Images of Galois representations

Anni, S.

Appendix A

Minimal level of realization

The aim of this appendix is to analyse degeneracy maps between modular curves. In the next sections are presented results similar to the ones obtained in [Edi06], where the action of Frobenius and multiplication by the Hasse invariant on Katz modular forms are studied. In particular, from this we deduce statements on residual modular Galois representations and their level of realization. This appendix is based on the theory of Katz modular forms, see [Kat73], [Kat77] and [Edi92], and modular curves, see [KM85] and [Gro90].

Let us recall that also in [DS05, Section 5.7] there is a detailed explanation about degeneracy maps between modular curves over $\overline{\mathbb{Q}}$ and are obtained similar results to the ones that we prove in this appendix, see [DS05, Theorem 5.7.1 (Main Lemma)]. The statement of [DS05, Theorem 5.7.1 (Main Lemma)] is proved through a reduction to linear algebra and representation theory: in particular, the first step is to change the congruence subgroups in order to pass from degeneracy maps to inclusions, see [DS05, p.191]. In this appendix, instead, we focus on the study of modular curves over finite fields and on a geometric interpretation of degeneracy maps.

A.1 Notations and preliminaries

For n, k positive integers, ℓ prime not dividing n and $\overline{\mathbb{F}}_\ell$ an algebraic closure of $\mathbb{F}_\ell$, let $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ be the space of Katz modular forms of weight k for $\Gamma_1(n)$ on $\overline{\mathbb{F}}_\ell$. Let $S(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ be the subspace of $M(\Gamma_1(n),k,\epsilon)_{\overline{\mathbb{F}}_\ell}$ whose elements have q-expansions that are power series with constant term zero at all cusps.

For any character $\epsilon\colon (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, let $S(\Gamma_1(n),k,\epsilon)_{\overline{\mathbb{F}}_\ell}$ be the space of Katz cusp forms of weight k for $\Gamma_1(n)$ and character ϵ:

$$S(\Gamma_1(n),k,\epsilon)_{\overline{\mathbb{F}}_\ell} := \{f \in S(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell} \,|\, \forall d \in (\mathbb{Z}/n\mathbb{Z})^*,\ \langle d\rangle f = \epsilon(d) f\}.$$

If $n = mp^r$ with $r \geq 1$ and p not dividing m, we will "split" the level structure accordingly, and denote the space as $S(\Gamma_1(m),\Gamma_1(p^r),k,\epsilon_m,\epsilon_p)_{\overline{\mathbb{F}}_\ell}$, but, in order to shorten the notation, we will write $S(m,p^r,k,\epsilon)_{\overline{\mathbb{F}}_\ell}$ instead. We will use analogous notation for modular curves.

If $n>4$, then $S(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ is isomorphic to $\mathrm{H}^0(X_1(n)_{\overline{\mathbb{F}}_\ell},\omega^{\otimes k}(-\mathrm{Cusps}))$, the space of global sections of the line bundle $\omega^{\otimes k}(-\mathrm{Cusps})$, while the space of Katz modular forms $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ is isomorphic to $\mathrm{H}^0(X_1(n)_{\overline{\mathbb{F}}_\ell},\omega^{\otimes k})$, see [Gro90, Proposition 2.2].

Let us recall some useful concepts and notations. Given a modular curve $X_1(n)_{\overline{\mathbb{F}}_\ell}$ with $(n,\ell)=1$, if $n=mp^r$ with $r\geq 1$ and p not dividing m, we have two degeneracy maps B_p and α:

$$\begin{array}{ccc} & X_1(m,p^r)_{\overline{\mathbb{F}}_\ell} & \\ {\scriptstyle B_p}\swarrow & & \searrow{\scriptstyle \alpha} \\ X_1(m,p^{r-1})_{\overline{\mathbb{F}}_\ell} & & X_1(m,p^{r-1})_{\overline{\mathbb{F}}_\ell}. \end{array} \tag{A.1}$$

Using the moduli interpretation for $X_1(n)_{\overline{\mathbb{F}}_\ell}$, i.e. considering E/S, an elliptic curve over an $\overline{\mathbb{F}}_\ell$-scheme S, with P and Q respectively points of order m and p^r, we give the following description of the degeneracy maps: α is the forgetful map $\alpha\colon (E,P,Q)\longmapsto(E,P,pQ)$ and B_p is the p-th degeneracy map defined by $B_p\colon (E,P,Q)\mapsto(E/\langle p^{r-1}Q\rangle,\beta(P),\beta(Q))$, where

$$\langle p^{r-1}Q\rangle \rightarrowtail E \xrightarrow{\beta} E/\langle p^{r-1}Q\rangle$$

is the degree p isogeny whose kernel is generated by $p^{r-1}Q$.

Let us fix ζ_{p^r} a root of unity of order p^r in $\overline{\mathbb{F}}_\ell$. The Atkin-Lehner map $w_{\zeta_{p^r}}$ on $X_1(n)_{\overline{\mathbb{F}}_\ell}$ is defined as follows:

$$\begin{array}{ccc} X_1(n)_{\overline{\mathbb{F}}_\ell} & \xrightarrow{w_{\zeta_{p^r}}} & X_1(n)_{\overline{\mathbb{F}}_\ell} \\ (E,P,Q) & \longmapsto & (E/\langle Q\rangle,\beta_r(P),Q') \end{array} \tag{A.2}$$

where β_r is the degree p^r isogeny whose kernel is generated by Q, and where Q' belongs to $\ker(\beta_r^t)(S)$:

$$\langle Q\rangle \rightarrowtail E \underset{\beta_r^t}{\overset{\beta_r}{\rightleftarrows}} E/\langle Q\rangle \twoheadleftarrow \langle Q'\rangle$$

and it is the unique element such that $e_\beta(Q,Q')=\zeta_{p^r}$, where e_β is the Weil pairing related to β i.e. the perfect μ_{p^r} valued pairing between $\ker(\beta)$ and $\ker(\beta^t)$, see [KM85, Section 2.8].

Let us recall basic facts about Tate curves. Precise results can be found in [DR73, Chapter VII], see also [Sil94, Chapter V] for a more elementary and explicit approach.

For every positive integer d, the d-th Tate curve is a certain generalized elliptic curve $\mathrm{Tate}(q^d)\to\operatorname{Spec}\mathbb{Z}[[q]]$ that becomes a Néron d-gon after

base change to the zero locus of q and that is a smooth elliptic curve over $\operatorname{Spec}\mathbb{Z}[[q]][q^{-1}]$, the complement of this zero locus.

Let d, e and n be positive integers such that n is the least common multiple of d and e. Then the curve $\mathrm{Tate}(q^d)$ over $\operatorname{Spec}\mathbb{Z}[[q,\zeta_e]]$, where ζ_e is a e-th root of unity, admits a $\Gamma_1(n)$-structure. Each choice of d, e and of the a $\Gamma_1(n)$-structure gives rise to an injective map from $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ to $\overline{\mathbb{F}}_\ell \otimes_{\mathbb{Z}} \mathbb{Z}[[q,\zeta_e]]$, which is called the q-expansion map relative to $\mathrm{Tate}(q^d)$ with the given $\Gamma_1(n)$-structure. The $\Gamma_1(n)$-structure on $\mathrm{Tate}(q^n)$ over $\operatorname{Spec}\mathbb{Z}[[q]]$ given by $\psi(i) = q^i$ for $i \in \mathbb{Z}/n\mathbb{Z}$, gives rise to a particular q-expansion called the q-expansion at ∞, see [KM85, Sections 8.8 and 8.11] for explanation. For any $f \in M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ we define $a_m(f)$ to be the m-th coefficient in this q-expansion.

A.2 Level lowering for Katz cusp forms

Main Lemma 1. *Let n and k be positive integers. Let ℓ and p be primes such that p strictly divides n and $n/p > 4$, while ℓ does not divide n and $1 \leq k \leq \ell+1$. Let f be a* mod ℓ *cusp form in $S(n/p,p,k)_{\overline{\mathbb{F}}_\ell}$ such that*

$$f(\mathrm{Tate}(q),\zeta_{n/p},\zeta_p) = \sum_{j\geq 1} a_j(f) q^j \left(\frac{dt}{t}\right)^{\otimes k} \in \overline{\mathbb{F}}_\ell[[q^p]] \left(\frac{dt}{t}\right)^{\otimes k}, \qquad \text{(A.3)}$$

where $\zeta_{n/p}$ and ζ_p are respectively n/p-th and p-th roots of unity. Then there exists a unique modular form $g \in S(n/p,k)_{\overline{\mathbb{F}}_\ell}$, such that $B_p^* g = f$, where B_p^* is the morphism induced by $B_p\colon X_1(n)_{\overline{\mathbb{F}}_\ell} \to X_1(n/p)_{\overline{\mathbb{F}}_\ell}$, the p-th degeneracy map.

Proof. Since p strictly divides n, let us write $n = mp$. Hypothesis (A.3) means that the q-expansion of f at the cusp at ∞ is such that $a_j(f) = 0$ for all positive integers j not divisible by p.

As $m > 4$ by hypothesis, f is an element of $\mathrm{H}^0(X_1(n)_{\overline{\mathbb{F}}_\ell}, \omega^{\otimes k}(-\mathrm{Cusps}))$, hence, using known relations and correspondences between modular curves, we have the following commutative diagram:

$$\begin{array}{ccc} X_1(n)_{\overline{\mathbb{F}}_\ell} & \xrightarrow{w_{\zeta_p}} & X_1(n)_{\overline{\mathbb{F}}_\ell} \\ {\scriptstyle B_p}\downarrow & & \downarrow{\scriptstyle \alpha} \\ X_1(m)_{\overline{\mathbb{F}}_\ell} & = & X_1(m)_{\overline{\mathbb{F}}_\ell} \end{array}$$

where B_p and α are the degeneracy maps defined in (A.1) and w_{ζ_p} is the Atkin-Lehner map associated to the isogeny β, defined in (A.2). The isogeny

β induces a morphism β^* from the line bundle $\omega^{\otimes k}(-\text{Cusps})$ on $X_1(m)_{\overline{\mathbb{F}}_\ell}$ to the line bundle $\omega^{\otimes k}(-\text{Cusps})$ on $X_1(n)_{\overline{\mathbb{F}}_\ell}$, because for each $(E/S, P, Q)$ we have an isomorphism of invertible O_S-modules β^* between $\omega_{E/\langle Q\rangle}$ and ω_E. Similarly, we define $w^*_{\zeta_p} : S(n,k)_{\overline{\mathbb{F}}_\ell} \to S(n,k)_{\overline{\mathbb{F}}_\ell}$ by

$$(w^*_{\zeta_p} h)(E,P,Q) = \beta^*(h(w_{\zeta_p}(E,P,Q))) = \beta^*(h(E/\langle Q\rangle, \beta(P), Q')),$$

where h belongs to $S(n,k)_{\overline{\mathbb{F}}_\ell}$, see [Gro90, Section 6]. In particular, it follows from the construction that there exists a unique $f' \in S(n,k)_{\overline{\mathbb{F}}_\ell}$ such that $w^*_{\zeta_p} f' = f$. In fact, let us consider the q-expansion at the cusp at ∞:

$$\begin{aligned}
(w^*_{\zeta_p} f')(\infty) &= (w^*_{\zeta_p} f')(\mathrm{Tate}(q), \zeta_m, \zeta_p) = \beta^*(f'(\infty')) = \\
&= \beta^*(f'(\mathrm{Tate}(q^p), \zeta_m^p, q)) = \beta^* \left(\sum_{j\geq 1} a_j(f') q^j \left(\frac{dt}{t}\right)^{\otimes k} \right) = \\
&= \left(\sum_{j\geq 1} a_j(f') q^j \right) p^k \left(\frac{dt}{t}\right)^{\otimes k}
\end{aligned}$$

where $\infty' := w_{\zeta_p}(\infty)$ and the last equality follows from:

$$\mu_p \rightarrowtail \mathrm{Tate}(q) \xrightarrow{\beta} \mathrm{Tate}(q^p)$$

hence $\beta^*((dt)/t) = p((dt)/t)$. Since $f(\mathrm{Tate}(q), \zeta_m, \zeta_p) \in \overline{\mathbb{F}}_\ell\,[[q^p]]\,((dt)/t)^{\otimes k}$ we deduce that for all positive integer j we have $a_j(f')p^k = a_j(f)$ and

$$f'(\mathrm{Tate}(q^p), \zeta_m^p, q) \in \overline{\mathbb{F}}_\ell\,[[q^p]] \left(\frac{dt}{t}\right)^{\otimes k}.$$

In order to prove that f comes from $X_1(m)_{\overline{\mathbb{F}}_\ell}$ via B_p^*, it is enough to show that f' does via α. To prove this claim, we study to the following diagram of modular curves:

$$\begin{array}{ccc}
X(\Gamma_1(m), \Gamma(p)^{\zeta_p - \mathrm{can}})_{\overline{\mathbb{F}}_\ell} & (E,P,Q_1,Q_2) & (\mathrm{Tate}(q^p), \zeta_m^p, q, \zeta_p) \\
\downarrow{\scriptstyle \gamma} & \downarrow & \downarrow \\
X(\Gamma_1(m), \Gamma_1(p))_{\overline{\mathbb{F}}_\ell} & (E,P,Q_1) & (\mathrm{Tate}(q^p), \zeta_m^p, q) \\
\downarrow{\scriptstyle \alpha} & \downarrow & \downarrow \\
X(\Gamma_1(m))_{\overline{\mathbb{F}}_\ell} & (E,P) & (\mathrm{Tate}(q^p), \zeta_m^p)
\end{array}$$

where Q_1, Q_2 are such that $e_p(Q_1,Q_2) = \zeta_p$, and α, γ are both forgetful maps.

On $X(\Gamma_1(m),\Gamma(p)^{\zeta_p-\mathrm{can}})_{\overline{\mathbb{F}}_\ell} \to X(\Gamma_1(m))_{\overline{\mathbb{F}}_\ell}$ there is the natural $\mathrm{SL}_2(\mathbb{F}_p)$ action, given by the action of $\mathrm{SL}_2(\mathbb{F}_p)$ on $\Gamma(p)^{\zeta_p-\mathrm{can}}$. This action is trivial on $X(\Gamma_1(m))_{\overline{\mathbb{F}}_\ell}$.

In the following diagram we describe the action of $\mathrm{SL}_2(\mathbb{F}_p)$:

$$\begin{array}{ccc} & & X(\Gamma_1(m),\Gamma(p)^{\zeta_p-\mathrm{can}})_{\overline{\mathbb{F}}_\ell} \\ & & \Big\downarrow {\scriptstyle \left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)} \\ \mathrm{SL}_2(\mathbb{F}_p) & \circlearrowleft & X(\Gamma_1(m),\Gamma_1(p))_{\overline{\mathbb{F}}_\ell} \\ & & \Big\downarrow \\ & & X(\Gamma_1(m))_{\overline{\mathbb{F}}_\ell} \end{array}$$

Taking into account this action, there exists $g \in S(m,k)_{\overline{\mathbb{F}}_\ell}$ such that $B_p^* g = f$ if and only if $\gamma^* f'$ is $\mathrm{SL}_2(\mathbb{F}_p)$-invariant.

The map $\gamma : X(\Gamma_1(m),\Gamma(p)^{\zeta_p-\mathrm{can}})_{\overline{\mathbb{F}}_\ell} \to X(\Gamma_1(m),\Gamma(p))_{\overline{\mathbb{F}}_\ell}$ corresponds to the action of elements of the form $\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{F}_p)$ and $\gamma^* f'$ is invariant under the action of $\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)$ by construction. Since $\{\left(\begin{smallmatrix}1 & 0\\ * & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)\}$ generate $\mathrm{SL}_2(\mathbb{F}_p)$, and $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$ generates the subgroup $\left(\begin{smallmatrix}1 & 0\\ * & 1\end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{F}_p)$, in order to conclude it is enough to prove that $\gamma^* f'$ is invariant under the action of $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$.

Let us remark that $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$ fixes $\infty' \in X(\Gamma_1(m),\Gamma(p)^{\zeta_p-\mathrm{can}})_{\overline{\mathbb{F}}_\ell}$ and it acts on the complete local ring at ∞', $\overline{\mathbb{F}}_\ell[[q]]$, as:

$$\begin{cases} \text{identity on } \overline{\mathbb{F}}_\ell \\ q \mapsto \zeta_p q \end{cases}.$$

It follows that $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)$ acts on $\overline{\mathbb{F}}_\ell[[q]](dt/t)^{\otimes k}$ by $t \mapsto t$, by definition, and, hence, $(dt/t)^{\otimes k} \mapsto (dt/t)^{\otimes k}$. As $a_j(f') = 0$ for all positive integers j not divisible by p, then $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)^* f'$ has the same q-expansion as f'.

Since $X(\Gamma_1(m),\Gamma(p)^{\zeta_p-\mathrm{can}})_{\overline{\mathbb{F}}_\ell}$ is an irreducible and reduced curve, this means that $\left(\begin{smallmatrix}1 & 0\\ 1 & 1\end{smallmatrix}\right)^* \gamma^* f' = \gamma^* f'$.

The modular form $g \in S(m,k)_{\overline{\mathbb{F}}_\ell}$ such that $B_p^* g = f$ is unique: this follows because, from the one hand, pullback does not change q-expansions and, on the other hand, the q-expansion principle holds, see [Kat73, Section 1.12]. □

Lemma A.2.1. *Given $r \in \mathbb{Z}_{>0}$ and a prime p, the set*

$$\left\{ \begin{pmatrix} 1 & 0 \\ p^r & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\} \subset \mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z})$$

generates the subgroup

$$\overline{\Gamma_1(p^r)} := \left\{ \begin{pmatrix} 1+p^r a & b \\ p^r c & 1+p^r d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z}) \right\}.$$

Proof. We will show that every matrix in $\overline{\Gamma_1(p^r)}$ can be written as a finite product of $\left(\begin{smallmatrix} 1 & 0 \\ p^r & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. Let $\left(\begin{smallmatrix} 1+p^r a & b \\ p^r c & 1+p^r d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z})$, with $a, b, c, d \in \mathbb{F}_p$, by direct computation in $\mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z})$ we get:

$$\begin{pmatrix} 1+p^r a & b \\ p^r c & 1+p^r d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ p^r & 1 \end{pmatrix}^{c-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{a} \begin{pmatrix} 1 & 0 \\ p^r & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{(p^r a-1)(a-b)}.$$

Let us remark that the computation is done by multiplying the matrix $\left(\begin{smallmatrix} 1+p^r a & b \\ p^r c & 1+p^r d \end{smallmatrix}\right)$ in $\mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z})$ on the left and on the right by powers of $\left(\begin{smallmatrix} 1 & 0 \\ p^r & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ in order to obtain the identity matrix. In particular, for $m \in \mathbb{Z}$, multiplying by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)^m$

– on the left means add m-times the first column to the second;
– on the right means add m-times the second row to the first;

and multiplying by $\left(\begin{smallmatrix} 1 & 0 \\ p^r & 1 \end{smallmatrix}\right)^m$

– on the left is equal to change the elements of the second row respectively multiplying by p^r the sum of the first element of the second row and m, adding mp^r times the second element of the first row to the second element of the second row;
– on the right is equal to change the elements of the first column respectively adding mp^r times the first element of the second column to the first element of the column; and multiplying by p^r the sum of the second element of the column and m.

□

Lemma A.2.2. *Let E/S be an elliptic curve over an $\overline{\mathbb{F}}_\ell$-scheme S, $r \geq 1$ an integer, p be a prime different from ℓ and*

$$E \xrightarrow[\beta_1]{} E/\langle p^r Q\rangle \xrightarrow[\beta_r]{} E/\langle Q\rangle, \qquad E \xrightarrow{\beta_{r+1}} E/\langle Q\rangle$$

the standard factorization of a cyclic p^{r+1}-isogeny into a cyclic p-isogeny followed by a cyclic p^r-isogeny, where Q is a point of order p^{r+1}. Let Q_{r+1} and Q_r be the unique points that normalize the Weil pairings: $e_{\beta_{r+1}}(Q, Q_{r+1}) = \zeta_{p^{r+1}}$ and $e_{\beta_r}(\beta_1(Q), Q_r) = \zeta_{p^r}$. Then

$$Q_r = pQ_{r+1}.$$

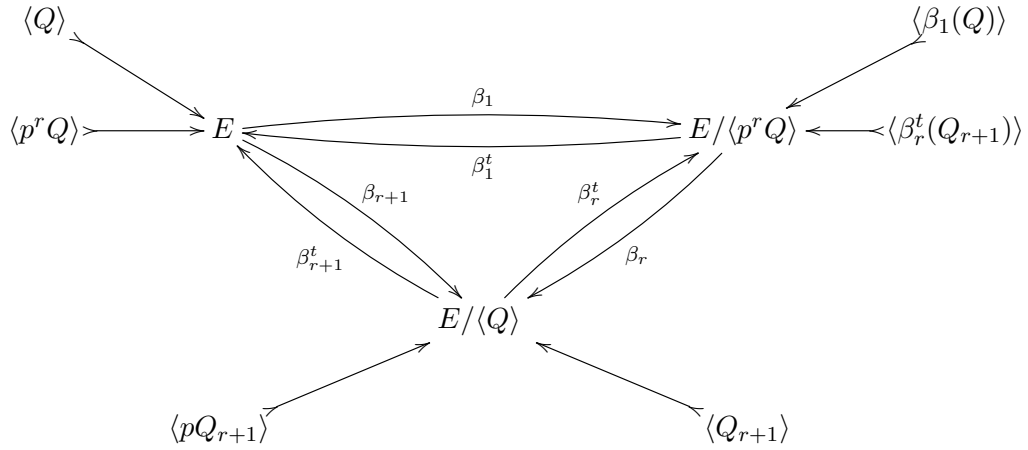
Proof. First of all, we apply the "Backing-up Theorem", see [KM85, 6.7.11], to the isogeny β_{r+1} and to its dual isogeny, we have that:

$$\langle \beta_1(Q)\rangle = \ker(\beta_r), \quad \langle p^r Q\rangle = \ker(\beta_1),$$

and, respectively,

$$\langle \beta_r^t(Q_{r+1})\rangle = \ker(\beta_1^t), \quad \langle p(Q_{r+1})\rangle = \ker(\beta_r^t).$$

In the following diagram, for clarity, we resume all the isogenies we have taken into account:



By definition of the Weil pairing, we have that $\langle Q_r\rangle = \ker(\beta_r^t) = \langle pQ_{r+1}\rangle$, so there exists $k \in (\mathbb{Z}/p^r\mathbb{Z})^*$ such that $kQ_r = pQ_{r+1}$, since they generate the same cyclic group of order p^r. Hence, by bilinearity of the pairing we have

$$e_{\beta_r}(\beta_1(Q), kQ_r) = \zeta_{p^r}^k = e_{\beta_r}(\beta_1(Q), pQ_{r+1}).$$

The compatibility of the pairing, see [KM85, 2.8] and [Sil09, III 8.1], implies that

$$e_{\beta_r}(\beta_1(Q), pQ_{r+1}) = e_{\beta_{r+1}}(Q, pQ_{r+1}) = \zeta_{p^{r+1}}^p = \zeta_{p^r}.$$

As $e_{\beta_r}(\beta_1(Q), Q_r) = \zeta_{p^r}$, then $k = 1$, hence $Q_r = pQ_{r+1}$. □

Main Lemma 2. *Let n and k be positive integers. Let ℓ and p be primes such that $n = mp^{r+1}$ with p and m co-prime, $r \in \mathbb{Z}_{\geq 1}$ and $mp^r > 4$, while ℓ does not divide n and $1 \leq k \leq \ell+1$. Let f be a* mod ℓ *cusp form in $S(m, p^{r+1}, k)_{\overline{\mathbb{F}}_\ell}$ such that*

$$f(\mathrm{Tate}(q), \zeta_m, \zeta_{p^{r+1}}) = \sum_{j\geq 1} a_j(f) q^j \left(\frac{dt}{t}\right)^{\otimes k} \in \overline{\mathbb{F}}_\ell\,[[q^p]] \left(\frac{dt}{t}\right)^{\otimes k}$$

where ζ_m and $\zeta_{p^{r+1}}$ are respectively fixed m-th and p^{r+1}-th roots of unity. Then there exists a unique modular form $g \in S(m, p^r, k)_{\overline{\mathbb{F}}_\ell}$, such that $B_p^* g = f$, where B_p^* is induced by $B_p : X_1(m, p^{r+1})_{\overline{\mathbb{F}}_\ell} \to X_1(m, p^r)_{\overline{\mathbb{F}}_\ell}$ the p-th degeneracy map.

Proof. Since $mp^r > 4$ we have the following diagram:

$$\begin{array}{ccc} X_1(m,p^{r+1})_{\overline{\mathbb{F}}_\ell} & \xrightarrow{w_{\zeta_{p^{r+1}}}} & X_1(m,p^{r+1})_{\overline{\mathbb{F}}_\ell} \\ \Big\downarrow{\scriptstyle B_p} & & \Big\downarrow{\scriptstyle \tilde{\alpha}} \\ X_1(m,p^r)_{\overline{\mathbb{F}}_\ell} & \xrightarrow{w_{\zeta_{p^r}}} & X_1(m,p^r)_{\overline{\mathbb{F}}_\ell} \end{array}$$

where B_p is the degeneracy map defined in (A.1), $w_{\zeta_{p^r}}$ and $w_{\zeta_{p^{r+1}}}$ are the Atkin-Lehner maps defined as in (A.2) and where $\tilde{\alpha} := w_{\zeta_{p^r}} \circ B_p \circ w^{-1}_{\zeta_{p^{r+1}}}$.

Our first goal is to prove that the map $\tilde{\alpha}$ is the forgetful map α defined in (A.1). On a elliptic curve E over S, $\overline{\mathbb{F}}_\ell$-scheme, with P and Q respectively points of order m and p^{r+1}, we have:

$$\begin{array}{ccc} (E,P,Q) & \xmapsto{w_{\zeta_{p^{r+1}}}} & (E/\langle Q\rangle, \beta_{r+1}(P), Q_{r+1}) \\ \Big\downarrow{\scriptstyle B_p} & & \Big\downarrow{\scriptstyle \tilde{\alpha}} \\ (E/\langle p^rQ\rangle, \beta_1(P), \beta_1(Q)) & \xmapsto{w_{\zeta_{p^r}}} & (E/\langle Q\rangle, \beta_r(\beta_1(P)), Q_r) \end{array}$$

and

$$(E/\langle Q\rangle, \beta_{r+1}(P), Q_{r+1}) \xmapsto{\alpha} (E/\langle Q\rangle, \beta_{r+1}(P), pQ_{r+1}) \ ,$$

where the maps $\beta_1, \beta_r, \beta_{r+1}$ are isogenies defined by:

$$\begin{array}{ccccc} & & \overset{\beta_{r+1}}{\frown} & & \\ E & \xrightarrow[\beta_1]{} & E/\langle p^rQ\rangle & \xrightarrow[\beta_r]{} & E/\langle Q\rangle \end{array}$$

so $\beta_r(\beta_1(P)) = \beta_{r+1}(P)$. In order to show that $\tilde{\alpha} = \alpha$, it is sufficient to apply Lemma A.2.2: $Q_r = pQ_{r+1}$.

We have that:

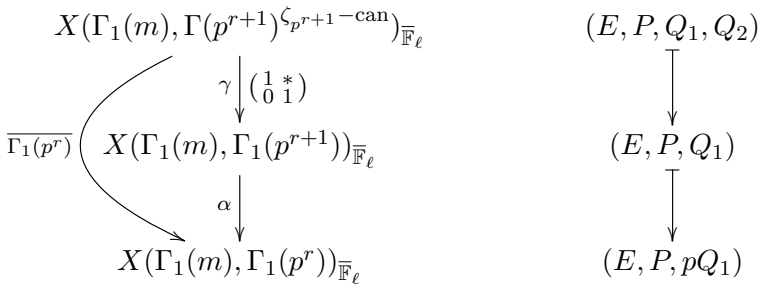
$$w_{\zeta_{p^{r+1}}}(\infty) = w_{\zeta_{p^{r+1}}}(\mathrm{Tate}(q), \zeta_m, \zeta_{p^{r+1}}) = (\mathrm{Tate}(q^{p^{r+1}}), \zeta_m^{p^{r+1}}, q) = \infty'.$$

Proceeding as in the Main Lemma 1, we deduce that there exists a unique Katz cusp form $f' \in S(m,p^{r+1},k)_{\overline{\mathbb{F}}_\ell}$ such that $w_{\zeta_{p^{r+1}}}(f') = f$: by direct computation at the standard cusp, we have that for all positive integers j

$$a_j(f')p^{(r+1)k} = a_j(f),$$

hence $f'(\mathrm{Tate}(q), \zeta_m, \zeta_{p^{r+1}}) \in \overline{\mathbb{F}}_\ell\,[[q^p]]\,((dt)/t)^{\otimes k}$. As in the Main Lemma 1,

on the modular curves there is a natural action on the level structure:



where

$$\overline{\Gamma_1(p^r)}\colon = \left\{ \begin{pmatrix} 1+p^r\cdot a & b \\ p^r\cdot c & 1+p^r\cdot d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z}) \right\}.$$

In analogy with Main Lemma 1, there exists $g \in S(m,p^r,k)_{\overline{\mathbb{F}}_\ell}$ such that $B_p^* g = f$ if and only if $\gamma^* f'$ is $\overline{\Gamma_1(p^r)}$-invariant. Since the set $\left\{ \left(\begin{smallmatrix}1 & 0\\ p^r & 1\end{smallmatrix}\right), \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right) \right\}$ generates $\overline{\Gamma_1(p^r)}$ by Lemma A.2.1, it is enough to show the invariance for the generators.

The map $\gamma : X(\Gamma_1(m),\Gamma(p^{r+1})^{\zeta_{p^{r+1}}-\mathrm{can}})_{\overline{\mathbb{F}}_\ell} \to X(\Gamma_1(m),\Gamma(p^{r+1}))_{\overline{\mathbb{F}}_\ell}$ corresponds to the action of elements of the form $\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}/p^{r+1}\mathbb{Z})$ and $\gamma^* f'$ is invariant under the action of such elements by construction. The action of $\left(\begin{smallmatrix}1 & 0\\ p^r & 1\end{smallmatrix}\right)$ fixes $\infty' \in X(\Gamma_1(m),\Gamma(p^{r+1})^{\zeta_{p^{r+1}}-\mathrm{can}})_{\overline{\mathbb{F}}_\ell}$ and it acts on the complete local ring at ∞', $\overline{\mathbb{F}}_\ell[[q]]$, as:

$$\begin{cases} \text{identity on } \overline{\mathbb{F}}_\ell \\ q \mapsto \zeta_{p^{r+1}}^{p^r} q = \zeta_p q \end{cases},$$

then, by definition, $\left(\begin{smallmatrix}1 & 0\\ p^r & 1\end{smallmatrix}\right)$ acts on $\overline{\mathbb{F}}_\ell[[q]](dt/t)^{\otimes k}$ by $t \mapsto t$.

Since $a_j(f') = 0$ for all positive integers j not divisible by p, then $\left(\begin{smallmatrix}1 & 0\\ p^r & 1\end{smallmatrix}\right)^* f'$ has the same q-expansion as f'. Now, since $X(\Gamma_1(m),\Gamma(p^{r+1})^{\zeta_{p^{r+1}}-\mathrm{can}})_{\overline{\mathbb{F}}_\ell}$ is an irreducible reduced curve, this means that $\left(\begin{smallmatrix}1 & 0\\ p^r & 1\end{smallmatrix}\right)^* \gamma^* f' = \gamma^* f'$. The uniqueness of the modular form $g \in S(m,p^r,k)_{\overline{\mathbb{F}}_\ell}$ such that $B_p^* g = f$ follows, as in the previous lemma, by the q-expansion principle. □

In the previous main lemmas, we have not used the action of diamond operators. First of all, let us recall briefly how this operators are defined. For $n > 4$, and for all $d \in (\mathbb{Z}/n\mathbb{Z})^*$, we define an automorphism

$$\begin{array}{rcl} r_d : X(n)_{\overline{\mathbb{F}}_\ell} & \to & X(n)_{\overline{\mathbb{F}}_\ell} \\ (E,P) & \mapsto & r_d(E,P) = (E,dP) \end{array}$$

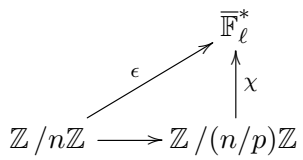
for all generalized elliptic curves E together with a $\Gamma_1(n)$-structure P. The diamond operator $\langle d\rangle$ on $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ for every $d \in (\mathbb{Z}/n\mathbb{Z})^*$ is defined as the automorphism of $M(\Gamma_1(n),k)_{\overline{\mathbb{F}}_\ell}$ induced by pullback via the automorphism r_d. If we are dealing with Katz cusp forms with a character $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$, we are imposing that for all $d \in (\mathbb{Z}/n\mathbb{Z})^*$, the diamond operator $\langle d\rangle$ acts as $\epsilon(d)$.

If we take this into account, we have an analogous to Main Lemma 1 and Main Lemma 2 for forms in $S(n,k,\epsilon)_{\overline{\mathbb{F}}_\ell}$.

Lemma A.2.3. *Let n and k be positive integers. Let ℓ and p be primes such that p divides n and $n/p > 4$, while ℓ does not divide n and $1 \leq k \leq \ell+1$. Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ and $\chi : (\mathbb{Z}/(n/p)\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be characters.*

Let f and g be mod ℓ *cusp forms in $S(n,k,\epsilon)_{\overline{\mathbb{F}}_\ell}$ and in $S(n/p,k,\chi)_{\overline{\mathbb{F}}_\ell}$ respectively, such that $B_p^*(g) = f$, where B_p^* is the morphism induced by the degeneracy map $B_p : X_1(n)_{\overline{\mathbb{F}}_\ell} \to X_1(n/p)_{\overline{\mathbb{F}}_\ell}$. Then*

$$\chi = \mathrm{Res}^{\mathbb{Z}/(n/p)\mathbb{Z}}_{\mathbb{Z}/n\mathbb{Z}}(\epsilon)$$



i.e. for all $d \in \mathbb{Z}/(n/p)\mathbb{Z}$ we have $\chi(d) = \epsilon(d)$.

Proof. Let E/S be an elliptic curve over an $\overline{\mathbb{F}}_\ell$-scheme S, let P be a point of order n, and let B_p be the degeneracy map $B_p : X_1(n)_{\overline{\mathbb{F}}_\ell} \to X_1(n/p)_{\overline{\mathbb{F}}_\ell}$ defined in (A.1) through the isogeny β then

$$(B_p^* g)(E,P) = \beta^*(g(E/\langle (n/p)P\rangle, \beta(P))).$$

The action of the diamond operator $\langle d\rangle$ for $d \in \mathbb{Z}/(n/p)\mathbb{Z}$ is given by

$$\begin{aligned}\langle d\rangle (B_p^* g)(E,P) = (B_p^* g)(E,dP) &= \beta^*(g(E/\langle (n/p)P\rangle, \beta(dP))) = \\ &= \beta^*(g(E/\langle (n/p)P\rangle, d\beta(P))) = \\ &= \beta^*(\chi(d) g(E/\langle (n/p)P\rangle, \beta(P))) = \chi(d)(B_p^* g)(E,P);\end{aligned}$$

hence, for all $d \in \mathbb{Z}/(n/p)\mathbb{Z}$ we have $\langle d\rangle (B_p^* g) = \chi(d)(B_p^* g)$. Since $B_p^*(g) = f$, then for all $d \in \mathbb{Z}/(n/p)\mathbb{Z}$ it follows that $\langle d\rangle f = \chi(d) f = \epsilon(d) f$. Hence, for all $d \in \mathbb{Z}/(n/p)\mathbb{Z}$ the equality $\chi(d) = \epsilon(d)$ holds. □

Applying this lemma, we have the following:

Corollary of Main Lemma 1. *Let n and k be positive integers. Let ℓ and p be primes such that p strictly divides n and $n/p > 4$, while ℓ does not divide*

n and $1 \leq k \leq \ell+1$. Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be a character. Let f be a mod *ℓ cusp form in $S(n/p, p, k, \epsilon)_{\overline{\mathbb{F}}_\ell}$ such that*

$$f(\mathrm{Tate}(q), \zeta_{n/p}, \zeta_p) = \sum_{j \geq 1} a_j(f) q^j \left(\frac{dt}{t}\right)^{\otimes k} \in \overline{\mathbb{F}}_\ell\left[[q^p]\right] \left(\frac{dt}{t}\right)^{\otimes k}$$

where $\mathrm{Tate}(q)$ is the Tate curve over $\overline{\mathbb{F}}_\ell((q))$, $\zeta_{n/p}$ and ζ_p are respectively fixed n/p-th and p-th roots of unity. Then there exists a unique form $g \in S(n/p, k, \epsilon')_{\overline{\mathbb{F}}_\ell}$, such that $B_p^* g = f$, where B_p^* is the morphism induced by the degeneracy map $B_p : X_1(n)_{\overline{\mathbb{F}}_\ell} \to X_1(n/p)_{\overline{\mathbb{F}}_\ell}$ and $\epsilon' = \mathrm{Res}^{\mathbb{Z}/(n/p)\mathbb{Z}}_{\mathbb{Z}/n\mathbb{Z}}(\epsilon)$.

Corollary of Main Lemma 2. *Let n and k be positive integers. Let ℓ and p be primes such that $n = mp^{r+1}$ with p and m coprime, $r \in \mathbb{Z}_{\geq 1}$ and $mp^r > 4$, while ℓ does not divide n and $1 \leq k \leq \ell+1$. Let $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be a character. Let f be a* mod *ℓ cusp form in $S(m, p^{r+1}, k, \epsilon)_{\overline{\mathbb{F}}_\ell}$ such that*

$$f(\mathrm{Tate}(q), \zeta_m, \zeta_{p^{r+1}}) = \sum_{j \geq 1} a_j(f) q^j \left(\frac{dt}{t}\right)^{\otimes k} \in \overline{\mathbb{F}}_\ell\left[[q^p]\right] \left(\frac{dt}{t}\right)^{\otimes k}$$

where $\mathrm{Tate}(q)$ is the Tate curve over $\overline{\mathbb{F}}_\ell((q))$, ζ_m and $\zeta_{p^{r+1}}$ are respectively fixed m-th and p^{r+1}-th roots of unity. Then there exists a unique form $g \in S(m, p^r, k, \epsilon')_{\overline{\mathbb{F}}_\ell}$, such that $B_p^* g = f$, where B_p^* is the morphism induced by the degeneracy map $B_p : X_1(m, p^{r+1})_{\overline{\mathbb{F}}_\ell} \to X_1(m, p^r)_{\overline{\mathbb{F}}_\ell}$ and and $\epsilon' = \mathrm{Res}^{\mathbb{Z}/(mp^r)\mathbb{Z}}_{\mathbb{Z}/n\mathbb{Z}}(\epsilon)$.

Remark A.2.4. In Main Lemma 1 and 2, and also in the corollaries above, we assume that the prime p, dividing the level n, is such that the quotient $n/p > 4$. This hypothesis implies that all the objects used in the proofs are modular curves. Without such hypothesis, we should use the theory of algebraic stacks: for level n smaller than 4, the algebraic object $X(\Gamma_1(n))_{\overline{\mathbb{F}}_\ell}$ is an algebraic stack, see [Con07, Theorem 1.2.1], and dealing with such objects is beyond our purposes. It is highly likely that this condition can be removed.

A.3 Optimization

Theorem A.3.1. *Let n and k be positive integers. Let ℓ be a prime not dividing n, such that $2 \leq k \leq \ell+1$. Let $f : \mathbb{T}_\epsilon \to \overline{\mathbb{F}}_\ell$ be a ring homomorphism from the Hecke algebra of level n, weight k and nebentypus $\epsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$, to $\overline{\mathbb{F}}_\ell$. Let $T_p \in \mathbb{T}_\epsilon$ be the p-th Hecke operator and $\overline{\epsilon} : (\mathbb{Z}/n\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell^*$ be the character defined by $a \mapsto f(\langle a \rangle)$ for all $a \in (\mathbb{Z}/n\mathbb{Z})^*$. Let us suppose that there exists a prime m dividing $n\ell$ such that the $\overline{\mathbb{F}}_\ell$-vector space*

$$V :\, = \bigcap_{p \neq m} \ker\left(T_p - f(T_p), S(n, k, \overline{\epsilon})_{\overline{\mathbb{F}}_\ell}\right),$$

has dimension bigger than 1.

If m is different from ℓ then there exists a mod ℓ cusp form g in $S(n/m, k, \mathrm{Res}(\epsilon))_{\overline{\mathbb{F}}_\ell}$ such that $B_m^* g = f$. If $m = \ell$ then $k \in \{\ell, \ell+1\}$; in the first case there exists a mod ℓ cusp form g in $S(n, 1, \epsilon)_{\overline{\mathbb{F}}_\ell}$ such that $F(g) = f$, where F is the Frobenius, while in the second case there exists a mod ℓ cusp form g in $S(n, 2, \epsilon)_{\overline{\mathbb{F}}_\ell}$ such that $A_\ell g = f$, where A_ℓ is the Hasse invariant.

Proof. Let v be the dimension of V, by hypothesis $v > 1$. As T_m commutes with all T_p, T_m acts on V, and since $v > 1$ hence V contains a non-zero eigenvector f for all T_p, $p \geq 1$, in particular $a_1(f) \neq 0$.

The subspace $V_1 \subset V$ consisting of the g in V with $a_1(g) = 0$ is of dimension $v - 1 > 0$. Every element $g \in V_1$ is such that $0 = a_1(g) = a_1(T_j(g))$ for all integer j not divisible by m.

This means that g is an eigenform with q-expansion in $\mathbb{F}\left[\left[q^m\right]\right]\left((dt)/t\right)^{\otimes k}$ at the standard cusp.

Let us first suppose $m \neq \ell$. By assumptions $n/m > 4$, then we are in the hypotheses of the Main Lemmas, so there exists a non zero modℓ modular form $g' \in S(n/m, k, \epsilon')_{\overline{\mathbb{F}}_\ell}$ such that $B_p^* g' = g$, where $\epsilon' = \mathrm{Res}(\epsilon)$ and B_p^* is the morphism induced by the degeneracy map B_p defined in (A.1). This means that $V_1 = B_p^* V_2$ where V_2 is the eigenspace of $S(n, k, \overline{\epsilon})_{\overline{\mathbb{F}}_\ell}$ associated to the system of eigenvalues

$$\begin{aligned} f_{n,k}^{\{m\}} \colon = f_{n,k}|_{\mathcal{P}\setminus\{m\}} \colon \{\mathcal{P} \setminus \{m\}\} &\to \overline{\mathbb{F}}_\ell \times \overline{\mathbb{F}}_\ell \\ p &\mapsto (f(T_p), f(\langle p \rangle)) \end{aligned}$$

Hence the system of eigenvalues $f_{n,k}^{\{m\}}$ occurs in level n/m.

Let us suppose $m = \ell$. As proved in [Edi06, Proposition 6.2], the only two following cases occur. First case: $k = \ell$. The form g, constructed as before, is in the image of the Frobenius F, i.e. there exists $g' \in S(n, 1, \epsilon)_{\mathbb{F}}$ such that $g = (g')^\ell = F(g')$. This means that the system of eigenvalues occurs already in weight 1. Second case: $k = \ell + 1$. We have that $g = A_\ell g'$ where A_ℓ is the Hasse invariant of weight $\ell - 1$ and $g' \in S(n, 2, \epsilon)_{\mathbb{F}}$, hence the system of eigenvalues occurs in weight 2. □

From the previous theorem we deduce the following result:

Corollary A.3.2. *In the same hypotheses of Theorem A.3.1, the Galois representation attached to f in Corollary 4.0.5, $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ arises from a lower level or weight.*

Moreover, we have that:

Corollary A.3.3. *In the same hypotheses of Theorem A.3.1, if $m \neq \ell$ then the dimension of V is at most $a+1$ where a is such that $m^a \operatorname{cond}(\rho_f) = n$.*

Proof. The subspace $V_1 \subset V$ consisting of the g in V with $a_1(g) = 0$ is of co-dimension 1 in V. Every element $g \in V_1$ is such that $0 = a_1(g) = a_1(T_j(g))$ for all integer j not divisible by m. This means that g is an eigenform with q-expansion in $\mathbb{F}\left[[q^m]\right]((dt)/t)^{\otimes k}$ at the standard cusp. The hypotheses of the Main Lemmas are satisfied, so there exists a non zero modℓ modular form $g' \in S(n/m, k, \operatorname{Res}(\epsilon))_{\overline{\mathbb{F}}_\ell}$ such that $B_p^* g' = g$. This means that $V_1 = B_p^* V_2$ where V_2 is the eigenspace of $S(n, k, \overline{\epsilon})_{\overline{\mathbb{F}}_\ell}$ associated to the system of eigenvalues $f_{n,k}^{\{m\}}$. We recursively apply the previous argument to the subspace V_1. This can be iterated at most a-times where a is the biggest power of m dividing $\operatorname{cond}(\rho_f)$. □

Bibliography

[Ann13] Samuele Anni. A local-global principle for isogenies of prime degree over number fields. `http://arxiv.org/pdf/1303.3809.pdf`, 2013.

[BD12] Nicolas Billerey and Luis V. Dieulefait. Explicit Large Image Theorems for Modular Forms. `http://arxiv.org/pdf/1210.5428v1.pdf`, 2012.

[Bea10] Arnaud Beauville. Finite subgroups of $\mathrm{PGL}_2(K)$. In *Vector bundles and complex geometry*, volume 522 of *Contemp. Math.*, pages 23–29. Amer. Math. Soc., Providence, RI, 2010.

[Ber06] Jacob Bernoulli. *The art of conjecturing.* Johns Hopkins University Press, Baltimore, MD, 2006. Together with "Letter to a friend on sets in court tennis", Translated from the Latin and with an introduction and notes by Edith Dudley Sylla.

[BK75] Bryan J. Birch and Willem Kuyk. *Modular functions of one variable. IV.* Lecture Notes in Mathematics, Vol. 476. Springer-Verlag, Berlin, 1975.

[Bos11] Johan Bosman. Modular forms applied to the computational inverse galois problem. `http://arxiv.org/pdf/1109.6879v1.pdf`, 2011.

[BS02] Kevin Buzzard and William A. Stein. A mod five approach to modularity of icosahedral Galois representations. *Pacific J. Math.*, 203(2):265–282, 2002.

[Buz00] Kevin Buzzard. On level-lowering for mod 2 representations. *Math. Res. Lett.*, 7(1):95–110, 2000.

[Car59a] Leonard Carlitz. Arithmetic properties of generalized Bernoulli numbers. *J. Reine Angew. Math.*, 202:174–182, 1959.

[Car59b] Leonard Carlitz. Some arithmetic properties of generalized Bernoulli numbers. *Bull. Amer. Math. Soc.*, 65:68–69, 1959.

[Car86] Henri Carayol. Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)*, 19(3):409–468, 1986.

[Car89] Henri Carayol. Sur les représentations galoisiennes modulo l attachées aux formes modulaires. *Duke Math. J.*, 59(3):785–801, 1989.

[CH05] Alina C. Cojocaru and Chris Hall. Uniform results for Serre's theorem for elliptic curves. *International Mathematics Research Notices*, (50):3065–3080, 2005.

[CKR10] Imin Chen, Ian Kiming, and Jonas B. Rasmussen. On congruences mod $\mathfrak{p}^m$ between eigenforms and their attached Galois representations. *J. Number Theory*, 130(3):608–619, 2010.

[Con07] Brian Conrad. Arithmetic moduli of generalized elliptic curves. *J. Inst. Math. Jussieu*, 6(2):209–278, 2007.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. A Wiley-Interscience Publication. John Wiley & Sons Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[CR06] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1962 original.

[Del73] Pierre Deligne. Les constantes des équations fonctionnelles des fonctions L. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 501–597. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[DI95] Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994)*, volume 17 of *CMS Conf. Proc.*, pages 39–133. Amer. Math. Soc., Providence, RI, 1995.

[Dia97] Fred Diamond. An extension of Wiles' results. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 475–489. Springer, New York, 1997.

[Dic58] Leonard E. Dickson. *Linear groups: With an exposition of the Galois field theory*. with an introduction by W. Magnus. Dover Publications Inc., New York, 1958.

[Die71] Jean A. Dieudonné. *La géométrie des groupes classiques*. Springer-Verlag, Berlin, 1971. Troisième édition, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 5.

[DR73] Pierre Deligne and Michael Rapoport. Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 143–316. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[DS74] Pierre Deligne and Jean-Pierre Serre. Formes modulaires de poids 1. *Ann. Sci. École Norm. Sup. (4)*, 7:507–530, 1974.

[DS05] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[EC11] Bas Edixhoven and Jean-Marc Couveignes, editors. *Computational aspects of modular forms and Galois representations*, volume 176 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2011. How one can compute in polynomial time the value of Ramanujan's tau at a prime.

[Edi92] Bas Edixhoven. The weight in Serre's conjectures on modular forms. *Invent. Math.*, 109(3):563–594, 1992.

[Edi97] Bas Edixhoven. Serre's conjecture. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 209–242. Springer, New York, 1997.

[Edi06] Bas Edixhoven. Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one. *J. Inst. Math. Jussieu*, 5(1):1–34, 2006. With appendix A (in French) by Jean-François Mestre and appendix B by Gabor Wiese.

[Fab11] Xander Faber. Finite p-irregular subgroups of $\mathrm{PGL}(2, k)$. `http://arxiv.org/pdf/1112.1999v2.pdf`, 2011.

[FH91] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[Gor02] Eyal Z. Goren. *Lectures on Hilbert modular varieties and modular forms*, volume 14 of *CRM Monograph Series*. American Mathematical Society, Providence, RI, 2002. With the assistance of Marc-Hubert Nicole.

[Gro90] Benedict H. Gross. A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Math. J.*, 61(2):445–517, 1990.

[Hid93] Haruzo Hida. *Elementary theory of L-functions and Eisenstein series*, volume 26 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1993.

[Kat73] Nicholas M. Katz. p-adic properties of modular schemes and modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 69–190. Lecture Notes in Mathematics, Vol. 350. Springer, Berlin, 1973.

[Kat77] Nicholas M. Katz. A result on modular forms in characteristic p. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 53–61. Lecture Notes in Math., Vol. 601. Springer, Berlin, 1977.

[Kat81] Nicholas M. Katz. Galois properties of torsion points on abelian varieties. *Inventiones mathematicae*, 62:481–502, 1981.

[KM85] Nicholas M. Katz and Barry Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[Koh04] Winfried Kohnen. On Fourier coefficients of modular forms of different weights. *Acta Arith.*, 113(1):57–67, 2004.

[Kra90] Alain Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta Math.*, 69(4):353–385, 1990.

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. I. *Invent. Math.*, 178(3):485–504, 2009.

[KW09b] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture. II. *Invent. Math.*, 178(3):505–586, 2009.

[Lan76] Serge Lang. *Introduction to modular forms.* Springer-Verlag, Berlin, 1976.

[Liv89] Ron Livné. On the conductors of mod l Galois representations coming from modular forms. *J. Number Theory*, 31(2):133–141, 1989.

[Maz77a] Barry Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[Maz77b] Barry Mazur. Rational points on modular curves. In Jean-Pierre Serre and DonBernard Zagier, editors, *Modular Functions of one Variable V*, volume 601 of *Lecture Notes in Mathematics*, pages 107–148. Springer Berlin Heidelberg, 1977.

[Maz11] Barry Mazur. How can we construct abelian Galois extensions of basic number fields? *Bull. Amer. Math. Soc. (N.S.)*, 48(2):155–209, 2011.

[Miy06] Toshitsune Miyake. *Modular forms.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda.

[Par99] Pierre J. R. Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999.

[Par05] Pierre J. R. Parent. Towards the triviality of $X_0^+(p^r)(\mathbb{Q})$ for $r > 1$. *Compos. Math.*, 141(3):561–572, 2005.

[PT07] Ariel Pacetti and Gonzalo Tornaría. Examples of the Shimura correspondence for level p^2 and real quadratic twists. In *Ranks of elliptic curves and random matrix theory*, volume 341 of *London Math. Soc. Lecture Note Ser.*, pages 289–314. Cambridge Univ. Press, Cambridge, 2007.

[Que95] Jordi Quer. Liftings of projective 2-dimensional galois representations and embedding problems. *J. of Algebra*, 171(2):541 – 566, 1995.

[Ras09] Jonas B. Rasmussen. *Higher congruences between modular forms.* PhD thesis, 2009. `http://www.math.ku.dk/~jonas/Thesis.pdf`.

[Rib76a] Kenneth A. Ribet. Galois action on division points of Abelian varieties with real multiplications. *Amer. J. Math.*, 98(3):751–804, 1976.

[Rib76b] Kenneth A. Ribet. A modular construction of unramified p-extensions of $Q(\mu_p)$. *Invent. Math.*, 34(3):151–162, 1976.

[Rib85] Kenneth A. Ribet. On l-adic representations attached to modular forms. II. *Glasgow Math. J.*, 27:185–194, 1985.

[Rib94] Kenneth A. Ribet. Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 639–676. Amer. Math. Soc., Providence, RI, 1994.

[Rob96] Derek J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.

[Sch12] George J. Schaeffer. *The Hecke Stability Method and Ethereal Forms*. PhD thesis, 2012. `http://www.math.ucla.edu/~gschaeff/schaeffer-thesis.pdf`.

[Ser66] Jean-Pierre Serre. Groupes de Lie l-adiques attachés aux courbes elliptiques. In *Les Tendances Géom. en Algébre et Théorie des Nombres*, pages 239–256. Éditions du Centre National de la Recherche Scientifique, Paris, 1966.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15:259–331, 1972.

[Ser77a] Jean-Pierre Serre. *Cours d'arithmétique*. Presses Universitaires de France, Paris, 1977. Deuxième édition revue et corrigée, Le Mathématicien, No. 2.

[Ser77b] Jean-Pierre Serre. Modular forms of weight one and Galois representations. In *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, pages 193–268. Academic Press, London, 1977.

[Ser78] Jean-Pierre Serre. *Représentations linéaires des groupes finis*. Hermann, Paris, revised edition, 1978.

[Ser87] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[Ser94] Jean-Pierre Serre. Sur la semi-simplicité des produits tensoriels de représentations de groupes. *Invent. Math.*, 116(1-3):513–530, 1994.

[Ser95] Jean-Pierre Serre. Corps locaux et isogénies. In *Séminaire Bourbaki, Vol. 5*, pages Exp. No. 185, 239–247. Soc. Math. France, Paris, 1995.

[Shi71] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, 1971. Kanô Memorial Lectures, No. 1.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[Sri79] Bhama Srinivasan. *Representations of finite Chevalley groups*, volume 764 of *Lecture Notes in Mathematics*. Springer-Verlag, Berlin, 1979. A survey.

[Ste07] William Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells.

[Stu87] Jacob Sturm. On the congruence of modular forms. In *Number theory (New York, 1984–1985)*, volume 1240 of *Lecture Notes in Math.*, pages 275–280. Springer, Berlin, 1987.

[Sut12] Andrew V. Sutherland. A local-global principle for rational isogenies of prime degree. *J. Théor. Nombres Bordeaux*, 24(2):475–485, 2012.

[Tak11] Yuuki Takai. An effective isomorphy criterion for mod ℓ Galois representations. *J. Number Theory*, 131(8):1409–1419, 2011.

[Vig89] Marie-France Vignéras. Correspondance modulaire galois-quaternions pour un corps p-adique. In *Number theory (Ulm, 1987)*, volume 1380 of *Lecture Notes in Math.*, pages 254–266. Springer, New York, 1989.

[Wal81] Jean-Loup Waldspurger. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl. (9)*, 60(4):375–484, 1981.

[Wie04] Gabor Wiese. Dihedral Galois representations and Katz modular forms. *Doc. Math.*, 9:123–133 (electronic), 2004.

[Wie05] Gabor Wiese. *Modular Forms of Weight One Over Finite Fields*. PhD thesis, 2005.

List of Notations

χ_ℓ	modℓ cyclotomic character, page 27
$\mathbb{F}_\ell$	finite field with ℓ elements, page 4
$\Gamma_0(n)$	subgroup of $\mathrm{SL}_2(\mathbb{Z})$ whose elements reduce to $\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)$ mod n, page 52
$\Gamma_1(n)$	subgroup of $\mathrm{SL}_2(\mathbb{Z})$ whose elements reduce to $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$ mod n, page iii
$\mathbb{P}^1(\mathbb{F}_\ell)^g$	set of elements fixed by g, page 5
$\mathbb{P}^1(\mathbb{F}_\ell)/g$	set of g-orbits of $\mathbb{P}^1(\mathbb{F}_\ell)$, page 5
$\mathfrak{A}_n$	alternating group on n-elements, page 9
$\mathfrak{S}_n$	symmetric group on n-elements, page 9
$\mathrm{N}(\rho)$	Artin conductor of ρ, page 33
$\mathrm{N}_p(\rho)$	valuation of $\mathrm{N}(\rho)$ at p, page 33
$\mathbb{T}(n,k)$	cuspidal Hecke algebra, page 25
$\mathbb{T}_\epsilon(n,k)$	cuspidal Hecke algebra related to $S(n,k,\epsilon)_{\mathbb{C}}$, page 25
θ_ℓ	$q\,d/dq$ operator, page 32
A_ℓ	Hasse invariant in characteristic ℓ, page 31
$B(n,k)$	Sturm bound, page 51
B_k^χ	k-th generalized Bernoulli number, page 69
B_p	p-th degeneracy map, page 53
e_β	Weil pairing related to the isogeny β, page 131
$f_{n,k}$	system of eigenvalues, page 50
$f_{n,k}^{(*)}$	system of eigenvalues truncated at $(*)$, page 65
$G_{\mathbb{Q}}$	absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, page i
$k(\rho)$	minimal weight of the representation ρ, page 33
$M(n,k)_{\mathbb{C}}$	complex vector space of weight k modular forms on $\Gamma_1(n)$, page 25
$M(n,k)_{\overline{\mathbb{F}}_\ell}$	Katz modular forms of weight k for $\Gamma_1(n)$ on $\overline{\mathbb{F}}_\ell$, page 30
$S(n,k,\epsilon)_{\mathbb{C}}$	complex vector space of weight k, level n cusp forms with character, page 25

$S(n,k)_{\mathbb{C}}$	complex vector space of weight k cusp forms on $\Gamma_1(n)$, page 25
$S(n,k)_{\overline{\mathbb{F}}_\ell}$	Katz cusp forms of weight k for $\Gamma_1(n)$ on $\overline{\mathbb{F}}_\ell$, page 30
V_4	Klein 4-group, page 20
$w_{\zeta_{p^r}}$	Atkin-Lehner map, page 131
$X(\ell)$	modular curve, page 17
$X_0(\ell)$	modular curve related to the Borel subgroup, page 18
$X_{\mathfrak{A}_4}(\ell)$, $X_{\mathfrak{S}_4}(\ell)$, $X_{\mathfrak{A}_5}(\ell)$	modular curves related to the exceptional subgroups, page 18
$X_{\mathrm{sp.Car}}(\ell)$	modular curve related to the split Cartan subgroup, page 4
$X_{\mathrm{split}}(\ell)$	modular curve related to the normalizer of a split Cartan subgroup, page 4
$X_{V_4}(\ell)$	modular curve related to V_4, page 20

Index

List of Algorithms