot 5$

1058.e1 $E_g : y^2 + xy = x^3 - x^2 - 332311x - 73733731$ $\qquad \deg \pi_g = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 23$

In fact $E_f[5] = E_g[5]$ inside $J_0(1058)$, $*$

and $\boxed{a_n(f) \equiv a_n(g) \pmod 5 \quad \forall n \geq 1}$

$E_f(\mathbb{Q}) \simeq \mathbb{Z}^2$, generated by $(-1, 1), (0, 1)$

$E_g(\mathbb{Q}) = \{O\}$

$L_f(1) = 0$ $\qquad \dfrac{L_g(1)}{\Omega^+} = 25$

(in agreement with Birch & Swinnerton-Dyer)

Actually, $* \Rightarrow \left(L_f(1) = 0 \Rightarrow \frac{L_g(1)}{\Omega^+} \equiv 0 \pmod 5 \right)$

BSD says $\frac{L_g(1)}{\Omega^+} = \frac{c_2 c_{23} \# Ш}{(\# E(\mathbb{Q})_{tors})^2}$ but $c_2 = c_{23} = 1$ and $\# E(\mathbb{Q})_{tors} = 1$

so should have $\# Ш = 25$

(Visibility) Construction of Cremona and Mazur directly links rational points of infinite order on E_f with elements in $Ш[5]$ for E_g, via the mod **5** congruence.

Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. We have ~~an exact~~ a short exact sequence of $G_{\mathbb{Q}}$-modules:

$$0 \longrightarrow E_f(\overline{\mathbb{Q}})[5] \longrightarrow E_f(\overline{\mathbb{Q}}) \xrightarrow{[5]} E_f(\overline{\mathbb{Q}}) \to 0$$

This gives rise to a long exact sequence in Galois cohomology:

$$0 \to H^0(G_{\mathbb{Q}}, E_f[5]) \to H^0(G_{\mathbb{Q}}, E_f(\overline{\mathbb{Q}})) \xrightarrow{[5]} H^0(G_{\mathbb{Q}}, E_f(\overline{\mathbb{Q}})) \xrightarrow{\delta}$$
$$H^1(G_{\mathbb{Q}}, E_f[5]) \to H^1(G_{\mathbb{Q}}, E_f(\overline{\mathbb{Q}})) \to H^1(G_{\mathbb{Q}}, E_f(\overline{\mathbb{Q}})) \to \dots$$

Part of this is

$$E_f(\mathbb{Q}) \xrightarrow{[5]} E_f(\mathbb{Q}) \xrightarrow{\delta} H^1(G_{\mathbb{Q}}, E_f[5])$$

$$H^1(G_{\mathbb{Q}}, E_f[5]) = \frac{Z^1(G_{\mathbb{Q}}, E_f[5])}{B^1(G_{\mathbb{Q}}, E_f[5])} \quad \left(\frac{\text{cocycles}}{\text{coboundaries}} \right)$$

where $Z^1(G_{\mathbb{Q}}, E_f[5]) = \{ c : G_{\mathbb{Q}} \to E_f[5] \mid c(\sigma\tau) = c(\sigma) + \sigma c(\tau) \ \forall \sigma, \tau \in G_{\mathbb{Q}} \}$

$B^1(G_{\mathbb{Q}}, E_f[5]) = \{ c : G_{\mathbb{Q}} \to E_f[5] \mid c(\sigma) = \sigma(m) - m \ \forall \sigma \in G_{\mathbb{Q}},$ for some $m \in E_f[5] \}$

$B^1 \subseteq Z^1$ because $\sigma\tau(m) - m = [\sigma(m) - m] + \sigma[\tau(m) - m]$

Given $P \in E_f(\mathbb{Q})$, $\exists Q \in E_f(\overline{\mathbb{Q}})$ such that $[5]Q = P$ (Q determined up to addition of element of $E_f[5]$).

$\delta(P)$ is represented by the cocycle

$$\sigma \longmapsto \sigma(Q) - Q$$

Remarks (i) This is a cocycle, for the same reason that $B^1 \subseteq Z^1$.

(ii) It is valued in $E_f[5]$, since $[5](\sigma(Q) - Q) = \sigma([5]Q) - [5]Q = \sigma(P) - P = 0$.

(iii) A different choice of Q only changes it by a coboundary.

For any prime p, fixing $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ so $G_{\mathbb{Q}_p} \hookrightarrow G_{\mathbb{Q}}$

$$\begin{array}{ccc} E_f(\mathbb{Q}) & \xrightarrow{\delta} & H^1(G_{\mathbb{Q}}, E_f[5]) \\ \downarrow & \circlearrowright & \downarrow \text{res.} \\ E_f(\mathbb{Q}_p) & \xrightarrow{\delta_p} & H^1(G_{\mathbb{Q}_p}, E_f[5]) \end{array}$$

so $\mathrm{res}(\delta(E_f(\mathbb{Q}))) \subseteq \delta_p(E_f(\mathbb{Q}_p))$ (similarly for $p=\infty$, $\mathbb{Q}_p = \mathbb{R}$)

i.e. $\delta(E_f(\mathbb{Q})) \subseteq \mathrm{Sel}_5(E_f)$.

Since $E_f(\mathbb{Q}) \simeq \mathbb{Z}^2$, $E_f(\mathbb{Q})/5E_f(\mathbb{Q}) \hookrightarrow H^1(G_{\mathbb{Q}}, E_f[5])$ gives a $(\mathbb{Z}/5\mathbb{Z})^2$ inside $H^1(G_{\mathbb{Q}}, E_f[5])$, in fact in $\mathrm{Sel}_5(E_f)$.

Recall $*$, that $E_f[5] = E_g[5]$ inside $J_0(1058)$, so certainly $E_f[5] \simeq E_g[5]$ as $G_{\mathbb{Q}}$-modules

and the $(\mathbb{Z}/5\mathbb{Z})^2$ inside $H^1(G_{\mathbb{Q}}, E_f[5])$, i.e. $\delta(E_f(\mathbb{Q}))$, is equally inside $H^1(G_{\mathbb{Q}}, E_g[5])$.

One may show it is even inside $\mathrm{Sel}_5(E_g)$.

But $E_g(\mathbb{Q}) = \{0\}$, so it can't be in the image of $E_g(\mathbb{Q})$.
It must map on to a $(\mathbb{Z}/5\mathbb{Z})^2$ in $H^1(G_{\mathbb{Q}}, E_g(\overline{\mathbb{Q}}))$, everywhere locally trivial

i.e. to $(\mathbb{Z}/5\mathbb{Z})^2$ inside $Ш_{E_g}$.

<u>Another look at $E = X_0(11)$</u>, $f = q\prod_{n=1}^{\infty}[(1-q^n)^2(1-q^{11n})^2]$

<u>and the congruence $a_p \equiv 1+p \pmod 5$</u> $\forall$ prime $p \neq 11$,

which came from the rational point $P=(5,5)$ of order 5.
(5 divides $\#\tilde{E}(\mathbb{F}_p) = 1+p-a_p$.)

$E[5]$ is a 2-dimensional $\mathbb{F}_5$-vector space, with a linear action of $G_{\mathbb{Q}}$.
$P \in E[5]$ is fixed by $G_{\mathbb{Q}}$
The same is true of any multiple of P.
So $G_{\mathbb{Q}}$ acts trivially on the line spanned by P inside $E[5]$.
As a representation of $G_{\mathbb{Q}}$, $E[5]$ is reducible, with a trivial 1-dimensional submodule.

Completing P to a basis for $E[5]$ we get a homomorphism

$$\rho: G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_5)$$

$$\sigma \longmapsto \begin{bmatrix} 1 & * \\ 0 & \chi(\sigma) \end{bmatrix}$$

What is the character χ (the other composition factor)?

Weil pairing $E[5] \times E[5] \longrightarrow \mu_5$ (group of 5th roots of unity)

is bilinear, non-degenerate, skew symmetric and $G_{\mathbb{Q}}$-equivariant $(\sigma Q, \sigma R) = \sigma(Q,R)$.

It follows that $\chi = \det\rho$ is the cyclotomic character by which $G_{\mathbb{Q}}$ acts on μ_5.

If $\mu_5 = \langle \zeta_5 \rangle$ then $G_{\mathbb{Q}}$ acts on μ_5 via the quotient

$$Gal(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \simeq (\mathbb{Z}/5\mathbb{Z})^\times$$

$$(\zeta_5 \mapsto \zeta_5^t) \longleftarrow [t]$$

On the 1-dimensional $\mathbb{F}_5$-vector space μ_5, this is scalar multiplication by $[t] \in \mathbb{F}_5$.

For $p \neq 5$, μ_5 survives reduction mod p,

and $G_{\mathbb{Q}_p}$ acts on μ_5 via $Gal(\overline{\mathbb{F}}_p/\mathbb{F}_p)$

If $Frob_p \in G_{\mathbb{Q}}$ is any element reducing to $(x \mapsto x^p)$ in $Gal(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, then $Frob_p(\zeta_5) = \zeta_5^p$ so $\chi(Frob_p) = p$.

$$\rho(Frob_p) = \begin{bmatrix} 1 & * \\ 0 & p \end{bmatrix} \quad (p \neq 5)$$

and $tr\,\rho(Frob_p) = 1 + p$ (in $\mathbb{F}_5$)

But Eichler-Shimura $\Rightarrow tr\,\rho(Frob_p) = a_p$ (for $p \neq 11, 5$)

We recover $a_p \equiv 1 + p \pmod 5$.

<u>A similar example for higher weight</u>

$$\Delta(\tau) = q\prod_{n=1}^{\infty}(1-q^n)^{24} = \sum_{n=1}^{\infty}\tau(n)q^n. \qquad S_{12}(SL_2(\mathbb{Z})) = \langle\Delta\rangle_{\mathbb{C}}.$$

Ramanujan's congruence

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

In particular, for prime p,

$$\tau(p) \equiv 1 + p^{11} \pmod{691}.$$

This is a congruence of Hecke eigenvalues between Δ and the Eisenstein series G_{12}.

A theorem of Deligne implies the following.

For any prime ℓ, there exists a continuous representation $\rho_\ell : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Q}_\ell)$ such that

(i) ρ_ℓ is unramified at any prime $p \neq \ell$, meaning $G_{\mathbb{Q}_p} \subset G_{\mathbb{Q}}$ acts through its quotient $G_{\mathbb{Q}_p}/I_p \simeq G_{\mathbb{F}_p}$

generated by Frob_p — I_p: inertia subgroup

(ii) $\rho_\ell(\mathrm{Frob}_p^{-1})$ has characteristic polynomial

$$X^2 - \tau(p)X + p^{11}$$

In particular $\mathrm{tr}\,\rho_\ell(\mathrm{Frob}_p^{-1}) = \tau(p)$.
$\det \rho_\ell(\mathrm{Frob}_p^{-1}) = p^{11}$.

<u>NB</u> The Euler factor at p in $L_\Delta(s)$ is

$$[\det(I - \rho_\ell(\mathrm{Frob}_p^{-1})p^{-s})]^{-1}.$$

Let $T_\ell\mu := \varprojlim_n \mu_{\ell^n}$, isomorphic to $\mathbb{Z}_\ell$ as a group.

$G_{\mathbb{Q}}$ acts on $T_\ell\mu$ via the ℓ-adic cyclotomic character

$$\varepsilon_\ell : G_{\mathbb{Q}} \longrightarrow \mathbb{Z}_\ell^\times \subset \mathbb{Q}_\ell^\times$$
$$\mathrm{Frob}_p \longmapsto p$$

and on μ_ℓ via the reduction $\bar{\varepsilon}_\ell : G_{\mathbb{Q}} \rightarrow \mathbb{F}_\ell^\times$

Given a $\mathbb{Z}_\ell[G_{\mathbb{Q}}]$-module M (or $\mathbb{Q}_\ell[G_{\mathbb{Q}}]$-module, or $\mathbb{F}_\ell[G_{\mathbb{Q}}]$-module), define the Tate twist $M(n)$ (for $n \in \mathbb{Z}$) to be the same as M, but with the $G_{\mathbb{Q}}$-action multiplied by the n^{th} power of ε_ℓ, so the action of Frob_p is multiplied by p^n.
i.e. $M(n) = M \otimes (T_\ell\mu)^{\otimes n}$

$$\det \rho_\ell(\mathrm{Frob}_p^{-1}) = p^{11} \Rightarrow \det \rho_\ell = \varepsilon_\ell^{-11}.$$

Choosing a $G_{\mathbb{Q}}$-invariant $\mathbb{Z}_\ell$-lattice, $\rho_\ell : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{Z}_\ell)$
Reduction $\bar{\rho}_\ell : G_{\mathbb{Q}} \rightarrow GL_2(\mathbb{F}_\ell)$.

Taking now $\ell = 691$, $\tau(p) \equiv 1 + p^{11} \pmod{691}$

$$\Rightarrow \mathrm{tr}\,\bar{\rho}_{691}(\mathrm{Frob}_p^{-1}) = 1 + p^{11} = \mathrm{id}(\mathrm{Frob}_p^{-1}) + \bar{\varepsilon}_{691}^{-11}(\mathrm{Frob}_p^{-1}).$$

Hence $\bar{\rho}_{691}$ is reducible, with composition factors id, $\bar{\varepsilon}_{691}^{-11}$
i.e. $\mathbb{F}_{691}$, $\mathbb{F}_{691}(-11)$.

The choice of $G_{\mathbb{Q}}$-invariant $\mathbb{Z}_{691}$-lattice determines whether we have

$$0 \to \mathbb{F}_{691} \to W \to \mathbb{F}_{691}(-11) \to 0$$

or $$0 \to \mathbb{F}_{691}(-11) \xrightarrow{i} W \xrightarrow{\pi} \mathbb{F}_{691} \to 0,$$

where W is the 2-dimensional $\mathbb{F}_{691}$-vector space on which $G_{\mathbb{Q}}$ acts via $\bar{\rho}_{691}$. Let's choose the latter.

By a theorem of Ribet, $\rho_{691} : G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_{691})$ is irreducible.

It follows (by an argument also due to Ribet) that we may further refine the choice of $\mathbb{Z}_{691}$-lattice so that $W \not\cong \mathbb{F}_{691}(-11) \oplus \mathbb{F}_{691}$,

i.e. W is a non-split extension of $\mathbb{F}_{691}$ by $\mathbb{F}_{691}(-11)$.

We can use this to define a cocycle $c \in Z^1(G_{\mathbb{Q}}, \mathbb{F}_{691}(-11))$ in the following way. Choose $w \in W$ such that $\pi(w) = 1$.

For any $\sigma \in G_{\mathbb{Q}}$, $\pi(\sigma(w) - w) = \pi(\sigma(w)) - \pi(w) = \sigma(\pi(w)) - \pi(w)$
$= \sigma(1) - 1 = 0$.

Hence $\sigma(w) - w \in \ker \pi = \operatorname{im} i$ so $\sigma(w) - w \in \mathbb{F}_{691}(-11)$
(meaning $i(\mathbb{F}_{691}(-11))$).

c is defined by $c(\sigma) = \sigma(w) - w$

Changing c by a coboundary exactly corresponds to adjusting w by an element of $i(\mathbb{F}_{691}(-11))$, so we have a well-defined cohomology class

$[c] \in H^1(G_{\mathbb{Q}}, \mathbb{F}_{691}(-11))$ $\qquad$ W non-split $\Rightarrow [c] \neq 0$.

Moreover, it follows from the fact that ρ_{691} is $\begin{cases} \text{unramified at all } p \neq 691 \\ \text{crystalline at } p = 691 \end{cases}$

that $[c]$, or rather its (non-zero) image in

$H^1(G_{\mathbb{Q}}, \mathbb{Q}_{691}/\mathbb{Z}_{691}(-11))$, satisfies the local restriction conditions

to belong to the Bloch-Kato Selmer group $H^1_f(G_{\mathbb{Q}}, \mathbb{Q}_{691}/\mathbb{Z}_{691}(-11))$.

By a theorem of Bloch and Kato (analogue of BSD)

$$\operatorname{ord}_\ell\left(\frac{\zeta(n)}{(2\pi i)^n}\right) = \frac{\# H^1_f(G_{\mathbb{Q}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(1-n))}{\# H^0(G_{\mathbb{Q}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(1-n)) \# H^0(G_{\mathbb{Q}}, \mathbb{Q}_\ell/\mathbb{Z}_\ell(n))}$$

for positive even n and $\ell > n$.

So letting $n = 12$, $\ell = 691$, the existence of $[c]$ fits with the known fact that $691 \mid \frac{\zeta(12)}{\pi^{12}}$.

Consider once again $E = X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20$

with its rational 5-torsion point $P = (5,5)$.

$$0 \longrightarrow \mathbb{F}_5 \longrightarrow E[5] \longrightarrow \mathbb{F}_5(1) \longrightarrow 0$$

This is not a direct sum, whereas for the 5-isogenous curve $E' = X_1(11) : y^2 + y = x^3 - x^2$

with rational 5-torsion point $(0,0)$, we would have $E'[5] \simeq \mathbb{F}_5 \oplus \mathbb{F}_5(1)$.

The 5-adic Tate modules $T_5[E] = \varprojlim_n E[5^n]$ and $T_5[E']$

are different choices of $G_{\mathbb{Q}}$-invariant $\mathbb{Z}_5$-lattice in a common 2-dimensional $\mathbb{Q}_5$-vector space on which $G_{\mathbb{Q}}$ acts, $V_5 = T_5[E] \otimes_{\mathbb{Z}_5} \mathbb{Q}_5$

Anyway, $0 \to \mathbb{F}_5 \to E[5] \longrightarrow \mathbb{F}_5(1) \to 0$ is non-split, as is its twist

$$0 \to \mathbb{F}_5(-1) \to E[5](-1) \longrightarrow \mathbb{F}_5 \to 0.$$

Arguing as above, we get non-zero $[c] \in H^1(G_{\mathbb{Q}}, \mathbb{F}_5(-1))$.

With $n = 2$, $1 - n = -1$, shouldn't this mean that $5 \mid \frac{\zeta(2)}{(2\pi i)^2}$, whereas in fact $\zeta(2) = \pi^2/6$?

In this case $\rho_5 : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(V_5) \simeq GL_2(\mathbb{Q}_5)$

is unramified at p not for all $p \neq 5$, only for $p \neq 5, 11$, since 11 is a prime of bad reduction.

The image of $[c]$ in $H^1(G_{\mathbb{Q}}, \mathbb{Q}_5/\mathbb{Z}_5(-1))$ satisfies all the Bloch-Kato local conditions <u>except at $p = 11$.</u>

It lies in $H^1_{\{11\}}(G_{\mathbb{Q}}, \mathbb{Q}_5/\mathbb{Z}_5(-1))$. On the LHS of the Bloch-Kato formula, we need to replace $\zeta(2)$ by $\zeta_{\{11\}}(2)$, where $\zeta_{\{11\}}(s) = \prod_{p \neq 11} \frac{1}{(1 - p^{-s})} = (1 - 11^{-s})\zeta(s)$

Since $1 - 11^{-2} = -\frac{1}{11^2}(11^2 - 1)$ and $11 \equiv 1 \pmod 5$,

we see that indeed $5 \mid \zeta_{\{11\}}(2)/\pi^2$

Consider once again $f, g \in S_2(\Gamma_0(1058))$ $\qquad$ $(1058 = 2 \cdot 23^2)$

$E_f : y^2 + xy + y = x^3 + 2$ $\qquad$, $\deg \pi_f = 2^4 \cdot 5$, $E_f(\mathbb{Q}) \simeq \mathbb{Z}^2$

$E_g : y^2 + xy = x^3 - x^2 - 332311x - 73733731$, $\deg \pi_g = 2^3 3 \cdot 5 \cdot 7 \cdot 23$, $E_g(\mathbb{Q}) = \{O\}$.

$a_n(f) \equiv a_n(g) \pmod 5$, $E_f[5] = E_g[5]$ inside $J_0(1058)$.

$\rho_{f,5}, \rho_{g,5} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{Z}_5)$

$\bar{\rho}_{f,5}, \bar{\rho}_{g,5} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_5)$

Since $E_f[5] = E_g[5]$, may choose bases so that $\bar{\rho}_{f,5} = \bar{\rho}_{g,5}$.

Given $\sigma \in G_{\mathbb{Q}}$, $\rho_{g,5}(\sigma) \equiv (I + 5c(\sigma))\rho_{f,5}(\sigma) \pmod{5^2}$

for some $c(\sigma) \in M_2(\mathbb{F}_5)$.

$\det \rho_{g,5}(\sigma) = \det \rho_{f,5}(\sigma) \; (= \varepsilon_5(\sigma)) \Rightarrow tr(c(\sigma)) = 0$.

Given $\sigma, \tau \in G_{\mathbb{Q}}$, $\rho_{g,5}(\sigma\tau) = \rho_{g,5}(\sigma)\rho_{g,5}(\tau)$

$\equiv (I + 5c(\sigma))\rho_{f,5}(\sigma)(I + 5c(\tau))\rho_{f,5}(\tau) \pmod{5^2}$

$\equiv (I + 5[c(\sigma) + \rho_{f,5}(\sigma)c(\tau)\rho_{f,5}(\sigma)^{-1}])\rho_{f,5}(\sigma)\rho_{f,5}(\tau)$

$\equiv (I + 5[c(\sigma) + \rho_{f,5}(\sigma)c(\tau)\rho_{f,5}(\sigma)^{-1}])\rho_{f,5}(\sigma\tau) \pmod{5^2}$

But $\rho_{g,5}(\sigma\tau) \equiv (I + 5c(\sigma\tau))\rho_{f,5}(\sigma\tau) \pmod{5^2}$.

Hence $c(\sigma\tau) = c(\sigma) + \rho_{f,5}(\sigma)c(\tau)\rho_{f,5}(\sigma)^{-1}$

This is $c(\sigma\tau) = c(\sigma) + \sigma(c(\tau))$, where the action of $G_{\mathbb{Q}}$ on $M_2(\mathbb{F}_5)^{tr=0}$ is via the adjoint action

$ad^0\bar{\rho}_{f,5} : G_{\mathbb{Q}} \longrightarrow Aut_{\mathbb{F}_5}(M_2(\mathbb{F}_5)^{tr=0})$

We write $c \in Z^1(G_{\mathbb{Q}}, ad^0\bar{\rho}_{f,5})$.

$a_3(f) = -2 \not\equiv 3 = a_3(g) \pmod{25} \Rightarrow c \neq 0$, in fact $[c] \neq 0$ in $H^1(G_{\mathbb{Q}}, ad^0\bar{\rho}_{f,5})$.

Moreover (with slight abuse of notation)

$[c] \in H^1_{\{2,23\}}(G_{\mathbb{Q}}, ad^0\bar{\rho}_{f,5})$

There is an adjoint L-function $L(\mathrm{ad}^0(f), s)$.
For a good prime $p \neq 2, 23$, the Euler factor at p is (choosing any $\ell \neq p$)

$$\det(I - \mathrm{ad}^0 \rho_{f,\ell}(\mathrm{Frob}_p^{-1})\, p^{-s})^{-1}$$

$$= \left[(1-p^{-s})\left(1-\frac{\alpha_p}{\beta_p} p^{-s}\right)\left(1-\frac{\beta_p}{\alpha_p} p^{-s}\right)\right]^{-1}$$

where $[(1-\alpha_p p^{-s})(1-\beta_p p^{-s})]^{-1}$ is the Euler factor at p in $L_f(s) = L_{E_f}(s)$.

[Since $\alpha_p \beta_p = p$,

$$(1-p^{-s})\left(1-\frac{\alpha_p}{\beta_p} p^{-s}\right)\left(1-\frac{\beta_p}{\alpha_p} p^{-s}\right) = (1-\alpha_p\beta_p p^{-(1+s)})(1-\alpha_p^2 p^{-(1+s)})(1-\beta_p^2 p^{-(1+s)})$$

and $L(\mathrm{ad}^0(f), s) = L(\mathrm{Sym}^2 E_f, 1+s)$.]

$L(\mathrm{ad}^0(f), s)$ has an analytic continuation to $\mathbb{C}$ and satisfies a functional equation for $s \leftrightarrow 1-s$.

Non-zero $[c] \in H^1_{\{2,23\}}(G_{\mathbb{Q}}, \mathrm{ad}^0 \bar{\rho}_{f,5})$ implies, by Bloch-Kato conjecture (theorem of Diamond, Flach & Guo in this case) that we should see a factor 5 in $\frac{L(\mathrm{ad}^0(f),1)}{\Omega}$ for some carefully chosen Deligne period Ω. (or maybe $\frac{L_{\{2,23\}}(\mathrm{ad}^0(f),1)}{\Omega}$)

In fact, $\Omega = -2(2\pi i)\,\Omega^+_{E_f}\,\Omega^-_{E_f}$

By a theorem of Rankin and Shimura,

$$L(\mathrm{ad}^0(f), 1) = \frac{4^2 \pi^3 \langle f, f\rangle}{1058\, \phi(1058)}$$

Hence

$$\frac{L(\mathrm{ad}^0(f),1)}{\Omega} = \frac{4\pi^2}{1058\,\phi(1058)} \frac{\langle f, f\rangle}{-i\,\Omega^+\Omega^-} = \frac{\frac{1}{2}\deg \pi_f}{1058\,\phi(1058)}$$

so $5 \mid \deg \pi_f \Rightarrow 5 \mid \frac{L(\mathrm{ad}^0(f),1)}{\Omega}$, as expected.

Next we shall look at something similar, but for higher weight.

Given a character $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, define a subspace $S_k(\Gamma_0(N), \chi) \subseteq S_k(\Gamma_1(N))$ by the condition

$$f\left(\frac{a\tau+b}{c\tau+d}\right) = \chi(d)(c\tau+d)^k f(\tau) \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Special case $N = D$, the discriminant of a real quadratic field $F = \mathbb{Q}(\sqrt{D})$, $\chi = \chi_D = \left(\frac{D}{\cdot}\right)$ the associated quadratic character.

Let $f \in S_k(\Gamma_0(D), \chi_D)$ be a Hecke eigenform.

Remarks (i) $D > 0 \Rightarrow \chi_D(-1) = 1$, i.e. χ_D is an even character.
Letting $\gamma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \Gamma_0(D)$, $f(\tau) = \chi(-1)(-1)^k f(\tau) \Rightarrow k$ is even

(ii) χ_D is a primitive character $\Rightarrow f$ is a newform, let's say normalised.

(iii) The T_n for $(n,N)=1$ are not quite self-adjoint, but still commute with their adjoints. For prime $q \nmid D$,

$$\langle T_q f, f \rangle = \chi_D(q) \langle f, T_q f \rangle$$

$$\Rightarrow a_q(f) \langle f, f \rangle = \chi_D(q) \overline{a_q(f)} \langle f, f \rangle$$

$$\Rightarrow a_q(f) \text{ is } \begin{cases} \text{real} & \text{if } \chi_D(q) = 1 \quad (\text{i.e. } q \text{ splits in } F) \\ \text{purely imaginary} & \text{if } \chi_D(q) = -1 \quad (\text{i.e. } q \text{ is inert in } F). \end{cases}$$

Examples $S_8(\Gamma_0(5), \chi_5)$ is spanned by a complex conjugate pair of Hecke eigenforms

$$f = q + 2\sqrt{-29}\,q^2 + 6\sqrt{-29}\,q^3 + 12q^4 + (75 - 50\sqrt{-29})q^5 - 348q^6 - 78\sqrt{-29}\,q^7 + \dots$$

$$f^c = q - 2\sqrt{-29}\,q^2 - 6\sqrt{-29}\,q^3 + 12q^4 + (75 + 50\sqrt{-29})q^5 - 348q^6 + 78\sqrt{-29}\,q^7 + \dots$$

$S_6(\Gamma_0(5), \chi_5)$ is spanned by a complex conjugate pair of Hecke eigenforms

$$g = q - 2\sqrt{-11}\,q^2 + 6\sqrt{-11}\,q^3 - 12q^4 + (-45 - 10\sqrt{-11})q^5 + 132q^6 + 18\sqrt{-11}\,q^7 + \dots$$

$$g^c = q + 2\sqrt{-11}\,q^2 - 6\sqrt{-11}\,q^3 - 12q^4 + (-45 + 10\sqrt{-11})q^5 + 132q^6 - 18\sqrt{-11}\,q^7 + \dots$$

$S_4(\Gamma_0(8), \chi_8)$ is spanned by

$$h = q + (-1 - \sqrt{-7})q^2 + 2\sqrt{-7}\,q^3 + (-6 + 2\sqrt{-7})q^4 - 4\sqrt{-7}\,q^5 + (14 - 2\sqrt{-7})q^6 - 8q^7 + \dots \text{ and } h^c$$

$S_{14}(\Gamma_0(8), \chi_8)$ is spanned by

$$r = q + (-56 - 8\sqrt{-79})q^2 + 258\sqrt{-79}\,q^3 + (-1920 + 896\sqrt{-79})q^4 - 2540\sqrt{-79}\,q^5 + (163056 - 14448\sqrt{-79})q^6 - 175832q^7 + \dots,$$
and r^c

Observe the following congruences:

$$a_n(f) \equiv a_n(f^c) \pmod{\sqrt{-29}} \quad \forall n \geq 1.$$

$$a_n(g) \equiv a_n(g^c) \pmod{\sqrt{-11}} \quad \forall n \geq 1.$$

$$a_n(h) \equiv a_n(h^c) \pmod{\sqrt{-7}} \quad \forall n \geq 1.$$

$$a_n(r) \equiv a_n(r^c) \pmod{\sqrt{-79}} \quad \forall n \geq 1.$$

It follows that $\sqrt{-29} \mid m(f)$, a "cohomological congruence ideal", analogous to the modular degree.

$\sqrt{-11} \mid m(g)$, $\sqrt{-7} \mid m(h)$, $\sqrt{-79} \mid m(r)$.

By a theorem of Hida

$$\langle f, f \rangle = i^{k-1} \Omega^+ \Omega^- \, m(f) \quad \text{(up to divisors of } D(k!))$$

where Ω^+, Ω^- are certain "canonical periods".

The natural Deligne period for $L(ad^\circ(f), 1)$ is

$$\Omega = 2(2\pi i)^{k+1} \Omega^+ \Omega^-,$$

and by the theorem of Rankin and Shimura

$$L(ad^\circ(f), 1) = \frac{4^k \pi^{k+1} \langle f, f \rangle}{(k-1)! \, D^2}$$

Hence $\dfrac{L(ad^\circ(f), 1)}{\Omega}$ is like $\dfrac{m(f)}{D^2}$

$\dfrac{L_{\{5\}}(ad^\circ(f), 1)}{\Omega}$ is like $\dfrac{(1-5^{-1})\, m(f)}{5^2}$

To account for the $q \mid m(f)$ where $q = \sqrt{-29}$, Bloch-Kato conjecture (theorem of Diamond, Flach & Guo) says there is a non-zero element in $H^1_{\{5\}}(G_{\mathbb{Q}}, ad^\circ \bar{\rho}_{f,q})$

We can construct this using $\bar{\rho}_{f,q} \simeq \bar{\rho}_{f^c,q}$ just like we did for $E_f[5] = E_g[5]$ (different f, g) earlier.

The right-of-centre "critical" values for $L(\mathrm{ad}^0(f), s)$ are at $s = 1, 3, 5, \ldots, k-1$. The Deligne period is $\Omega_s := (2\pi i)^{2(s-1)}\Omega$.

For $s > 1$, a theorem of Katsurada allows the critical values to be computed.

It says something a bit like

$$G_s(z) = \frac{L_{\{S\}}(\mathrm{ad}^0(f), s)}{\pi^{k+2s-1}\langle f, f\rangle} f(z) + \frac{L_{\{S\}}(\mathrm{ad}^0(f^c), s)}{\pi^{k+2s-1}\langle f^c, f^c\rangle} f^c(z)$$

in our case where $S_k(\Gamma_0(D), \chi_D) = \langle f, f^c\rangle_{\mathbb{C}}$.

$G_s(z)$ is a certain cusp form obtained from a genus-2 Siegel Eisenstein series by applying differential operators and restriction from $\mathfrak{h}_2$ to $\mathfrak{h}_1 \times \mathfrak{h}_1$.

Looking at the coefficients of some q^{n_1}, q^{n_2} gives linear equations

$$\begin{cases} a_{n_1}(G_s) = a_{n_1}(f)\, x(f) + a_{n_1}(f^c)\, x(f^c) \\ a_{n_2}(G_s) = a_{n_2}(f)\, x(f) + a_{n_2}(f^c)\, x(f^c) \end{cases}$$

where $x(f) = \frac{L_{\{S\}}(\mathrm{ad}^0(f), s)}{\pi^{k+2s-1}\langle f, f\rangle}$, $x(f^c) = \frac{L_{\{S\}}(\mathrm{ad}^0(f^c), s)}{\pi^{k+2s-1}\langle f^c, f^c\rangle}$

Since $a_n(f) \equiv a_n(f^c) \pmod{\mathfrak{q}}$, the coefficient matrix

$$\begin{bmatrix} a_{n_1}(f) & a_{n_1}(f^c) \\ a_{n_2}(f) & a_{n_2}(f^c) \end{bmatrix}$$ is singular $(\mathrm{mod}\ \mathfrak{q})$, so $\mathfrak{q} \mid \det\begin{bmatrix} a_{n_1}(f) & a_{n_1}(f^c) \\ a_{n_2}(f) & a_{n_2}(f^c) \end{bmatrix}$

and one would expect Cramer's rule to put $\mathfrak{q}$ in the denominators of the solutions $x(f)$, $x(f^c)$, thus avoiding $\mathfrak{q} \mid \frac{L_{\{S\}}(\mathrm{ad}^0(f), s)}{\Omega_s}$ despite $\mathfrak{q} \mid \frac{\langle f, f\rangle}{\Omega}$.

This is what would typically happen where there is a congruence between two newforms (same weight, level, character), but in this special situation of a congruence between complex conjugates, $x(f)$ and $x(f^c)$ are actually the same.

[Recall that for prime $q \nmid D$, $a_q(f) = \chi_D(q)\overline{a_q(f)} = \chi_D(q)\, a_q(f^c)$.
Since $a_q(f) = \mathrm{tr}\, \rho_{f,\lambda}(\mathrm{Frob}_q^{-1})$ etc., it follows that

$$\rho_{f,\lambda} \simeq \rho_{f^c,\lambda} \otimes \chi_D, \text{ hence } \mathrm{ad}^0(\rho_{f,\lambda}) \simeq \mathrm{ad}^0(\rho_{f^c,\lambda})$$]

So, taking $n_1=1$, we actually have a single equation in one unknown:

$$2x(f) = a_1(G_s)$$

The RHS is complicated, but one can show it is integral at q.
So in fact $q \mid \frac{L_{\{5\}}(ad^0(f),s)}{\Omega_s}$ not just for $s=1$, but

for all $s=1,3,5,\dots,k-1$.

In summary (neglecting powers of π)

each $L_{\{5\}}(ad^0(f),s)$ is a q-integral multiple of $\langle f,f\rangle$

(Rankin-Shimura for $s=1$, Katsurada for $s>1$).

But $q \mid \frac{\langle f,f\rangle}{\Omega_s}$ as a consequence of $a_n(f) \equiv a_n(f^c) \pmod{q}$

so $q \mid \frac{L_{\{5\}}(ad^0(f),s)}{\Omega_s}$ for $s=1,3,\dots,k-1$.

For $s=1$, $1-s=0$, we already constructed a non-zero element in $H^1_{\{5\}}(G_{\mathbb{Q}}, ad^0(\overline{\rho}_{f,q}))$.

Bloch-Kato conjecture $\Rightarrow$ for the $s>1$ we should also have non-zero elements in $H^1_{\{5\}}(G_{\mathbb{Q}}, ad^0(\overline{\rho}_{f,q})(1-s))$.

How can we construct these?

We will need some more congruences, involving Hilbert modular forms.

Newform $f \in S_k(\Gamma_0(D), \chi_D)$ $F = \mathbb{Q}(\sqrt{D})$ real quadratic field.

$a_n(f) \equiv a_n(f^c) \pmod{q}$ $\forall n \geq 1$

For $s = 3, 5, \ldots, k-1$ we want a non-zero element of
$H^1_{\{p|D\}}(G_{\mathbb{Q}}, ad^0(\bar{\rho}_{f,q})(1-s))$, in accord with the Bloch-Kato conjecture,

since $q \mid m(f) \Rightarrow q \mid \frac{L_{\{p|D\}}(ad^0(f), s)}{\Omega_s}$

We need a closer look at $\rho_{f,q}$ and $\bar{\rho}_{f,q}$.

$\rho_{f,q} : G_{\mathbb{Q}} \longrightarrow GL_2(K_q)$ (e.g. $K = \mathbb{Q}(\sqrt{-29})$, $q = (\sqrt{-29})$)

is irreducible, and is unramified at all primes $p \nmid qD$
(i.e. $\rho_{f,q}|_{I_p}$ is trivial for such p).

At $p \mid D$ it is known that $\rho_{f,q}|_{I_p} \simeq id. \oplus \chi_D$
where $\chi_D : (\mathbb{Z}/D\mathbb{Z})^\times \to \{\pm 1\}$
is thought of as a character of $G_{\mathbb{Q}}$, using $(\mathbb{Z}/D\mathbb{Z})^\times \simeq Gal(\mathbb{Q}(\mu_D)/\mathbb{Q})$

In particular, if $\mathfrak{P} | p$ in F then $\rho_{f,q}|_{I_{\mathfrak{P}}}$ is trivial,
i.e. $\rho_{f,q}|_{G_F}$ is unramified at all primes $\mathfrak{P} | D$.
It can be ramified at most at primes dividing q.
The same applies to $\bar{\rho}_{f,q}|_{G_F}$. *

Recall that $\rho_{f,q} \simeq \rho_{f^c,q} \otimes \chi_D$

Substituting $\bar{\rho}_{f^c,q} \simeq \bar{\rho}_{f,q}$, we get

$$\bar{\rho}_{f,q} \simeq \bar{\rho}_{f,q} \otimes \chi_D \qquad **$$

One can check in our examples that
(i) $\bar{\rho}_{f,q}$ is absolutely irreducible
(ii) f is <u>ordinary</u> at q: $q \nmid a_q(f)$

Using also * and **, it follows that $(q) = \mathfrak{Q}\mathfrak{Q}^\sigma$ splits in F
(say $Gal(F/\mathbb{Q}) = \langle\sigma\rangle$)

and that $\bar{\rho}_{f,q} : G_{\mathbb{Q}} \longrightarrow GL_2(\mathbb{F}_q) \subset GL_2(\bar{\mathbb{F}}_q)$

is induced from a character $\psi : G_F \to \bar{\mathbb{F}}_q^{\times}$
ramified only at Q (among finite primes)

Equally it is induced from $\psi^{\sigma} : G_F \to \bar{\mathbb{F}}_q^{\times}$
ramified only at Q^{σ} (among finite primes),

where $\psi^{\sigma}(g) := \psi(\sigma g \sigma^{-1}) \quad \forall g \in G_F$.

$\bar{\rho}_{f,q}|_{G_F} \simeq \psi \oplus \psi^{\sigma}$.

Using $\det \bar{\rho}_{f,q} \simeq \chi_D \bar{\varepsilon}_q^{\,1-k} \simeq \mathbb{F}_q(1-k) \otimes \chi_D$,

in fact the finite parts of the conductors of ψ and ψ^{σ} are precisely Q and Q^{σ}, respectively, and we can say precisely what these characters must be.

For simplicity, assume from now on that O_F has narrow class number one — every ideal is generated by a totally positive element. This is certainly true for $F = \mathbb{Q}(\sqrt{5})$ and $F = \mathbb{Q}(\sqrt{2})$.

As an abstract field, $F = \mathbb{Q}(\alpha)$ with $\alpha^2 = D$.
Two real embeddings $\theta_1, \theta_2 : F \hookrightarrow \mathbb{R}$
$\theta_1 : \alpha \mapsto \sqrt{D}$, $\quad \theta_2 : \alpha \mapsto -\sqrt{D}$.
Associated valuations $|x|_{\infty_1} = |\theta_1(x)|$, $\quad |x|_{\infty_2} = |\theta_2(x)|$.

Unit group $O_F^{\times}$ is generated by -1 and a fundamental unit u.

$\psi : G_F \to \bar{\mathbb{F}}_q^{\times}$ factors through $\mathrm{Gal}(H_{Q\infty_1}/F)$, where

$H_{Q\infty_1}$ is the ray class field of conductor $Q\infty_1$.

$\mathrm{Gal}(H_{Q\infty_1}/F) \simeq C_{Q\infty_1}$, a generalised ideal class group.

$$C_{Q\infty_1} \simeq I_{Q\infty_1} / P_{Q\infty_1}, \text{ where}$$

$I_{Q\infty_1}$ is the group of fractional ideals of F coprime to Q

$P_{Q\infty_1}$ is the subgroup of principal ideals (x) with
$x \equiv 1 \pmod{Q}$, ~~$\theta_1(x), \theta_2(x) > 0$ (totally positive)~~
$\theta_1(x) > 0$.

We define $\psi : C_{Q\infty_1} \longrightarrow \mathbb{F}_q^\times$ (hence : $G_F \longrightarrow \mathbb{F}_q^\times$)

in the following way, to make $\psi\psi^\sigma = \varepsilon_q^{1-k} \circ \mathrm{Norm}_{F/\mathbb{Q}}$.

Given $\mathfrak{a} \in I_{Q\infty_1}$, $\exists\ a \in F^\times$, $\mathrm{ord}_Q(a) = 0$ such that $\mathfrak{a} = (a)$ and $\theta_1(a), \theta_2(a) > 0$ (a is totally positive).

This is because $\mathcal{O}_F$ has narrow class number 1, i.e. $C_{\infty_1\infty_2}$ is trivial.

Define $\psi : I_{Q\infty_1} \longrightarrow \mathbb{F}_q^\times$ by

$$\psi(\mathfrak{a}) = \bar{a}^{1-k}$$, where $\bar{a}$ is the image of a in $\mathcal{O}_F/Q \simeq \mathbb{F}_q$.

For this to be well-defined independent of the choice of a, we must have $(u^2)^{1-k} \equiv 1 \pmod{Q}$, ⊛

since $u^2 a$ is also a totally positive generator of $\mathfrak{a}$.

Note that u is not totally positive. It is a consequence of $\mathcal{O}_F$ having narrow class number 1 that $\theta_1(u)$ and $\theta_2(u)$ are opposite in sign.

By ⊛, $u^{k-1} \equiv \pm 1 \pmod{Q}$.

Replacing u by $-u$ if necessary (k is even) we may assume $u^{k-1} \equiv 1 \pmod{Q}$,

and replacing u by u^σ if necessary (and Q by Q^σ) we may assume $\theta_1(u) > 0$, $\theta_2(u) < 0$.

Now if $(x) \in P_{Q\infty_1}$ with $x \equiv 1 \pmod{Q}$, $\theta_1(x) > 0$

there are two possibilities.

(i) If $\theta_2(x) > 0$ then $\psi((x)) = \bar{x}^{1-k} = 1$ since $x \equiv 1 \pmod{Q}$.

(ii) If $\theta_2(x) < 0$ then ux is a totally positive generator of (x), so $\psi((x)) = \overline{ux}^{1-k} = 1$ since $u^{k-1} \equiv x \equiv 1 \pmod{Q}$.

We have shown that $\psi : I_{Q\infty_1} \longrightarrow \mathbb{F}_q^\times$ factors through $I_{Q\infty_1}/P_{Q\infty_1} \simeq C_{Q\infty_1} \simeq \mathrm{Gal}(H_{Q\infty_1}/F)$, as desired.

Example: $F = \mathbb{Q}(\alpha)$, $\alpha^2 = 5$ $\quad u = \frac{1+\alpha}{2}$, $k = 8$, $q = 29$.

$\frac{1+\sqrt{5}}{2} > 0$, $\frac{1-\sqrt{5}}{2} < 0$

$x^2 - 5 \equiv (x+11)(x-11) \pmod{29}$

$Q = (29, \alpha+11)$, $Q^\sigma = (29, \alpha - 11)$

$\alpha \equiv -11 \pmod{Q}$

$u \equiv -5 \pmod{Q}$

$u^7 \equiv 1 \pmod{Q}$.

Suppose that $(p) = \mathfrak{p}\mathfrak{p}^\sigma$ splits in F, and let $\mathfrak{p} = (a)$ with a totally positive.

We have $\mathrm{Frob}_p = \mathrm{Frob}_{\mathfrak{p}} \in G_F \subseteq G_{\mathbb{Q}}$.

Recall that $\bar{\rho}_{f,q}|_{G_F} \simeq \psi \oplus \psi^\sigma$.

Evaluating at $\mathrm{Frob}_{\mathfrak{p}}^{-1}$ and taking the trace, we should find

$$a_p(f) \equiv a^{k-1} + (a^\sigma)^{k-1} \pmod{\mathcal{Q}}.$$

p	a	$a \pmod{\mathcal{Q}}$	$a^\sigma \pmod{\mathcal{Q}}$	$a^7 \pmod{\mathcal{Q}}$	$(a^\sigma)^7 \pmod{\mathcal{Q}}$	$a_p(f)$
11	$4+\alpha$	-7	15	-1	17	$-6828 \equiv 16$
19	$12+5\alpha$	15	9	17	-1	$6860 \equiv 16$
31	$6+\alpha$	-5	17	1	12	$82112 \equiv 13$
29	$7+2\alpha$	14	0	12	0	$25590 \equiv 12$

Another example: $F = \mathbb{Q}(\alpha)$, $\alpha^2 = 5$, $u = \frac{1+\alpha}{2}$, $k = 6$, $q = 11$

$x^2 - 5 \equiv (x+4)(x-4) \pmod{11}$

$\mathcal{Q} = (11, \alpha+4)$, $\mathcal{Q}^\sigma = (11, \alpha-4)$

$\alpha \equiv -4 \pmod{\mathcal{Q}}$
$u \equiv 4 \pmod{\mathcal{Q}}$
$u^5 \equiv 1 \pmod{\mathcal{Q}}$

p	a	$a \pmod{\mathcal{Q}}$	$a^\sigma \pmod{\mathcal{Q}}$	$a^5 \pmod{\mathcal{Q}}$	$(a^\sigma)^5 \pmod{\mathcal{Q}}$	$a_p(g)$
11	$4+\alpha$	0	8	0	-1	$252 \equiv -1$
19	$12+5\alpha$	3	-1	1	-1	$-220 \equiv 0$
29	$7+2\alpha$	-1	4	-1	1	$6930 \equiv 0$
31	$6+\alpha$	2	-1	-1	-1	$6752 \equiv -2$

This is consistent with $a_p(g) \equiv a^{k-1} + (a^\sigma)^{k-1} \pmod{\mathcal{Q}}$

and $\bar{\rho}_{g,q}|_{G_F} \simeq \psi \oplus \psi^\sigma$

$$\bar{\rho}_{g,q} \simeq \mathrm{Ind}_{G_F}^{G_{\mathbb{Q}}} \psi \simeq \mathrm{Ind}_{G_F}^{G_{\mathbb{Q}}} \psi^\sigma.$$

There exists a Hilbert modular form $\hat{f} \in S_{[k,k]}(SL_2(\mathcal{O}_F))$

the <u>base change</u> of f.

$\hat{f} : \mathfrak{h} \times \mathfrak{h} \longrightarrow \mathbb{C}$ holomorphic,

$$\hat{f}\left(\left(\frac{a_1\tau_1 + b_1}{c_1\tau_1 + d_1}, \frac{a_2\tau_2 + b_2}{c_2\tau_2 + d_2}\right)\right) = (c_1\tau_1 + d_1)^k (c_2\tau_2 + d_2)^k \hat{f}(\tau_1, \tau_2)$$

$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathcal{O}_F)$, where $a_1 = \theta_1(a)$, $a_2 = \theta_2(a)$, etc.

$\hat{f}$ vanishes at the cusps.

$\hat{f}$ is an eigenform for Hecke operators T_β (β prime ideals of $\mathcal{O}_F$)

$$T_\beta(\hat{f}) = a_\beta(\hat{f})\,\hat{f}$$

There is an irreducible, continuous $\rho_{\hat{f},q} : G_F \longrightarrow GL_2(K_q)$

unramified at $\beta \nmid qD$

$$\mathrm{tr}\left(\rho_{\hat{f},q}(\mathrm{Frob}_\beta^{-1})\right) = a_\beta(\hat{f})$$

To say $\hat{f}$ is the base-change of f is simply to say that

$$\rho_{\hat{f},q} = \rho_{f,q}\big|_{G_F}.$$

Put another way,
$$a_\beta(\hat{f}) = \begin{cases} a_p(f) & (p) = \beta\beta^\sigma \text{ split;} \\ a_p(f)^2 - 2p^{k-1} & (p) = \beta \text{ inert.} \end{cases}$$

Note that $\overline{\rho}_{\hat{f},q} \simeq \psi \oplus \psi^\sigma$

For $s = 3, 5, \ldots, k-1$, what we actually need is a Hecke eigenform $F_s \in S_{[k+s-1,\,k+1-s]}(SL_2(\mathcal{O}_F))$

[of non-parallel weight, $F_s\left(\left(\frac{a_1\tau_1+b_1}{c_1\tau_1+d_1}, \frac{a_2\tau_2+b_2}{c_2\tau_2+d_2}\right)\right) = (c_1\tau_1+d_1)^{k+s-1}(c_2\tau_2+d_2)^{k+1-s} F_s(\tau_1,\tau_2)$
$\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathcal{O}_F)$, $(\tau_1,\tau_2) \in \mathfrak{h}\times\mathfrak{h}$]

such that $\overline{\rho}^{\,ss}_{F_s,q} \simeq (\psi \otimes \overline{\varepsilon}_q^{\,1-s}) \oplus \psi^\sigma$

For $s=1$, $\hat{f}$ plays this rôle, but it appears that F_s exists in general.

For $(p) = \beta\beta^\sigma$ split, $\beta = (a)$, a totally positive, we would have $a_\beta(F_s) \equiv (a^\sigma)^{k-1} + a^{k-1}p^{s-1} \pmod{Q}$

Example: $F = \mathbb{Q}(\sqrt{5})$, $k=8$, $q=29$

p	a	$(a^\sigma)^7 \pmod{Q}$	$a^7 \pmod{Q}$	$(a^\sigma)^7 + a^7 p^{s-1} \pmod{Q}$ for $s=3$	$s=5$	$s=7$
11	$4+\alpha$	17	-1	12	21	8
19	$12+5\alpha$	-1	17	17	1	25
29	$7+2\alpha$	0	12	0	0	0
31	$6+\alpha$	12	1	16	-1	18

$\wp$	$F_3 \in S_{[10,6]}(SL_2(\mathcal{O}_F))$ $a_\wp(F_3)$	$F_5 \in S_{[12,4]}(SL_2(\mathcal{O}_F))$ $a_\wp(F_5)$	$F_7 \in S_{[14,2]}(SL_2(\mathcal{O}_F))$ $a_\wp(F_7)$
11	$1092 - 22680\alpha \equiv 12$	$-397788 + 156240\alpha \equiv 21$	$4303332 - 1580040\alpha \equiv 8$
19	$-66820 + 214200\alpha \equiv 17$	$10814300 \mp 1386000\alpha \equiv 1$	$166703900 + 52353000\alpha \equiv 25$
29	$1085070 + 982800\alpha \equiv 0$	$-18469050 - 14364000\alpha \equiv 0$	$-3830443650 + 128142000\alpha \equiv 0$
31	$-315328 + 2227680\alpha \equiv 16$	$46411232 + 20784960\alpha \equiv -1$	$-100191808 - 947691360\alpha \equiv 18$

Assuming that F_5 exists, here is what we can do with it.

We have $\rho_{F_5,q} : G_F \longrightarrow GL_2(K_q)$ (irreducible)

Also $\rho^{\sigma}_{F_5,q}$ defined by $\rho^{\sigma}_{F_5,q}(g) = \rho_{F_5,q}(\sigma g \sigma^{-1})$ $\forall g \in G_F$.

Let $\rho := \mathrm{Ind}_{G_F}^{G_\mathbb{Q}} \rho_{F_5,q} : G_\mathbb{Q} \longrightarrow GL_4(K_q)$.

Since $\rho^{\sigma}_{F_5,q} \not\simeq \rho_{F_5,q}$, ρ is irreducible.

But $\bar{\rho}$ is reducible. We can find its composition factors as follows:

$$\bar{\rho}^{ss} = \mathrm{Ind}_{G_F}^{G_\mathbb{Q}} \bar{\rho}^{ss}_{F_5,q} \simeq \mathrm{Ind}_{G_F}^{G_\mathbb{Q}} [(\psi \otimes \bar{\varepsilon}_q^{1-s}) \oplus \psi^{\sigma}]$$
$$\simeq \mathrm{Ind}_{G_F}^{G_\mathbb{Q}} (\psi \otimes \bar{\varepsilon}_q^{1-s}) \oplus \mathrm{Ind}_{G_F}^{G_\mathbb{Q}} (\psi^{\sigma})$$
$$\simeq \mathrm{Ind}_{G_F}^{G_\mathbb{Q}} (\psi) \otimes \bar{\varepsilon}_q^{1-s} \oplus \mathrm{Ind}_{G_F}^{G_\mathbb{Q}} (\psi^{\sigma})$$
$$\simeq \bar{\rho}_{f,q} \otimes \bar{\varepsilon}_q^{1-s} \oplus \bar{\rho}_{f,q}$$

Since ρ is irreducible, a Ribet-style argument shows that we can choose the $G_\mathbb{Q}$-invariant $\mathcal{O}_q$-lattice for ρ in such a way that we have a <u>non-split</u> extension of $\mathbb{F}_q[G_\mathbb{Q}]$-modules

$$0 \longrightarrow \bar{\rho}_{f,q} \otimes \bar{\varepsilon}_q^{1-s} \longrightarrow \bar{\rho} \longrightarrow \bar{\rho}_{f,q} \longrightarrow 0$$

i.e. $$0 \longrightarrow \bar{\rho}_{f,q}(1-s) \xrightarrow{i} \bar{\rho} \underset{\lambda}{\overset{\pi}{\rightleftarrows}} \bar{\rho}_{f,q} \longrightarrow 0$$

i and π are maps of $\mathbb{F}_q[G_\mathbb{Q}]$-modules

Choose a section λ, an $\mathbb{F}_q$-linear map such that $\pi \circ \lambda = id$.
Since the extension is non-split, λ is not an $\mathbb{F}_q[G_\mathbb{Q}]$-module map.

Now define $c : G_{\mathbb{Q}} \longrightarrow \mathrm{Hom}_{\mathbb{F}_q}(\tilde{\rho}_{f,q}, \bar{\rho}_{f,q}(1-s))$

by $c(g)(w) := g\lambda(g^{-1}w) - \lambda(w) \qquad \forall g \in G_{\mathbb{Q}}$.

Strictly speaking it is $i^{-1}(g\lambda(g^{-1}w) - \lambda(w))$

This makes sense, since

$$\pi(g\lambda(g^{-1}w) - \lambda(w)) = g(\pi\circ\lambda)(g^{-1}w) - (\pi\circ\lambda)w$$

(since π is an $\mathbb{F}_q[G_{\mathbb{Q}}]$-module map)

$$= g(g^{-1}w) - w$$

(since $\pi\circ\lambda = id.$)

$$= w - w = 0$$

and $\ker(\pi) = \mathrm{im}(i)$.

Given $g, h \in G_{\mathbb{Q}}$,

$$c(gh)(w) = gh\lambda((gh)^{-1}w) - \lambda(w)$$
$$= gh\lambda(h^{-1}g^{-1}w) - g\lambda(g^{-1}w) + g\lambda(g^{-1}w) - \lambda(w)$$
$$= g\,c(h)(g^{-1}w) + c(g)(w)$$

Hence c is a cocycle with values in $(\mathrm{ad}\,\bar{\rho}_{f,q})(1-s)$

A different choice of section λ only changes c by a coboundary.

So we have $[c] \in H^1(G_{\mathbb{Q}}, (\mathrm{ad}\,\bar{\rho}_{f,q})(1-s))$

Non-split extension $\Rightarrow [c] \neq 0$.

Special form of $\rho = \mathrm{Ind}_{G_F}^{G_{\mathbb{Q}}} \rho_{F_s,q} \Rightarrow [c] \in H^1(G_{\mathbb{Q}}, (\mathrm{ad}^0\bar{\rho}_{f,q})(1-s))$

ρ unramified at $p \nmid D$, crystalline at q

$\Rightarrow [c] \in H^1_{\{p|D\}}(G_{\mathbb{Q}}, \mathrm{ad}^0(\bar{\rho}_{f,q})(1-s))$.

This is what we wanted.

Further example: $F = \mathbb{Q}(\sqrt{5}) = \mathbb{Q}(\alpha)$, $\alpha^2 = 5$, $k = 6$, $q = 11$

$Q = (11, \alpha + 4)$

$\alpha \equiv -4 \pmod{Q}$

p	a	$(a^\sigma)^5 \pmod{Q}$	$a^5 \pmod{Q}$	$(a^\sigma)^5 + a^5 p^{s-1} \pmod{Q}$ for $s=3$	$s=5$
11	$4+\alpha$	-1	0	-1	-1
19	$12+5\alpha$	-1	1	8	3
29	$7+2\alpha$	1	-1	7	9
31	$6+\alpha$	-1	-1	6	9

$G_3 \in S_{[8,4]}(SL_2(\mathcal{O}_F))$ Problem: $S_{[10,2]}(SL_2(\mathcal{O}_F)) = \{0\}$

p	$a_p(G_3)$	~~$a_p(G_5)$~~
11	$2172+1800\alpha \equiv -1$	
19	$-21340-9000\alpha \equiv 8$	
29	$86790+54000\alpha \equiv 7$	
31	$106112+79200\alpha \equiv 6$	

Explanation: When G_s exists, we use it to construct a non-zero
$[c] \in H^1_{\{5\}}(G_{\mathbb{Q}}, \mathrm{ad}^0(\bar{\rho}_{g,q})(1-s))$
accounting for $q \mid \dfrac{L_{\{5\}}(\mathrm{ad}^0(g), s)}{\Omega_s}$.

But one can show that actually $[c] \in H^1_f(G_{\mathbb{Q}}, \mathrm{ad}^0(\rho_{g,q})(1-s))$
so we should have $q \mid \dfrac{L(\mathrm{ad}^0(g), s)}{\Omega_s} = \dfrac{1}{1-5^{-s}} \dfrac{L_{\{5\}}(\mathrm{ad}^0(g), s)}{\Omega_s}$

$1-5^{-s} = \frac{1}{5^s}(5^s - 1)$ When $s=5$ this is divisible by 11, since $5^5 \equiv 1 \pmod{11}$,
so it can cancel the q we had in $\dfrac{L_{\{5\}}(\mathrm{ad}^0(g), 5)}{\Omega_5}$, making

$q \nmid \dfrac{L(\mathrm{ad}^0(g), 5)}{\Omega_5}$, so G_5 had better not exist.

Remarks (i) When G_s exists, there is an associated vector-valued Siegel modular Hecke eigenform of genus 2, $\mathcal{F}_s$, of weight $\det^{s+1} \otimes \mathrm{Sym}^{k-(s+1)}$, paramodular level $K(D^2)$. (Generalisation of Johnson-Leung Roberts lift.) Its associated 4-dimensional representations of $G_{\mathbb{Q}}$ are $\mathrm{Ind}_{G_F}^{G_{\mathbb{Q}}}$ of 2-dim reps. attached to G_s.

When G_s doesn't exist, a suitable $\mathcal{F}_s$ that is not lifted from a Hilbert modular form may still exist, and provide the Galois representation required to construct $[c] \in H^1_{\{p \nmid D\}}(G_{\mathbb{Q}}, \mathrm{ad}^0(\bar{\rho}_{g,q})(1-s))$

If $\lambda_p(\mathcal{F}_s)$ is the Hecke eigenvalue of "$T(p)$" on $\mathcal{F}_s$ (lifted from G_s) then

$$\lambda_p(\mathcal{F}_s) = a_{\mathfrak{p}}(G_s) + a_{\mathfrak{p}^\sigma}(G_s)$$
$$\equiv \left[(a^\sigma)^{k-1} + a^{k-1}p^{s-1}\right] + \left[a^{k-1} + (a^\sigma)^{k-1}p^{s-1}\right] \pmod{\mathfrak{Q}}$$
$$\equiv (a^{k-1} + (a^\sigma)^{k-1})(1 + p^{s-1})$$
$$\equiv a_p(g)(1 + p^{s-1}) \pmod{\mathfrak{Q}}$$

This is a congruence of Hecke eigenvalues between $\mathcal{F}_s$ and a Klingen-Eisenstein series (same weight and level) attached to g.

(ii) Another place where non-parallel weight Hilbert modular forms appear.

The projectivisation of the quintic $P(x,y) = P(z,w)$ where $P(x,y) = x^5 + y^5 - (5xy-5)(x^2+y^2-x-y)$, has 120 singular points, which may be blown up to give a non-singular Calabi-Yau 3-fold, the Consani-Scholten quintic X.

The representation of $G_{\mathbb{Q}}$ on $H^3_{\text{ét}}(X_{\bar{\mathbb{Q}}}, \mathbb{Q}_\ell)$ is 4-dimensional.

In 2012, Dieulefait, Pacetti and Schütt proved that this is induced from the representation of $G_{\mathbb{Q}(\sqrt{5})}$ attached to a Hilbert modular eigenform of weight $[4,2]$, level 30.

(iii) Hida informs me that numerical examples of congruences of this type, for non-parallel weight Hilbert modular forms, were discovered over 30 years ago by Naganuma (unpublished).

Bibliography

Joseph H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics 106, Springer.
A good place to learn more about such things as genus, separable isogenies, Frobenius morphisms, good and bad reduction, Weierstrass $\wp$-function, Shafarevich-Tate group, with a useful appendix on group cohomology and intro. chapters on algebraic geometry.

Fred Diamond, Jerry Shurman, A First Course in Modular Forms, Graduate Texts in Mathematics 228, Springer.
Includes in its later chapters modular curves as algebraic curves over $\mathbb{Q}$, Jacobians, the Eichler-Shimura construction and congruence relation.

John E. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press. Second Edition (1997) available online at the author's website.
Explains how examples are computed, e.g. how did we know Weierstrass equations for these elliptic curves E_f, E_g, their rational points and real periods, and the q-expansions of the associated newforms f and g?
For some more on computational aspects, including for weight greater than 2, see William A. Stein, Modular Forms: A Computational Approach, AMS Graduate Studies in Mathematics 79, available online on the author's website.
The L-functions and Modular Forms Database, www.lmfdb.org.

For the Cremona-Mazur construction, see their paper Visualizing elements in the Shafarevich-Tate group, Experiment. Math. 9 (2000), no. 1, 13-28, and also their appendix to A. Agashe, W. Stein, Mathematics of Computation 74 (2005), 455-484.

A. Agashe, K. A. Ribet, W. A. Stein, The modular degree, congruence primes, and multiplicity one, in Number Theory, Analysis and Geometry, 19-49, Springer 2012.

H. Hida, Modular Forms and Galois Cohomology, Cambridge University Press, 2000.
Around Section 5.3 for more on $L(\mathrm{ad}^0(f), 1)$, Ω^+, Ω^- and the cohomological congruence ideal.

F. Diamond, M. Flach, L. Guo, The Tamagawa number conjecture of adjoint ~~motives~~ motives of modular forms, Ann. Sci. École Norm. Sup. (4) 37 (2004), 663-727.

S. Bloch, K. Kato, L-functions and Tamagawa numbers of motives, The Grothendieck Festschrift Volume I, 333-400, Progress in Mathematics 86, Birkhäuser 1990. In a connection with Chol Park's lecture series, a good understanding of their conjecture involves p-adic Hodge theory.
Another good article on their conjecture is J.M. Fontaine, Valeurs spéciales des fonctions L des motifs, Séminaire Bourbaki, Vol. 1991/92, Astérisque 206 (1992), Exp. No. 751, 4, 205-249. For Deligne's conjecture (a precursor to the Bloch-Kato conjecture) see P. Deligne, Valeurs de Fonctions L et Périodes d'Intégrales, AMS Proc. Symp. Pure Math. Vol. 33 (1979), part 2, 247-290. There is an English translation by E. Ghate et. al.

H. Katsurada, Special values of the standard zeta functions for elliptic modular forms, Experiment. Math. 14 (2005), 27-45.

K. Ribet, A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$, Invent. Math. ~~[illegible]~~ 34 (1976), 151-162.

A.F. Brown, E.P. Ghate, Dihedral congruence primes and class fields of real quadratic fields, J. Number Theory 95 (2002), 14-37. For more on congruences between complex conjugate newforms in $S_k(\Gamma_0(D), \chi_D)$.

For congruences between Klingen-Eisenstein series and cusp forms, E. Urban, Selmer groups and the Eisenstein-Klingen ideal, Duke Math. J. 106 (2001), 485-525, and my paper Symmetric square L-functions and Shafarevich-Tate groups II, Int. J. Number Theory 5 (2009), 1321-1345.