Modular forms on noncongruence subgroups
and Atkin-Swinnerton-Dyer relations

Jerome William Hoffman

October 21, 2004
Outline

1. Definitions
2. Classical modular forms: coefficients
3. Classical modular forms: $l$-adic representations
4. A noncongruence subgroup
5. Parabolic cohomology
6. First main theorem: modularity
7. Second main theorem: congruences
Abstract

This is a joint project with

Liqun Fang

Ben Linowitz

Andrew Rupinski

Helena Verrill

We give new examples of modular forms on noncongruence subgroups whose $l$-adic representations are modular and whose expansion coefficients satisfy Atkin-Swinnerton-Dyer congruences.
1. **Definitions**

Let $\Gamma \subset \text{SL}(2, \mathbb{Z})$ be a subgroup of finite index. We distinguish two cases:

1. $\Gamma$ is a **congruence subgroup**. This means that $\Gamma$ contains

   $$\Gamma(N) = \{ \gamma \in \text{SL}(2, \mathbb{Z}) \mid \gamma \equiv I \mod N \}$$

   for some integer $N \geq 1$.

2. $\Gamma$ is a **noncongruence subgroup**, which means that it is not a congruence subgroup.

Recall that $\text{SL}(2, \mathbb{R})$ acts on the upper half-plane of complex numbers $\mathfrak{H}$ by linear fractional transformations. For any $\Gamma$ as above the quotient $\Gamma \backslash \mathfrak{H}$ is a Riemann surface, which on adding a finite number of points, called **cusps**, becomes compact. It is known that this Riemann surface is the set of $\mathbb{C}$-points of a projective smooth algebraic curve $X(\Gamma)$ defined over a finite extension $K$ of $\mathbb{Q}$. We let $j : Y(\Gamma) \hookrightarrow X(\Gamma)$ be the open set corresponding to $\Gamma \backslash \mathfrak{H}$; the complement $Z(\Gamma) = X(\Gamma) - Y(\Gamma)$ is the set of cusps. In most cases there is a family of elliptic curves $f : E(\Gamma) \rightarrow X(\Gamma)$, which is universal in a certain sense: often $X(\Gamma)$ is a **moduli space** classifying elliptic curves with additional structures.
A modular form of weight $k$ for $\Gamma$ is a complex-valued function $f(z)$ defined in $\mathcal{H}$ such that

1. $f(z)$ is holomorphic.

2. 
   
   \[ f\left(\frac{az + b}{cz + d}\right) = (cz + d)^k f(z) \quad \text{for all} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma. \]

3. $f(z)$ is holomorphic at all the cusps of $\Gamma$.

A modular form will have a Fourier expansion

\[ f(z) = \sum_{n=0}^{\infty} a_n(f)(q^{1/\mu})^n, \quad q = e^{2\pi iz}. \]

with no nonnegative exponents - holomorphy at $i\infty$. The integer $\mu$ is called the width of the cusp $i\infty$. There are analogous expansions at each cusp. We say that $f$ is a cusp form if the constant term $a_0 = 0$ at each cusp. We let $M_k(\Gamma)$ and $S_k(\Gamma)$ denote the finite dimensional space of modular forms, respectively cusp forms, of weight $k$ for $\Gamma$. 


Example: \( \Gamma' = \Gamma_1(4) \cap \Gamma_0(8). \)

\[
\Gamma' = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}(2, \mathbb{Z}) \ \bigg| \begin{array}{c}
\begin{align*}
&c \equiv 0 \mod 8, \\
&a \equiv d \equiv 1 \mod 4
\end{align*}
\end{array} \right\}.
\]

\( \Gamma' \) has index 12 inside \( \text{PSL}(2, \mathbb{Z}) \). The modular curve \( X(\Gamma') \) has genus 0 and four cusps. Since \( X(\Gamma') \cong \mathbb{P}^1 \) we can choose a coordinate - a generator of the function field (Hauptmodul)-call it \( t \). We normalize \( t \) by its values at the cusps: \( t(0) = 0, \ t(1/2) = \infty, \ t(\infty) = 1, \ t(1/4) = -1 \). The family of elliptic curves \( E(\Gamma') \to X(\Gamma') \) is given by

\[
y^2 + 4xy + 4t^2y = x^3 + t^2x^2.
\]

This has 4 universal points of order 4 which are

\[
P = (0,0), \ 2P = (-t^2,0), \ 3P = (0,-4t^2), \ 4P = O.
\]

The \( j \)-invariant is

\[
j = \frac{16(t^4 - 16t^2 + 16)^3}{t^8(1+t)(1-t)}
\]

which shows cusp widths of 8, 2, 1, 1 at \( t = 0, \infty, 1, -1 \).
A picture of the fundamental domain is:

The three elements labeled in the picture generate the stabilizers at the indicated cusp. \( \Gamma_1(4) \cap \Gamma_0(8) \) is the free group generated by these three elements.
2. Classical modular forms: coefficients

The expansion coefficients \( a(n) \) of a modular form on a congruence subgroup, a “classical modular form”, is an interesting arithmetical function. For instance, we know that

\[
\dim S_6(\Gamma_1(4)) = 1.
\]

In fact it is easy to see that

\[
g(z) = \sqrt{\Delta(2z)} = \eta(2z)^{12} = q \prod_{n=1}^{\infty} (1 - q^{2n})^{12}, \quad q = e^{2\pi i z}
\]

\[
= q - 12 q^3 + 54 q^5 - 88 q^7 - 99 q^9 + 540 q^{11} - 418 q^{13}
\]

\[
- 648 q^{15} + 594 q^{17} + 836 q^{19} + 1056 q^{21} - 4104 q^{23}
\]

\[
- 209 q^{25} + 4104 q^{27} - 594 q^{29} + 4256 q^{31} - 6480 q^{33}
\]

\[
- 4752 q^{35} - 298 q^{37} + 5016 q^{39} + 17226 q^{41} - 12100 q^{43} + 
\]

The coefficients \( a(n) \) satisfy

1. \( a(mn) = a(m)a(n) \) if \( \gcd(m, n) = 1 \).

2. \( a(p^{r+1}) = a(p)a(p^r) - p^3a(p^{r-1}) \) for all primes \( p \neq 2 \), all \( r \geq 1 \).

3. \( |a(p)| \leq 2p^{5/2} \), for all primes \( p \neq 2 \).

The first two reflect the fact that \( g \) is an eigenvector for the Hecke algebra \( \mathbf{T} \). The second is a special case of a theorem of Deligne (Ramanujan-Petersson conjecture).
3. Classical modular forms: $l$-adic representations

**Theorem 0.1.** Let $0 \neq f \in M_k(\Gamma_0(N), \chi)$. Suppose that $k \geq 2$ and that $f$ is an eigenfunction of $T_p \in T$, all $p \nmid N$, with eigenvalue $a_p$. Let $K$ be the necessarily finite extension of $\mathbb{Q}$ generated by the $a_p$ and the $\chi(p)$. Let $\lambda$ be a finite place of $K$, of residual characteristic $l$, and let $K_{\lambda}$ be the completion of $K$ in $\lambda$. There exists a semisimple continuous representation

$$\rho_{f,\lambda} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}(2, K_{\lambda})$$

which is unramified outside $Nl$ and such that

$$\text{Tr}(\rho_{f,\lambda}(\text{Frob}_p)) = a_p, \quad \text{det}(\rho_{f,\lambda}(\text{Frob}_p)) = \chi(p)p^{k-1}, \text{ if } p \nmid Nl.$$

This theorem is attributed to Deligne. Another way to formulate: The characteristic polynomial of $\text{Frob}_p$ acting in this representation is the Hecke polynomial

$$T^2 - a_p T + \chi(p)p^{k-1}$$

Note that $a_p$ is also the $p$th Fourier expansion coefficient of $f$. 
Let 

$$\rho : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}(n, \mathbb{Q}_l)$$

be a continuous representation. Let us say that $\rho$ is modular if it is isomorphic with a direct sum of representations $\rho_f$ coming from classical modular forms as in Deligne’s theorem. For this to make sense, $\rho$ must be unramified outside a finite set of places of $\mathbb{Q}$. We can weaken this to say the semisimplification of $\rho$ has such a decomposition. Wiles’ big theorem is that the two-dimensional $l$-adic representations coming from elliptic curves over $\mathbb{Q}$ are modular. This implied Fermat’s last theorem.

In general, it is a belief (Langlands’ philosophy) that the $L$-functions associated to $l$-adic representations arising in geometry, i.e., from motives, are equal to $L$-functions coming from automorphic forms. Classical modular forms are automorphic forms on $\text{GL}(2, \mathbb{Q})$. Winnie Li, Ling Long and Zifeng Yang gave an example of a 4-dimensional representation, attached to cusp forms of weight 3 on a noncongruence subgroup that is modular in this sense. This is a nontrivial relation between cusp forms on noncongruence subgroups and cusp forms on congruence subgroups.
4. A noncongruence subgroup

We let $\Gamma \subset \Gamma_0(8) \cap \Gamma_1(4)$ be the subgroup of index 3 defined by the covering $X = X(\Gamma) \to X(\Gamma')$ with equation $t = u^3$. In other words, we let $X = \mathbb{P}^1$ with coordinate $u$ and define a map $X \to X(\Gamma')$ by this rule. This covering ramifies only the cusps $t = 0, \infty$ with ramification index 3, so that $\Gamma$ has 8 cusps, at $u = 0, \infty, u = \zeta^i, \ i = 0, \ldots 5$ with widths 24, 6, 1 respectively. Here $\zeta$ is a primitive sixth root of unity.

Looking at Sebbar’s table we see that $\Gamma$ is not a congruence subgroup.

Here is a picture of its fundamental domain:
We are interested in the cusp forms of weight 3 for this \( \Gamma \). Using standard formulas, we compute \( \dim S_3(\Gamma) = 2 \). We can find explicit expansions for these at the cusp \( u = 1 \), of width 1. We do this as in LLY by defining

\[
    h_1 = \sqrt[3]{E_1^2 E_2}, \quad h_2 = \sqrt[3]{E_1 E_2^2}.
\]

where \( E_1 \) and \( E_2 \) are Eisenstein series of weight 3 for \( \Gamma_1(4) \cap \Gamma_0(8) \). We found the expansion for the Hauptmodul by recursively solving

\[
t - 1 = aq + bq^2 + cq^3 + \ldots
\]

from the equation

\[
j = \frac{16(t^4 - 16t^2 + 16)^3}{t^8(1 + t)(1 - t)}
\]

and the known expansion of \( j \). Then we used the identities \( t = E_1/E_2 \) and \( E_1^2 = g \cdot (t^2 - 1) \), where \( g \) is the weight 6 cusp form discussed earlier.
These relations are deduced from the data of zeros and poles of modular forms:

<table>
<thead>
<tr>
<th>Widths</th>
<th>2</th>
<th>8</th>
<th>1</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>$z$</td>
<td>$1/2$</td>
<td>0</td>
<td>$\infty$</td>
<td>$1/4$</td>
</tr>
<tr>
<td>$s$</td>
<td>$\infty^2$</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$t$</td>
<td>$\infty$</td>
<td>0</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>$g$</td>
<td>$0^2$</td>
<td>$0^2$</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$E_1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$E_2$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$E_1^2/g$</td>
<td>$\infty^2$</td>
<td>*</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Table 1: Data for modular forms on $\Gamma_0(8)$

$t = E_1/E_2$ and $E_1^2 = g \cdot (t^2 - 1)$. 
We get

\[ E_1 = q - 4q^2 + 8q^3 - 16q^4 + 26q^5 - 32q^6 + 48q^7 - 64q^8 + 73q^9 \]
\[ -104q^{10} + 120q^{11} - 128q^{12} + 170q^{13} - 192q^{14} + 208q^{15} \]
\[ -256q^{16} + 290q^{17} - 292q^{18} + 360q^{19} - 416q^{20} + 384q^{21} \]
\[ -480q^{22} + 528q^{23} + O(q^{24}) \]

\[ E_2 = q + 4q^2 + 8q^3 + 16q^4 + 26q^5 + 32q^6 + 48q^7 + 64q^8 + 73q^9 \]
\[ +104q^{10} + 120q^{11} + 128q^{12} + 170q^{13} + 192q^{14} + 208q^{15} \]
\[ +256q^{16} + 290q^{17} + 292q^{18} + 360q^{19} + 416q^{20} + 384q^{21} \]
\[ +480q^{22} + 528q^{23} + O(q^{24}) \]

\[ h_1 = q - \frac{4}{3}q^2 + \frac{8}{9}q^3 - \frac{176}{81}q^4 - \frac{850}{243}q^5 - \frac{3488}{729}q^6 - \frac{5968}{6561}q^7 \]
\[ + \frac{152512}{9}q^8 + \frac{56881}{59049}q^9 - \frac{2497000}{1594323}q^{10} - \frac{35104520}{4782969}q^{11} \]
\[ - \frac{15246464}{14348907}q^{12} + \frac{952141694}{129140163}q^{13} + O(q^{14}) \]

\[ h_2 = q + \frac{4}{3}q^2 + \frac{8}{9}q^3 + \frac{176}{81}q^4 + \frac{850}{243}q^5 + \frac{3488}{729}q^6 + \frac{5968}{6561}q^7 \]
\[ - \frac{152512}{9}q^8 + \frac{56881}{59049}q^9 + \frac{2497000}{1594323}q^{10} + \frac{35104520}{4782969}q^{11} \]
\[ + \frac{15246464}{14348907}q^{12} + \frac{952141694}{129140163}q^{13} + O(q^{14}) \]
5. Parabolic cohomology

The family of elliptic curves $f : E \to X$ is given by

$$y^2 + 4xy + 4u^6y = x^3 + u^6x^2.$$ 

Let $j : Y \hookrightarrow X$ be the inclusion of the open set minus the cusps, so $f : E \to Y$ is a smooth morphism, all of whose fibers are elliptic curves. We are interested in the 4-dimensional Galois representation

$$\Gamma V_l = H^1_{et}(X(\Gamma) \otimes \overline{\mathbb{Q}}, j_* R^1 f_* \mathbb{Q}_l)$$

This is the $l$-adic version of parabolic cohomology. Deligne proved that this representation is pure of weight 2. The DeRham version of this has a Hodge decomposition of type $(2, 0) + (0, 2)$.

$$\Gamma V_{DR} = H^1(X(\Gamma)^{an}, j_* R^1 f_* \mathbb{Q}) \otimes \mathbb{C} = S_3(\Gamma) \oplus \overline{S_3(\Gamma)}$$

which shows the connection to cusp forms. To understand this representation we compute the traces of Frobenius elements $\text{Frob}_p$. 


Let $\mathcal{F} = j_* R^1 f_* \mathbb{Q}_l$. We use the Grothendieck-Lefschetz trace formula:
\[
\text{Tr}(\text{Frob}_q | H^1(X(\Gamma), \mathcal{F})) = - \sum_{x \in X(\mathbb{F}_q)} \text{Tr}(\text{Frob}_q | \mathcal{F}_x).
\]
(Note that $H^i(X(\Gamma), \mathcal{F}) = 0$ for $i = 0, 2$.) The local traces are of two types:

1. The fiber $E_x$ is smooth. Then
\[
\text{Tr}(\text{Frob}_q | \mathcal{F}_x) = \text{Tr}(\text{Frob}_q | H^1(E_x, \mathbb{Q}_l)) = q + 1 - \#E_x(\mathbb{F}_q).
\]

2. The fiber $E_x$ is singular. Tate’s algorithm is then used to determine the fiber in the Néron model of the reduction mod $x$. Then
\[
\text{Tr}(\text{Frob}_q | \mathcal{F}_x) = \begin{cases} 
1 & \text{if the fiber is split multiplicative.} \\
-1 & \text{if the fiber is nonsplit multiplicative.} \\
0 & \text{if the fiber is additive.}
\end{cases}
\]

Code was written in Magma to accomplish this.
6. First main theorem: modularity

The traces of Frobenius computed this way gave

<table>
<thead>
<tr>
<th>p</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{Tr}_p$</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>-44</td>
<td>0</td>
<td>52</td>
<td>0</td>
</tr>
<tr>
<td>$\text{Tr}_{p^2}$</td>
<td>100</td>
<td>-188</td>
<td>484</td>
<td>292</td>
<td>1156</td>
<td>-92</td>
<td>2116</td>
</tr>
<tr>
<td>p</td>
<td>29</td>
<td>31</td>
<td>37</td>
<td>41</td>
<td>43</td>
<td>47</td>
<td>53</td>
</tr>
<tr>
<td>$\text{Tr}_p$</td>
<td>0</td>
<td>-92</td>
<td>52</td>
<td>0</td>
<td>-44</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$\text{Tr}_{p^2}$</td>
<td>3364</td>
<td>388</td>
<td>-4124</td>
<td>6724</td>
<td>-6428</td>
<td>8836</td>
<td>11236</td>
</tr>
</tbody>
</table>

Table 2: Table of $\text{Tr} \rho_t(Frob_q)$

Compare this to the coefficients of the unique element $f \in S_3(\Gamma_0(12), \chi)$, where $\chi : (\mathbb{Z} / 12)^\ast \to \mathbb{C}^\ast$ is the unique character of order 2 and conductor 3:

$$f = q - 3q^3 + 2q^7 + 9q^9 - 22q^{13} + 26q^{19} - 6q^{21} + 25q^{25} - 27q^{27} - 46q^{31} + 26q^{37} + 66q^{39} - 22q^{43} - 45q^{49} - 78q^{57} + 74q^{61} + 18q^{63} + 122q^{67} - 46q^{73} - 75q^{75} - 142q^{79} + 81q^{81} - 44q^{91} + 138q^{93} + 2q^{97} + O(q^{102})$$

This was found using MAGMA and corresponds to 12k3A[0, 1]1 in William Stein’s database.
One can observe that $|\text{Tr}_q| \leq 4q$. If $p \equiv 2 \mod 3$ then $\text{Tr}_p = 0$, and when this happens, $\text{Tr}_{p^2} = 4p^2$. Also, the table of traces is periodic: $p_1 \equiv p_2 \mod 6$ implies $\text{Tr}_{p_1} \equiv \text{Tr}_{p_2} \mod 48$.

**Theorem 0.2.** The $l$-adic representation $\rho_l$ attached to $S_3(\Gamma)$ is modular. More precisely, the $l$-adic representation on $\Gamma V_l = H^1(X(\Gamma), j_*R^1 f_* \mathbb{Q}_l)$ is isomorphic with $\rho_{f,l}^2$, where $\rho_{f,l}$ is the representation attached by Deligne to the newform $f \in S_3(\Gamma_0(12), \chi)$.

The proof is based on the method of Serre. In brief, one can conclude the isomorphism of two $l$-adic representations by comparing their traces at a finite number of primes, and verifying certain other, easily checkable, hypotheses.

The decomposition arises geometrically: There is an involution $A$ on the whole situation $E \to X$ that lifts up the map $u \to -u$ on $X$. Then the eigenspace decomposition

$$\Gamma V_l = (\Gamma V_l)^{A=1} \oplus (\Gamma V_l)^{A=-1}$$

corresponds to the decomposition $\rho_{f,l}^2$. 

17
7. Second main theorem: congruences

Symbolically, these can be expressed as

\[ S_3(\Gamma) \equiv S_3(\Gamma_0(48), \chi) \mod p^2. \]

What this means is that the \( p^{\text{th}} \) expansion coefficients of \( h_1, h_2 \in S_3(\Gamma) \) are congruent to the \( p^{\text{th}} \) expansion coefficient of \( f \otimes \psi \in S_3(\Gamma_0(48), \chi) \) modulo \( p^2 \), for almost all \( p \). Let \( c_n \) be the coefficients of \( h_1 \) and \( a_n \) be the coefficients of \( f \otimes \psi \). For instance:

\[
\begin{align*}
c_5 &= -\frac{850}{243} \equiv a_5 = 0 \mod 5^2, \\
c_7 &= -\frac{5968}{6561} \equiv a_7 = -2 \mod 7^2, \\
c_{11} &= -\frac{35104520}{478269} \equiv a_{11} = 0 \mod 11^2, \\
c_{13} &= \frac{952141694}{129140163} \equiv a_{13} = -22 \mod 13^2, \\
c_{17} &= -\frac{206256733102}{31381059609} \equiv a_{17} = 0 \mod 17^2, \\
c_{19} &= \frac{60201506159720}{2541865828329} \equiv a_{19} = -26 \mod 19^2, \\
c_{23} &= -\frac{5602670870929616}{617673396283947} \equiv a_{23} = 0 \mod 23^2, \\
c_{29} &= -\frac{43256611603055969890}{36472996377170786403} \equiv a_{29} = 0 \mod 29^2, \\
c_{31} &= -\frac{13177188009969486833216}{984770902183611232881} \equiv a_{31} = 46 \mod 31^2
\end{align*}
\]
The Riemann surface $\Gamma \backslash \mathfrak{H}^*$ is the set of $\mathbb{C}$-points of an algebraic curve $X(\Gamma)$ defined over a number field $K$. There exists a subfield $L$ of $K$, an element $\kappa \in K$ with $\kappa^\mu \in L$, where $\mu$ is the width of the cusp $\infty$, and a positive integer $M$ such that $\kappa^\mu$ is integral outside $M$ and $S_k(\Gamma)$ has a basis consisting of $M$-integral forms. Here a form $h \in S_k(\Gamma)$ is called $M$-integral if in its Fourier expansion at the cusp $\infty$,

$$h(\tau) = \sum_{n \geq 1} c_n(h)q^{n/\mu},$$

the Fourier coefficients $c_n(h)$ can be written as $\kappa^n b_n(h)$ with $b_n(h)$ lying in the ring $O_L[1/M]$, where $O_L$ denotes the ring of integers of $L$.

Let $h = \sum_{n \geq 1} c_n(h)q^{n/\mu}$ be an $M$-integral cusp form in $S_k(\Gamma)$, and let $f = \sum_{n \geq 1} a_n(f)q^n \in S_k(\Gamma_0(N), \chi)$ be a normalized newform of weight $k$ level $N$ and character $\chi$. The following definition is taken from LLY.

**Definition 0.3.** The two forms $f$ and $h$ above are said to satisfy the Atkin-Swinnerton-Dyer congruence relation if, for all primes $p$ not dividing $MN$ and for all $n \geq 1$,

$$(c_{np}(h) - a_p(f)c_n(h) + \chi(p)p^{k-1}c_{n/p}(h))/(np)^{k-1}$$

is integral at all places dividing $p$. 


Our second result is:

**Theorem 0.4.** The cusp forms \( h_1, h_2 \in S_3(\Gamma) \) satisfy Atkin-Swinnerton-Dyer congruences relative to \( f \otimes \psi \in S_3(\Gamma_0(48), \chi) \).

In the statement \( \psi \) is the Dirichlet character \((-1/n)\). The reason for this is that Scholl’s representation differs from our \( \Gamma V_i \) by a twist by \( \psi \). We omit this twist from the notation that follows.

Here is an idea of the proof: There is a version of parabolic cohomology in \( p \)-adic crystalline cohomology, denote it \( \Gamma V_p^\circ \). This is a free \( \mathbb{Z}_p \)-module of the same rank as its \( l \)-adic brother. Moreover

\[
S_3(\Gamma, \mathbb{Z}_p) \subset \Gamma V_p^\circ
\]

where the left hand side refers to cusp forms with expansion coefficients in \( \mathbb{Z}_p \). In our case, \( \Gamma V_p := \Gamma V_p^\circ \otimes \mathbb{Q}_p \) is a 4-dimensional \( \mathbb{Q}_p \)-vectorspace with an action of a Frobenius - it’s an F-isocrystal. For each cusp there is an expansion map

\[
taylor : \Gamma V_p^\circ \longrightarrow \Gamma V_p^\infty
\]

where

\[
\Gamma V_p^\infty = \text{coker} \left( (p\partial)^2 : t\mathbb{Z}_p[[t]] \to t\mathbb{Z}_p[[t]] \right)
\]

Here \( t \) is a local coordinate at the cusp and

\[
\partial = Ct \frac{d}{dt}, \quad C \in \mathbb{Z}[1/M] \subset \mathbb{Z}_p^\times.
\]
There is an action of Frobenius $F$ on $\Gamma V_p^\infty$ that commutes with the taylor map. Also $F$ has a very simple form on $\Gamma V_p^\infty$:

$$F(\sum c_n t^n) \equiv \sum p^2 c_n \gamma_p^n t^{pn} \mod \text{Im}(p\partial)^2$$

for some explicit $\gamma_p \in 1 + p\mathbb{Z}_p$ depending on the local coordinate. Now we have the

**Congruence principle:** Let $H(T) \in \mathbb{Z}[T], h \in S_k(\Gamma, \mathbb{Z}_p)$ and suppose that $H(F)h = 0$ in $\Gamma V_p$. Then the expansion coefficients of $h$ satisfy ASwD congruences relative to the coefficients of $H(T)$.

**Proof.**

To fix ideas take $k = 3$, \text{taylor}(h) = $\sum c(n)t^n$ and suppose

$$H(T) = \sum_{r=0}^{2d} a(r) T^{2d-r} \quad \text{has even degree.}$$

Then \text{taylor}(H(F)h) = H(F) \text{taylor}(h) = 0, so

$$H(F) \text{taylor}(h) \in \text{Im}(p\partial)^2.$$  

But the $n$th expansion coefficient of any element of $\text{Im}(p\partial)^2$ is in $(np)^2\mathbb{Z}_p$, hence

$$n$$th coefficient of $H(F) \text{taylor}(h)$ is in $(np)^2\mathbb{Z}_p$.  


Since we know an explicit form for the action of $F$ on $\Gamma V_p^\infty$, we can write out the $n$th coefficient of $H(F) \text{ taylor}(h)$, and this gives congruences. They have a simple form when we assume that $a(0) = 1$, $a(2d - r) = p^{2(d-r)}a(r)$. It leads to the conclusion
\[
\text{ord}_p \left( \sum_{r=0}^{2d} a(r)c(np^{d-r}) \right) \geq 2(\text{ord}_p(n) + 1)
\]

To finish the proof of the second main theorem, we observe that
\[
h_1 \in S_3(\Gamma, \mathbb{Z}_p)^{A=1} \subset (\Gamma V_p \otimes \psi)^{A=1}
\]
the right hand side being a 2-dimensional space. By our modularity theorem, we know that
\[
\text{det} \left( T - \text{Frob}_p : (\Gamma V_\ell \otimes \psi)^{A=1} \right) = T^2 - a_p(f \otimes \psi)T + \chi(p)p^2
\]
for $f \in S_3(\Gamma_0(12), \chi)$. Call this polynomial $H(T)$. I claim that
\[
\text{det} \left( T - \text{Frob}_p : (\Gamma V_\ell \otimes \psi)^{A=1} \right) = \text{det} \left( T - F : (\Gamma V_p \otimes \psi)^{A=1} \right)
\]
The Cayley-Hamilton theorem shows that $H(F) \equiv 0$ on $(\Gamma V_p \otimes \psi)^{A=1}$, hence $H(F)h_1 = 0$, so we win by the congruence principle.
As for the equality of $l$-adic and $p$-adic characteristic polynomials, it follows from

**Theorem 0.5.** Let $f : E \to X$ be a projective smooth morphism, where $X$ is a smooth projective curve over a finite field $\mathbb{F}_q$. Suppose that the general fiber of $f$ is an elliptic curve, that $f$ is nonconstant and semiabelian, i.e., the Néron fibers at the singular fibers of $f$ are of multiplicative type. Then

$$\det (1 - T \text{Frob}_q : V_l(E/X)) = \det (1 - TF : V_p(E/X))$$

Here, $V_l(E/X)$ and $V_p(E/X)$ are the $l$-adic and $p$-adic versions of parabolic cohomology, and $F$ lifts up the $q$th power map.

The proof is a comparison of the Grothendieck-Lefschetz trace formula and the Monsky-Washnitzer-Reich-Scholl trace formula. If the fiber $E_x$ is smooth the equality of local traces is due to Katz and Messing. In a place of bad reduction, the equality of local traces depends on more recent results of Mokrane and Trihan.

The polynomial in the theorem is equal to the $L$-function of the elliptic curve $E_\eta$ over the function field $\eta = \text{Spec}(\mathbb{F}_q(X))$. 

Thanks to

Winnie Li

and the

Penn. State Math. Dept.
Thanks to

Steve Weintraub

and the

Lehigh Math. Dept.
Thanks to

Jorge Morales

and the

LSU Math. Dept.