L-functions of Universal Elliptic Curves Over Igusa Curves

Douglas L. Ulmer
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, MA 02139

This paper is concerned with computing the L-functions of the title in terms of modular forms. Because one can produce zeros of these L-functions, they seem to provide interesting test cases for various conjectures relating L-functions to cycles.

In the first three sections we state the theorem, review some consequences, and give a brief sketch of the proof. This proof is based on recent results of Katz and Mazur, so in sections 4 through 6 we establish notation by reviewing the relevant parts of their work. In sections 7 and 8 we prove an Eichler-Shimura style result on a Hecke operator. The proof proper occupies sections 9 through 12. The paper [11] provides an introduction to the universal curves over Igusa curves.

The theorem and some consequences

1. Statement of the theorem. Fix a prime p, an extension $\mathbf{F}_q$ of the field of p elements $\mathbf{F}_p$, and an integer n so that $p^n \geq 3$. Let K_n be the function field of the Igusa curve of level p^n over $\mathbf{F}_q$. The field K_n is an extension of degree $(p^n - p^{n-1})/2$ of the rational function field $\mathbf{F}_q(j)$. There is a unique elliptic curve E over K_n whose modular invariant is j and such that $E^{(p^n)}$ has p^n points of order p^n rational over K_n. For each non-negative integer d, let E^d be the d-fold self product of E over K_n. We will be interested in the L-functions associated to the cohomology groups of E^d.

Fix a separable closure $\overline{K}_n$ of the function field K_n and let $G = \mathrm{Gal}(\overline{K}_n/K_n)$. For each prime $\ell \neq p$, one has the étale cohomology group $H^i(E^d \otimes \overline{K}_n, \mathbf{Q}_\ell)$; it is a finite dimensional $\mathbf{Q}_\ell$ vector space. The group G acts on $E^d \otimes \overline{K}_n$ and one obtains a linear representation

$$\rho_i : G \to \mathrm{Aut}_{\mathbf{Q}_\ell}(H^i(E^d \otimes \overline{K}_n, \mathbf{Q}_\ell)).$$

For each place v of K_n, let $\deg(v)$ be its degree, D_v a decomposition group at v and I_v the inertia subgroup of D_v. The quotient D_v/I_v is isomorphic to $\hat{\mathbf{Z}}$, and has a canonical topological generator F_v, the Frobenius element at v. Define, as usual, the L function associated to the representation ρ_i by

$$L(\rho_i, s) = \prod_v \det\left(1 - \rho_i(F_v^{-1}) q^{-\deg(v)s} | H^i(E^d \otimes \overline{K}_n, \mathbf{Q}_\ell)^{I_v}\right)^{-1}.$$

This product converges absolutely, as a function of the complex variable s, in the half plane $\mathrm{Re}\ s > \frac{i}{2} + 1$, and is independent of the choice of ℓ. It is known to have a

meromorphic extension to the entire plane and to satisfy a functional equation ([3], or [5], VI.11-13).

Before stating the main theorem we make a preliminary reduction. First of all by the Künneth formula,

$$H^1(E^d \otimes \overline{K}_n, \mathbf{Q}_\ell) \cong H^1(E \otimes \overline{K}_n, \mathbf{Q}_\ell)^{\oplus^d},$$

and, as for any Abelian variety,

$$H^i(E^d \otimes \overline{K}_n, \mathbf{Q}_\ell) \cong \bigwedge^i H^1(E^d \otimes \overline{K}_n, \mathbf{Q}_\ell).$$

But for any irreducible two dimensional representation $\rho : G \to \mathrm{Aut}(H)$ of G, there is an isomorphism

$$\bigwedge^i (H^{\oplus^d}) \cong \bigoplus_{j=0}^{i/2} \left(\mathrm{Sym}^{i-2j} H \otimes (\wedge^2 H)^{\otimes^j} \right)^{c_{i,j,d}}$$

where the multiplicities are

$$c_{i,j,d} = \binom{d}{j}\binom{d}{i-j} - \binom{d}{j-1}\binom{d}{i-(j-1)}.$$

(Here and from now on we assume that $i \leq d$; the case $i > d$ can be handled similarly or by using the functional equation.) Now setting $H = H^1(E \otimes \overline{K}_n, \mathbf{Q}_\ell)$ and $\rho : \mathrm{Gal}(\overline{K}_n/K_n) \to \mathrm{Aut}_{\mathbf{Q}_\ell}(H)$ in the above isomorphism and noting that $\wedge^2 H \cong \mathbf{Q}_\ell(-1)$, we see that the L-function decomposes as a product of translates of the L-function associated to symmetric powers of H:

$$L(\rho_i, s) = \prod_{j=0}^{i/2} L(\mathrm{Sym}^{i-2j}\rho, s-j)^{c_{i,j,d}}.$$

Thus it suffices to compute the $L(\mathrm{Sym}^k \rho, s)$.

To state the theorem we need some notations related to modular forms. For χ a Dirichlet character modulo p^n, let $S_k(\Gamma_0(p^n), \chi)$ be the space of modular forms of weight k and character χ for the group $\Gamma_0(p^n)$. For every power q of p, the Hecke operator U_q acts on this finite dimensional complex vector space, and we set

$$E_q(\Gamma_1(p^n), k, s) = \prod_{cond(\chi)=p^n} \det(1 - U_q q^{-s} | S_k(\Gamma_0(p^n), \chi))$$

where $n \geq 1$ and the product is over the characters of maximal conductor modulo p^n. Similarly, the Hecke operator T_q acts on $S_k(\Gamma_0(1))$, and we set

$$E_q(\Gamma_1(1), k, s) = \det(1 - T_q q^{-s} + q^{k-1-2s} | S_k(\Gamma_0(1))).$$

Combining all these, put

$$H_q(\Gamma_1(p^n), k, s) = \prod_{m=0}^{n} E_q(\Gamma_1(p^m), k, s).$$

These products of Euler factors are the basic ingredients in the L-functions of the universal curves.

Theorem. *Let K_n be the function field of the Igusa curve of level p^n over the field $\mathbf{F}_q$ and let E be the universal curve over K_n. If*

$$\rho : Gal(\overline{K}_n / K_n) \to H^1(E \otimes \overline{K}_n, \mathbf{Q}_\ell)$$

is the usual representation of the Galois group on ℓ-adic étale cohomology, then

$$L(Sym^k \rho, s) = H_q(\Gamma_1(p^n), k+2, s)$$

for $k \geq 1$, while for $k = 0$,

$$L(Sym^0\rho, s) = \frac{H_q(\Gamma_1(p^n), 2, s)}{(1 - q^{-s})(1 - q^{1-s})}.$$

Remarks: 1) Of course $\mathrm{Sym}^0\rho \cong \mathbf{Q}_\ell$ so the L-function is just the zeta-function of the field K_n.

2) The case $k = 0$, $n = 1$ also follows from Wiles [12], thm. 5.4.

3) We will actually prove somewhat more in that prime to p level structure will be allowed; see section 9.

2. Consequences. The main interest of this theorem is that one can use results about modular forms to study the L-function. First, note that $L(\rho_i, s)$ is a rational function in q^{-s} and so meromorphic in the plane. By a theorem of Ogg ([6], cor. 1 of thm. 4), the zeroes of $L(\rho_i, s)$ lie on the line $\mathrm{Re}\ s = (i+1)/2$. Evidently $L(\rho_i, s)$ is holomorphic for odd i and for even i has a pole of order $\binom{d}{i/2}^2 - \binom{d}{\frac{i}{2}-1}\binom{d}{\frac{i}{2}+1}$ at $s = i/2$ and at $s = (i/2) + 1$.

Now the order of poles of the L-functions for even i are related to the ranks of certain cycle groups by conjectures of Tate ([10]). He conjectures that the rank of the group of cycles of codimension $i/2$ modulo homological equivalence on E^d is equal to the order of pole of $L(\rho_i, s)$ at $s = (i/2) + 1$. This is indeed the case for E^d, since as Tate observed ([10], p. 106), there are $\binom{d}{i/2}^2 - \binom{d}{\frac{i}{2}-1}\binom{d}{\frac{i}{2}+1}$ independent cycles of codimension i on the d-fold product E^d of an elliptic curve without complex multiplication.

On the other hand, it is conjectured by Swinnerton-Dyer [9] that the order of vanishing of $L(\rho_{2i-1}, s)$ at $s = i$ for odd i should be equal to the rank of the

group $\mathrm{A}^i(E^d)$ of cycles of codimension i homologically equivalent to zero modulo rational equivalence on E^d. The existence of CM forms (see [8], lemma 3) furnishes zeroes of the $L(\rho_{2i-1}, s)$. For example, when $p \equiv 3 \pmod 4$, $p > 3$, and $\mathbf{F}_{p^2} \subseteq \mathbf{F}_q$, $L(\rho_{2i-1}, s)$ vanishes to order at least $h\binom{d}{(i-1)/2}\binom{d}{(i+1)/2}$ at $s = i$ where h is the class number of $\mathbf{Q}(\sqrt{-p})$. Some examples of the predicted cycles for small p and $d = 1$ are given in [11]; a general construction would be of great interest.

3. Sketch of the proof. Using Grothendieck's theory of L-functions, the problem is reduced to computing the action of Frobenius on the first étale cohomology group of the Igusa curve with coefficients in the sheaf associated to $\mathrm{Sym}^k \rho$. Now the good reduction theorem of Katz-Mazur identifies the subspace of this H^1 where $(\mathbf{Z}/p^n\mathbf{Z})^\times$ acts (via its natural action on the Igusa curves) through characters of maximal conductor with a similar subspace of the first étale cohomology group of the modular curve $X_1(p^n)$ in characteristic 0. The Shimura isomorphism relates the first cohomology group of this curve (in the complex topology) with coefficients in a suitable sheaf to modular forms and both of these identifications are compatible with the action of the Hecke algebra. The proper base change and comparison theorems thus allow us to compute the action of the Hecke operator U_p on the cohomology of the Igusa curve. Applying the geometric analysis of the correspondence U_p done in section 8 gives a calculation of the action of Frobenius on a subspace of the cohomology of the Igusa curve and an induction argument, using the natural projection from the Igusa curve of level p^n to the Igusa curve of level p^{n-1}, finishes the proof.

Review of arithmetic moduli.

In what follows, constant use will be made of the notations and results of Katz-Mazur [4]. For the convenience of the reader, we briefly review some essential notions.

4. Moduli problems. Let R be a ring; (Ell/R) will denote the category whose objects are elliptic curves

$$E \to S$$

over R-schemes S and whose morphisms are Cartesian diagrams

$$\begin{array}{ccc} E' & \longrightarrow & E \\ \downarrow & & \downarrow \\ S' & \xrightarrow{f} & S \end{array}$$

where f is an R-morphism. A *moduli problem* $\mathcal{P}$ on (Ell/R) is a contravariant functor from (Ell/R) to sets. Here are some basic examples:

Fix an integer N and let $E[N]$ be the subgroup scheme $\operatorname{Ker} N : E \to E$, where N is the multiplication by N isogeny of E. Then the moduli problem $[\Gamma(N)]$ on (Ell/$\mathbf{Z}$) associates to E/S the set of homomorphisms $\phi : (\mathbf{Z}/N\mathbf{Z})^2 \to E[N](S)$ from $(\mathbf{Z}/N\mathbf{Z})^2$ to the group $E[N](S)$ of S-valued points of $E[N]$ which are Drinfeld bases in the sense that

$$\sum_{(a,b)\in(\mathbf{Z}/N\mathbf{Z})^2} \phi(a,b) = E[N]$$

is an equality of effective Cartier divisors. When S is a field of characteristic zero, this coincides with the usual notion of "a basis of the points of order N on E."

The moduli problem $[\Gamma_1(N)]$ on (Ell/$\mathbf{Z}$) assigns to E/S the set of homomorphisms

$$\phi : \mathbf{Z}/N\mathbf{Z} \to E[N](S)$$

such that the effective Cartier divisor

$$\sum \phi(a)$$

is a subgroup scheme of E, or equivalently, the set of generators (in the sense of [4] 1.4.1) of cyclic subgroups of order N in E.

The problem [bal.$\Gamma_1(N)$] on (Ell/$\mathbf{Z}$) assigns to E/S the set of diagrams

$$P \in E \xrightarrow{\pi} E' \ni P'$$

where π is a cyclic S-isogeny of degree N, $P \in E[N](S)$ is a generator of $\operatorname{Ker}\pi$ and $P' \in E'[N](S)$ is a generator of the kernel of the dual isogeny π^t.

The moduli problem [$\Gamma_0(N)$] on (Ell/$\mathbf{Z}$) assigns to E/S the set of cycl.

For every E/S, the group $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ acts on the right on the set $[\Gamma(N)](S)$, compatibly with morphisms in (Ell/$\mathbf{Z}$). For any subgroup $\Gamma \subset \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, we have a quotient moduli problem $[\Gamma(N)]/\Gamma$ defined by

$$[\Gamma(N)]/\Gamma\,(E/S) = [\Gamma(N)](E/S)/\Gamma.$$

One sees that the moduli problem [bal.$\Gamma_1(N)$] is isomorphic to $[\Gamma(N)]/\Gamma$ where

$$\Gamma = \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z}) \right\},$$

$[\Gamma_1(N)]$ is isomorphic to $[\Gamma(N)]/\Gamma$ where

$$\Gamma = \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z}) \right\},$$

and $[\Gamma_0(N)]$ is isomorphic to $[\Gamma(N)]/\Gamma$ where

$$\Gamma = \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z}) \right\}$$

([4], 7.4.2). Imbedding $(\mathbf{Z}/N\mathbf{Z})^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$ in $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ via

$$(a, b) \to \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},$$

we get an action of $(\mathbf{Z}/N\mathbf{Z})^\times \times (\mathbf{Z}/N\mathbf{Z})^\times$ on the $[\mathrm{bal}.\Gamma_1(N)]$ problem. Concretely,

(a, b) sends

$$P \in E \xrightarrow{\pi} E' \ni P'$$

to

$$aP \in E \xrightarrow{\pi} E' \ni bP'.$$

Similarly, $(\mathbf{Z}/N\mathbf{Z})^\times$ acts on $[\Gamma_1(N)]$ structures, with $a \in (\mathbf{Z}/N\mathbf{Z})^\times$ sending

$$P \in E \xrightarrow{\pi} E'$$

to

$$aP \in E \xrightarrow{\pi} E'.$$

In [4] (ch. 9), a general approach to moduli problems over cyclotomic integer rings is developed. We limit ourselves to some *ad hoc* definitions. Recall ([4], 2.8) that for any (finite, locally free) isogeny $\pi : E \to E'$ of degree N, there is a canonical pairing $\langle , \rangle_\pi : \mathrm{Ker}\, \pi \times \mathrm{Ker}\, \pi^t \to \mu_N$ which makes $\mathrm{Ker}\, \pi$ and $\mathrm{Ker}\, \pi^t$ Cartier dual group schemes. Using this, we define a moduli problem $[\mathrm{bal}.\Gamma_1(p^n)]^{can}$ on $(\mathrm{Ell}/\mathbf{Z}[\zeta_{p^n}])$ which assigns to $E/S/\mathbf{Z}[\zeta_{p^n}]$ the set of $[\mathrm{bal}.\Gamma_1(p^n)]$ structures

$$P \in E \xrightarrow{\pi} E' \ni P'$$

such that $\langle P, P' \rangle_\pi = \zeta_{p^n}$. The $[\Gamma_1(p^n)]^{can}$ problem on (Ell/$\mathbf{Z}$) turns out to be equal to the $[\Gamma_1(p^n)]$ problem. Note that, for any $\mathbf{Z}[\zeta_{p^n}]$-algebra of characteristic $\neq p$, the moduli problems $[\Gamma_1(p^n)]^{can}$ and $[\mathrm{bal}.\Gamma_1(p^n)]^{can}$ are isomorphic on (Ell/R): given a $[\Gamma_1(p^n)]^{can}$ structure on $E/S/R$

$$P \in E \xrightarrow{\pi} E',$$

let P' be the unique element of $E'[p^n](S)$ with $\langle P, P' \rangle_\pi = \zeta_{p^n}$. Then

$$P \in E \xrightarrow{\pi} E' \ni P'$$

is a $[\mathrm{bal}.\Gamma_1(p^n)]^{can}$ structure on E and this defines the isomorphism.

Fix a prime p and let $\mathbf{F}_p$ be the field of p elements. For each $E/S/\mathbf{F}_p$, we define an elliptic curve $E^{(p)}$ and an isogeny $F : E \to E^{(p)}$ via the diagram

$$\begin{array}{ccccc} E & \xrightarrow{F} & E^{(p)} & \longrightarrow & E \\ & \searrow & \downarrow & & \downarrow \\ & & S & \xrightarrow{F_{abs}} & S \end{array}$$

where F_{abs} is the absolute Frobenius morphism of S and the square is Cartesian. The isogeny F is called the relative Frobenius of E/S; it is purely inseparable of degree p and the dual isogeny will be denoted $V : E^{(p)} \to E$. This construction can be iterated to give $V^n : E^{(p^n)} \to E$. When S is the spectrum of an algebraically closed field, E is said to be ordinary if V is separable. In this case, $\mathrm{Ker}\, V$ is an étale group scheme over S, thus it becomes isomorphic to the constant group $\mathbf{Z}/p\mathbf{Z}$ over a separable field extension. When V is inseparable, E is said to be supersingular; there are finitely many isomorphism classes of supersingular E over S and their

j-invariants all lie in the field of p^2 elements. For a general S, E is said to be ordinary if all of its geometric fibers are ordinary.

On $(\mathrm{Ell}/\mathbf{F}_p)$, the moduli problem $[\mathrm{Ig}(p^n)]$ of Igusa structures of level p^n associates to E/S the set of $P \in E^{(p^n)}[p^n](S)$ which generate the subgroup scheme $\mathrm{Ker}\, V^n$ of $E^{(p^n)}$. A slight variation is the moduli problem $[\mathrm{Ig}(p^n)^{ord}]$ which assigns the empty set to non-ordinary elliptic curves, and the set $[\mathrm{Ig}(p^n)](E/S)$ to ordinary E/S. The group $(\mathbf{Z}/p^n\mathbf{Z})^\times$ acts on $[\mathrm{Ig}(p^n)]$ via

$$a : (E, P) \mapsto (E, aP)$$

and the quotient of $[\mathrm{Ig}(p^n)]$ by the subgroup $\{a | a \equiv 1 \bmod p^m\}$ is isomorphic to $[\mathrm{Ig}(p^m)]$ ([4], 12.6.1(3)).

If $\mathcal{P}$ and $\mathcal{P}'$ are two moduli problems on (Ell/R), an "exotic" morphism between them is the assignment, for each $(E/S, \alpha)$ with $\alpha \in \mathcal{P}(E/S)$, of a $\mathcal{P}'$ structure on a possibly different elliptic curve E':

$$(E/S, \alpha) \mapsto (E'/S, \alpha')$$

with $\alpha' \in \mathcal{P}'(E'/S)$; this assignment is required to be compatible with morphisms in (Ell/R). For example, the W_N involution of $[\mathrm{bal}.\Gamma_1(N)]^{can}$ sends

$$P \in E \xrightarrow{\pi} E' \ni P'$$

to

$$-P' \in E' \xrightarrow{\pi^t} E \ni P,$$

which is a $[\mathrm{bal}.\Gamma_1(N)^{can}]$ structure on E'.

If k is a perfect field of charactersitic p and $\sigma : k \to k$ is its absolute Frobenius, then for any k-scheme S, define $S^{(\sigma^i)}$ by the Cartesian diagram

$$\begin{array}{ccc} S^{(\sigma^i)} & \longrightarrow & S \\ \downarrow & & \downarrow \\ Spec\ k & \xrightarrow{\sigma^i} & Spec\ k. \end{array}$$

If $\mathcal{P}$ is a moduli problem on (Ell/k), define a new moduli problem $\mathcal{P}^{(\sigma^i)}$ by

$$\mathcal{P}^{(\sigma^i)}(E^{(\sigma^i)}/S^{(\sigma^i)}) = \mathcal{P}(E/S).$$

Evidently $\mathcal{P}^{(\sigma^i)}$ is exotically isomorphic to $\mathcal{P}$. If $\mathcal{P}$ is actually defined on (Ell/$\mathbf{F}_p$), then $\mathcal{P}^{(\sigma^i)} = \mathcal{P}$ as moduli problems on (Ell/$\mathbf{F}_p$).

Finally, if $R \to R'$ is a homomorphism of rings and $\mathcal{P}$ is a moduli problem on (Ell/R), we write $\mathcal{P} \otimes R'$ for the "restriction" of $\mathcal{P}$ to (Ell/R').

5. Moduli spaces. One says that a moduli problem $\mathcal{P}$ on (Ell/R) is representable if it is so as a functor. Concretely, this means that there exists an R-scheme $\mathcal{M}(\mathcal{P})$ and an elliptic curve

$$\mathbf{E} \to \mathcal{M}(\mathcal{P})$$

such that $\mathcal{P}(E/S) = \mathrm{Hom}_{(\mathrm{Ell}/R)}(E/S, \mathbf{E}/\mathcal{M}(\mathcal{P}))$. According to [4] (2.7.2, 2.7.3, 3.6.0, and 4.7.1), the moduli problems $[\Gamma(N)]$ ($N \geq 3$), $[\mathrm{bal}.\Gamma_1(N)]$, and $[\Gamma_1(N)]$ ($N \geq 4$) are represented on (Ell/$\mathbf{Z}[1/N]$) by smooth affine $\mathbf{Z}[1/N]$-curves. Similarly, $[\mathrm{Ig}(p^n)^{ord}]$ is representable on (Ell/$\mathbf{F}_p$) for $p^n \geq 3$ ([4], 12.6.3).

When $\mathcal{P}$ is not representable, there is a next-best replacement for $\mathcal{M}$, namely the coarse moduli scheme $M(\mathcal{P})$. Localising if necessary, we assume some prime l is invertible on R. Then $M(\mathcal{P})$ is defined to be the quotient of the R-scheme

$\mathcal{M}(\mathcal{P}, [\Gamma(l)])$ by the group $\mathrm{GL}_2(\mathbf{Z}/l\mathbf{Z})$. One checks that this is independent of the choice of l and thus patches to give $M(\mathcal{P})$ over all of R. When $\mathcal{P}$ is representable, $M(\mathcal{P}) = \mathcal{M}(\mathcal{P})$.

For any $\mathcal{P}$, the j-invariant provides a morphism

$$M(\mathcal{P}) \to \mathbf{A}^1_R$$

to the affine line over R. For moduli problems satisfying mild hypotheses (including all the problems considered here), it is possible to compactify $M(\mathcal{P})$ to a $\mathbf{P}^1_R$-scheme

$$\overline{M}(\mathcal{P}) \to \mathbf{P}^1_R$$

by "normalizing near infinity." The scheme of cusps of $\mathcal{P}$, $Cusps(\mathcal{P})$ is by definition the reduced scheme $(j^{-1}(\infty))^{red}$. A modular interpretation of the cusps, in terms of certain degenerations of elliptic curves, is given in [2]. See [4], chapter 8 for more details on coarse moduli schemes and compactifications.

6. Modular forms. In this section, we define modular forms from the point of view of the two preceding sections and define a correspondence which induces the Hecke operator T_l. Let $E \xrightarrow{\pi} S$ be an elliptic curve and $\Omega^1_{E/S}$ the relative dualising sheaf. Define an invertible sheaf ω on S by $\omega = \pi^* \Omega^1_{E/S}$. Let $\mathcal{P}$ be a moduli problem on (Ell/R). Then a (not necessarily holomorphic at infinity) *modular form* of weight k for $\mathcal{P}$ over R is an assignment for each $E/S/R$ and $\alpha \in \mathcal{P}(E/S)$ of a section

$$f \in H^0(S, \omega^{\otimes k}),$$

compatible with morphisms in (Ell/R). (In [2] (VII.3.5), some doubt is expressed about the wisdom of such a definition in this generality. We will in fact use it only

over the complex numbers, where one is certain that it is correct.) We will call this assignment f; if it extends to the cusps, i.e., to generalized elliptic curves E/S and $\alpha \in \mathcal{P}(E/S)$, f will be said to be holomorphic at infinity. Also, f will be called a *cusp form* if it vanishes on $(E/S, \alpha)$ for degenerate E/S. It is shown in [2] (VII.4) that this definition agrees with the usual one when the base ring R is the complex numbers.

When $\mathcal{P}$ is representable, a modular form of weight k for $\mathcal{P}$ amounts to a section of $H^0(\mathcal{M}(\mathcal{P}), \omega^{\otimes k})$ where ω is deduced from the universal curve

$$\mathbf{E} \to \mathcal{M}(\mathcal{P}).$$

In many cases, in particular for $[\Gamma(N)]^{can}$ on $(\mathrm{Ell}/\mathbf{Z}[\zeta_N, 1/N])$ for $N \geq 3$, it is true that a holomorphic modular form of weight k amounts to a section of $H^0(\overline{\mathcal{M}}(\mathcal{P}), \omega^{\otimes k})$ for a certain extension of ω to $\overline{\mathcal{M}}(\mathcal{P})$ ([4], 10.13) and a cusp form of weight k for $\mathcal{P}$ is a section of $H^0(\overline{\mathcal{M}}(\mathcal{P}), \Omega^1_{\overline{\mathcal{M}}(\mathcal{P})} \otimes \omega^{\otimes k-2})$. For $\mathcal{P}$ a moduli problem on (Ell/R), let $S_k(\mathcal{P})$ be the space of cusp forms of weight k for the problem $\mathcal{P}$. We remark that use will be made of this definition only in the case $R = \mathbf{C}$.

Consider a moduli problem $\mathcal{P}$ of level N on (Ell/R), an R-scheme S and a prime l not dividing N. If $\pi : E \to E'$ is a cyclic S-isogeny of degree l, and α is a $\mathcal{P}$ structure on E, then π defines (by composition) a $\mathcal{P}$ structure on E', and this induces an isomorphism $\mathcal{P}(E/S) \to \mathcal{P}(E'/S)$. Using this we define two exotic morphisms from the simultaneous moduli problem $(\mathcal{P}, [\Gamma_0(l)])$ to $\mathcal{P}$ by sending

$$E \xrightarrow{\pi} E',\ \alpha$$

to either (E, α) or to $(E', \pi\alpha)$. Passing to compactified moduli spaces, we get two maps $\overline{M}(\mathcal{P}, [\Gamma_0(l)]) \to \overline{M}(\mathcal{P})$ which we can use to define a correspondence T_l on $\overline{M}(\mathcal{P})$. When l is invertible in R, this correspondence defines an endomorphism of the space of modular forms of a fixed weight for $\mathcal{P}$. When $R = \mathbf{C}$, this construction agrees with the usual definition of T_l. The analogous construction for U_p when p divides N is more involved. We give it in the case $\mathcal{P} = [\text{bal.}\Gamma_1(p^n)^{can}]$ in the next section.

We will need the analogues of the functions E and H of section 2 for the case of extra prime to p level structure. Let $R = \mathbf{C}$ and assume that $\mathcal{P} = [\Gamma(N)/\Gamma]^{can}$ for some subgroup $\Gamma \subset \mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$. As before, we have an action of $(\mathbf{Z}/p^n\mathbf{Z})^\times$ on the space of modular forms $S_k(\mathcal{P}, \Gamma_1(p^n))$ via its action on $[\Gamma_1(p^n)]$ structures. If χ is a complex valued character of $(\mathbf{Z}/p^n\mathbf{Z})^\times$, the subspace $S_k(\mathcal{P}, \Gamma_1(p^n), \chi)$ consists of those forms which satisfy $\langle a \rangle f = \chi(a) f$ for all $a \in (\mathbf{Z}/p^n\mathbf{Z})^\times$.

Now define polynomials in q^{-s}, for q a power of p, via

$$E_q(\mathcal{P}, \Gamma_1(p^n), k, s) = \prod_{cond(\chi)=p^n} \det\left(1 - U_q q^{-s} | S_k(\mathcal{P}, \Gamma_1(p^n), \chi)\right) \quad (n \geq 1)$$

and

$$E_q(\mathcal{P}, \Gamma_1(1), k, s) = \det\left(1 - T_q q^{-s} + q^{k-1-2s} | S_k(\mathcal{P}, \Gamma_1(1))\right).$$

As before, set

$$H_q(\mathcal{P}, \Gamma_1(p^n), k, s) = \prod_{m=0}^{n} E_q(\mathcal{P}, \Gamma_1(p^m), k, s). \tag{6.1}$$

The correspondence U_p

7. Definition of the correspondence. First a notational convention: if

$$\pi : E_0 \to E_m$$

is a cyclic p^m-isogeny, we write

$$E_0 \xrightarrow{\pi_{0,1}} E_1 \longrightarrow \cdots \longrightarrow E_{m-1} \xrightarrow{\pi_{m-1,m}} E_m$$

for the factorization of π into cyclic isogenies in standard order ([4], 6.7). We also abbreviate $\pi_{i,j} = \pi_{j-1,j} \circ \cdots \circ \pi_{i,i+1}$ and $\pi_{j,i} = \pi_{i,j}^t$ (the dual isogeny) for $0 \leq i < j \leq m$.

Next we introduce the $[\Gamma_0(p^{n+1}), n, n]^{can}$ moduli problem on $(\mathrm{Ell}/\mathbf{Z}[\zeta_{p^n}])$. This functor assigns to E_0/S the set of cyclic p^{n+1}-isogenies $\pi : E_0 \to E_{n+1}$, together with generators $P \in E_1(S)$ of $\pi_{1,n+1}$ and $Q \in E_n(S)$ of $\pi_{n,0}$ subject to the condition that $\langle \pi_{1,0}(P), Q \rangle_{\pi_{0,n}} = \zeta_{p^n}$ (or equivalently, $\langle P, \pi_{n,n+1}(Q) \rangle_{\pi_{1,n+1}} = \zeta_{p^n}$); diagramatically:

$$\begin{array}{ccccccc} & & P & & Q & & \\ \pi : E_0 & \to & E_1 & \longrightarrow & E_n & \to & E_{n+1}. \end{array}$$

According to [4], 7.9.6, $[\Gamma_0(p^{n+1}), n, n]^{can}$ is isomorphic to the quotient problem $[\Gamma(p^{n+1})/\Gamma]^{can}$ where

$$\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} | c \equiv 0 \pmod{p^{n+1}},\ a \equiv d \equiv 0 \pmod{p^n} \right\} \subseteq \mathrm{GL}_2(\mathbf{Z}/p^{n+1}\mathbf{Z})$$

Given any moduli problem $\mathcal{P}$ of level prime to p on (Ell/R) for R a $\mathbf{Z}[\zeta_{p^n}]$-algebra, there are two exotic morphisms from $(\mathcal{P}, [\Gamma_0(p^{n+1}), n, n]^{can})$ to $(\mathcal{P}, [\mathrm{bal}.\Gamma_1(p^n)]^{can})$, namely

$$\begin{array}{ccccccc} & & P & & Q & & \\ \pi : E_0 & \to & E_1 & \longrightarrow & E_n & \to & E_{n+1},\ \alpha \end{array}$$

is sent either to

$$P \in E_1 \xrightarrow{\pi_{1,n+1}} E_{n+1} \ni \pi_{n,n+1}(Q),\ \pi_{0,1}(\alpha)$$

or to

$$\pi_{1,0}(P) \in E_0 \xrightarrow{\pi_{0,n}} E_n \ni Q,\ \alpha.$$

To check that the first map, call it pr_1 is defined, first note that, by the definition of $[\Gamma_0(p^{n+1}), n, n]^{can}$, P generates the kernel of the cyclic isogeny $\pi_{1,n+1}$, and $\langle P, \pi_{n,n+1}(Q)\rangle_{\pi_{1,n+1}} = \zeta_{p^n}$. To finish, we must show that $\pi_{n,n+1}(Q) \in E_{n+1}(S)$ is a generator of the kernel of $\pi_{n+1,1}$. But $\pi_{n+1,n}(\pi_{n,n+1}(Q)) = pQ$ which, by the defintion of a standard factorization, generates the kernel of $\pi_{n,1}$. By the "Backing-up theorem" ([4], 6.7.11(2)), $\pi_{n,n+1}(Q)$ generates the kernel of $\pi_{n+1,1}$. Thus the map is defined. One checks similarly that the second map, pr_2 is also well-defined. The induced maps on compactified moduli schemes are finite and flat of degree p.

Using the maps pr_1 and pr_2, we define in the usual way a correspondence U_p on $\mathcal{M}(\mathcal{P}, \text{bal.}\Gamma_1(p^n)^{can})$. On points,

$$U_p(x) = \sum_{pr_1(y)=x} pr_2(y)$$

where the sum is over the points of $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^{n+1}), n, n]^{can})$ mapping via pr_1 to x, taken with multiplicities. We leave it to the reader to check that this correspondence agrees with the usual U_p.

8. Geometry mod p. Fix a moduli problem $\mathcal{P}$ which is representable, finite and étale over $R = \mathbf{Z}[\zeta_{p^n}, \zeta_N, 1/N]$ for some N relatively prime to p. (For example, $\mathcal{P} = [\Gamma(N)]^{can}$ with $N \geq 3$.) In this section we will study the geometry of $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^{n+1}), n, n]^{can})$ modulo p.

Let k be a perfect field of characteristic p and let $R \to k$ be a homomorphism. We recall a result of [4] (13.11.4).

Proposition 8.1. *The scheme* $\overline{\mathcal{M}}(\mathcal{P}, [bal.\Gamma_1(p^n)]^{can}) \otimes_R k$ *is the disjoint union, with crossings at the supersingular points, of the following smooth* k*-curves: for each pair of non-negative integers* a, b *with* $a+b=n$ *and each* $u \in (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times$*, one copy of* $\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-b})}, Ig(p^{\max(a,b)}))$.

For the precise definition of "crossings at the supersingular points," see [4] (13.1-2). We will refer to the curve $\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-b})}, \mathrm{Ig}(p^{\max(a,b)}))$ indexed by a, b, and $u \in (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times$ as the (a,b,u) component.

In order to use this result, we must describe the correspondence between the various (a,b,u) components and $[\mathrm{bal}.\Gamma_1(p^n)]^{can}$ structures. Given an S-valued point

$$P \in E_0 \xrightarrow{\pi} E_n \ni Q$$

of $\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{bal}.\Gamma_1(p^n)]^{can}) \otimes k$ where S is a k-scheme, there exists a unique pair of non-negative integers a, b such that π can be factored as a purely inseparable isogeny of degree p^a followed by an étale isogeny of degree p^b. There also exists a unique elliptic curve E/S such that $E_0 \cong E^{(p^b)}$ and $E_n \cong E^{(p^a)}$; P and Q are $\mathrm{Ig}(p^a)$ and $\mathrm{Ig}(p^b)$ structures respectively on E/S. If $a \geq b$, then there is a unique unit $u \in (\mathbf{Z}/p^b\mathbf{Z})^\times$ such that $uP = V^{a-b}(Q)$, while if $a \leq b$, there exists a unique unit $u \in (\mathbf{Z}/p^a\mathbf{Z})^\times$ such that $uV^{b-a}(P) = Q$. Thus we get (a,b,u) and, using $\alpha \in \mathcal{P}(E_0) = \mathcal{P}^{(\sigma^{-b})}(E)$, an S-valued point of $\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-b})}, \mathrm{Ig}(p^{\max(a,b)}))$.

Conversely, given (a,b,u) as in the statement, if $a \geq b$, let (E,Q) be an S-valued point of $\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-b})}, \mathrm{Ig}(p^a))$ (so $Q \in E^{(p^a)}(S)$) and set $P = u^{-1}V^{a-b}(Q) \in E^{(p^b)}(S)$.

If $a \leq b$, let (E, P) be an S-valued point of $\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-b})}, \mathrm{Ig}(p^b))$ (so $P \in E^{(p^b)}(S)$) and set $Q = uV^{b-a}(P) \in E^{(p^a)}(S)$. Then the diagram

$$P \in E^{(p^b)} \xrightarrow{F^a} E^{(p^n)} \xrightarrow{V^b} E^{(p^a)} \ni Q$$

is a $[\mathrm{bal}.\Gamma_1(p^n)]^{can}$ structure on $E^{(p^b)}$, which together with $\alpha \in \mathcal{P}^{(\sigma^{-b})}(E) = \mathcal{P}(E^{(p^b)})$ defines an S-valued point of $\overline{\mathcal{M}}(\mathcal{P}, [\mathrm{bal}.\Gamma_1(p^n)]^{can}) \otimes k$.

As for $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^{n+1}), n, n]^{can})$, we have the following result.

Proposition 8.2. *The scheme $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^{n+1}), n, n]^{can}) \otimes_R k$ is the disjoint union, with crossings at the supersingular points, of the following smooth k-curves: for each pair of non-negative integers a, b with $a + b = n + 1$ and each $u \in (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times$, one copy of $\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-(b-1)})}), Ig(p^{\max(a,b)}))$ if $ab \neq 0$, one copy of $\overline{\mathcal{M}}(\mathcal{P}, Ig(p^n))$ for $(a, b) = (n + 1, 0)$, and one copy of $\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-(n+1)})}, Ig(p^n))$ for $(a, b) = (0, n + 1)$.*

The proof of this result is a direct translation of that of Proposition 8.1, which the reader can consult in [4] (13.11.2-4). We merely describe the correspondence between points on the (a, b, u) components and $[\Gamma_0(p^{n+1}), n, n]^{can}$ structures. Given an S-valued point

$$\pi : E_0 \to E_1 \underset{P}{\longrightarrow} E_n \underset{Q}{\to} E_{n+1}.$$

of $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^{n+1}), n, n]^{can}) \otimes k$ where S is a k-scheme, there exists a unique pair of non-negative integers a, b with $a + b = n + 1$ such that $\pi : E_0 \to E_{n+1}$ can be factored as a purely inseparable isogeny of degree p^a followed by an étale isogeny of degree p^b. Again, there exists a unique elliptic curve E/S such that $E_0 \cong E^{(p^b)}$ and $E_{n+1} \cong E^{(p^a)}$. Assume for the moment that $ab \neq 0$. Then $P \in E^{(p^b)}(S)$

is an $\mathrm{Ig}(p^b)$ structure on E, $Q \in E^{(p^a)}(S)$ is an $\mathrm{Ig}(p^a)$ structure on E, and there exists a unique unit $u \in (\mathbf{Z}/p^{\min(a,b)}\mathbf{Z})^\times$ such that $uP = V^{a-b}(Q)$ if $a \geq b$, while if $a \leq b$, there exists a unique unit $u \in (\mathbf{Z}/p^a\mathbf{Z})^\times$ such that $uV^{b-a}(P) = Q$. Thus we get (a, b, u) and, using $\alpha \in \mathcal{P}(E_0) = \mathcal{P}^{(\sigma^{-(b-1)})}(E)$, an S-valued point of $\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-(b-1)})}, \mathrm{Ig}(p^{\max(a,b)}))$. If $(a, b) = (n+1, 0)$ then Q is an $\mathrm{Ig}(p^n)$ structure on E_0, P is the identity element of $E_1(S)$, and we get, using $\alpha \in \mathcal{P}(E_0)$, an S-valued point of $\overline{\mathcal{M}}(\mathcal{P}, \mathrm{Ig}(p^n))$. If $(a, b) = (0, n+1)$, then P is an $\mathrm{Ig}(p^n)$ structure on E_{n+1}, Q is the identity element of $E_n(S)$, and using $\alpha \in \mathcal{P}(E_0) = \mathcal{P}^{(\sigma^{-(n+1)})}(E_n + 1)$, we get an S valued point of $\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-(n+1)})}, \mathrm{Ig}(p^n))$.

Conversely, given (a, b, u) as in the statement, if $n+1 > a \geq b$, let (E, Q, α) be an S-valued point of $\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-(b-1)})}, \mathrm{Ig}(p^a))$ and set $P = u^{-1}V^{a-b}(Q) \in E^{(p^b)}(S)$. If $a \leq b < n+1$, let (E, P, α) be an S-valued point of $\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-(b-1)})}, \mathrm{Ig}(p^b))$ (so $P \in E^{(p^b)}(S)$) and set $Q = uV^{b-a}(P) \in E^{(p^a)}(S)$. Then the diagram

$$\begin{array}{ccccccccc} E^{(p^{b-1})} & \xrightarrow{Fr} & E^{(p^b)} & \xrightarrow{Fr^{a-1}} & E^{(p^n)} & \xrightarrow{V^{b-1}} & E^{(p^a)} & \xrightarrow{V} & E^{(p^{a-1})} \\ & & P & & & & Q & & \end{array}$$

is a $[\Gamma_0(p^{n+1}), n, n]^{can}$ structure on $E^{(p^{b-1})}$, which together with $\alpha \in \mathcal{P}^{(\sigma^{-(b-1)})}(E) = \mathcal{P}(E^{(p^{b-1})})$ defines an S-valued point of $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^{n+1}), n, n]^{can}) \otimes k$. If $(a, b) = (n+1, 0)$ and (E, Q, α) is an S-valued point of $\overline{\mathcal{M}}(\mathcal{P}, \mathrm{Ig}(p^n))$, let P be the identity element of $E^{(p^n)}(S)$. Then

$$\begin{array}{ccccccc} E & \xrightarrow{Fr} & E^{(p)} & \xrightarrow{Fr^{n-1}} & E^{(p^n)} & \xrightarrow{V} & E^{(p^{n-1})} \\ & & P & & Q & & \end{array}$$

is a $[\Gamma_0(p^{n+1}), n, n]^{can}$ structure on E which together with $\alpha \in \mathcal{P}(E)$ gives an S-valued point of $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^{n+1}), n, n]^{can}) \otimes k$. If $(a, b) = (0, n+1)$ and (E, P, α) is an

S-valued point of $\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-(n+1)})}, \mathrm{Ig}(p^n))$, let Q be the identity element of $E^{(p)}(S)$. Then

$$E^{(p^{n+1})} \xrightarrow{V} E^{(p^n)} \xrightarrow{V^{n-1}} E^{(p)} \xrightarrow{V} E$$
$$P \qquad\qquad Q$$

is a $[\Gamma_0(p^{n+1}), n, n]^{can}$ structure on $E^{(p^{n+1})}$ which together with $\alpha \in \mathcal{P}^{(\sigma^{-(n+1)})}(E/S) = \mathcal{P}(E^{(p^{n+1})})$ defines an S-valued point of $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^{n+1}), n, n]^{can}) \otimes k$.

Next, we need to describe the two maps $\overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^{n+1}), n, n]^{can}) \otimes k \to \overline{\mathcal{M}}(\mathcal{P}, \mathrm{bal}.\Gamma_1(p^n)^{can}) \otimes k$ in terms of the (a, b, u) components. In what follows, we write F for the absolute Frobenius of a curve over k, and V for the map on Igusa curves induced by $(E, P) \mapsto (E, VP)$. For simplicity, we omit the effect of the maps on $\mathcal{P}$ structures in the next statement; for pr_1, they are induced by the isomorphism $\pi_{0,1} : \mathcal{P}(E_0) \to \mathcal{P}(E_1)$, while for pr_2, they are just the identity map on $\mathcal{P}(E_0)$.

Proposition 8.3. *Restricted to the various (a, b, u) components, the map*

$$pr_1 : \overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^{n+1}), n, n]^{can}) \otimes k \to \overline{\mathcal{M}}(\mathcal{P}, [bal.\Gamma_1(p^n)]^{can}) \otimes k$$

is:

$$\begin{array}{rcll}
\overline{\mathcal{M}}(\mathcal{P}, Ig(p^n))_{(n+1,0,1)} & \xrightarrow{F} & \overline{\mathcal{M}}(\mathcal{P}, Ig(p^n))_{(n,0,1)} & \\
\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-(b-1)})}, Ig(p^{\max(a,b)}))_{(a,b,u)} & \xrightarrow{V} & \overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-b})}, Ig(p^{\max(a,b)}))_{(a-1,b,u)} & b < a \\
\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-(b-1)})}, Ig(p^{\max(a,b)}))_{(a,b,u)} & \xrightarrow{id} & \overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-b})}, Ig(p^{\max(a,b)}))_{(a-1,b,u)} & b \geq a \\
\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-(n+1)})}, Ig(p^n))_{(0,n+1,1)} & \xrightarrow{id} & \overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-n})}, Ig(p^n))_{(0,n,1)} &
\end{array}$$

and the map

$$pr_2 : \overline{\mathcal{M}}(\mathcal{P}, [\Gamma_0(p^{n+1}), n, n]^{can}) \otimes k \to \overline{\mathcal{M}}(\mathcal{P}, [bal.\Gamma_1(p^n)]^{can}) \otimes k$$

is:

$$\begin{array}{rcll}
\overline{\mathcal{M}}(\mathcal{P}, Ig(p^n))_{(n+1,0,1)} & \xrightarrow{id} & \overline{\mathcal{M}}(\mathcal{P}, Ig(p^n))_{(n,0,1)} & \\
\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-(b-1)})}, Ig(p^{\max(a,b)}))_{(a,b,u)} & \xrightarrow{id} & \overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-b})}, Ig(p^{\max(a,b)}))_{(a,b-1,u)} & b \leq a \\
\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-(b-1)})}, Ig(p^{\max(a,b)}))_{(a,b,u)} & \xrightarrow{V} & \overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-b})}, Ig(p^{\max(a,b)}))_{(a,b-1,u)} & b > a \\
\overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-(n+1)})}, Ig(p^n))_{(0,n+1,1)} & \xrightarrow{F} & \overline{\mathcal{M}}(\mathcal{P}^{(\sigma^{-n})}, Ig(p^n))_{(0,n,1)} &
\end{array}$$

Here we use subscripts to indicate the component on which a point lies. The proof is a simple exercise in tracing through the identifications of Propositions 8.1 and 8.2. We leave it to the reader.

The case $n = 1$ of the following corollary is due to Wiles ([12], thm 5.4).

Corollary 8.4. *The correspondence U_p on $\overline{\mathcal{M}}(\mathcal{P}, bal.\Gamma_1(p^n)^{can}) \otimes k$ is given on ordinary points by the following correspondences:*

On the $(n, 0, 1)$ component,

$$U_p(x) = (p\, F^{-1}(x))_{(n,0,1)} = Ver(x).$$

On the (a, b, u) component for $a \geq b > 0$,

$$U_p(x) = (V^{-1}(x))_{(a+1,b-1,u)}.$$

On the (a, b, u) component for $0 < a < b$,

$$U_p(x) = \sum_{\substack{u' \bmod p^{a+1} \\ u' \equiv u \bmod p^a}} (V(x))_{(a+1,b-1,u)}.$$

On the $(0, n, 1)$ component,

$$U_p(x) = (F(x))_{(0,n,1)} + \sum_{u \in (\mathbf{Z}/p\mathbf{Z})^\times} (V(x))_{(1,n-1,u)}.$$

Note that only the $(n, 0, 1)$ component is left stable by this correspondence.

Proof of the Theorem

9. First reductions We begin with a statement of the more general theorem we are going to prove. Fix a prime p and for q a power of p, let $\mathbf{F}_q$ be the field of q elements. Let N be a positive integer relatively prime to p and fix a subgroup Γ of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$; $\mathcal{P}$ will be the moduli problem $[\Gamma(N)/\Gamma]^{can}$ on $(\mathrm{Ell}/\mathbf{Z}[\zeta_N, 1/N])$. Fix a power p^n of p and assume that either $p^n \geq 3$, or that $\mathcal{P} \otimes \mathbf{F}_q$ is representable. In this case, the simultaneous problem $[\mathcal{P}, \mathrm{Ig}(p^n)^{ord}]$ is representable on $(\mathrm{Ell}/\mathbf{F}_q)$ by a smooth $\mathbf{F}_q$-curve which is an open subset of $\overline{M}(\mathcal{P}, \mathrm{Ig}(p^n))$. We have a universal curve

$$\mathbf{E} \to \mathcal{M}(\mathcal{P}, \mathrm{Ig}(p^n)^{ord}). \tag{9.1}$$

Let K be the function field of $\mathcal{M}(\mathcal{P}, \mathrm{Ig}(p^n)^{ord})$ and $\overline{K}$ a separable closure; the generic fiber of (9.1) is an elliptic curve E over K. When $\mathcal{P}$ is the trivial problem, we recover the situation of section 1. Let ℓ be a prime dividing N (so ℓ is prime to p and invertible in $\mathbf{Z}[\zeta_N, 1/N]$). As before, there is a representation of the Galois group

$$\rho : \mathrm{Gal}(\overline{K}/K) \to \mathrm{Aut}_{\mathbf{Q}_\ell}(H^1(E \otimes \overline{K}, \mathbf{Q}_\ell))$$

and the L-function associated to $H^i(E^d \otimes \overline{K}, \mathbf{Q}_\ell)$ can be expressed as products of translates of the $L(\mathrm{Sym}^k \rho, s)$.

Let $\mathcal{F}(k)$ be the constructible étale sheaf on $\overline{M}(\mathcal{P}, \mathrm{Ig}(p^n))$ associated to the representation $\mathrm{Sym}^k \rho$. Explicitly, if

$$\mathbf{E} \xrightarrow{\pi} \overline{M}(\mathcal{P}, \mathrm{Ig}(p^n))$$

is the Néron model of (9.1), then $\mathcal{F}(k) \cong \mathrm{Sym}^k R^1\pi_*\mathbf{Q}_\ell$. According to Grothendieck's theory of L-functions ([3], or [5], VI.13.3), we have

$$L(\mathrm{Sym}^k\rho, s) = \prod_{i=0}^{2} \det\left(1 - \mathrm{Fr}\cdot q^{-s} | H^i(\overline{M}(\mathcal{P}, \mathrm{Ig}(p^n)) \otimes \overline{\mathbf{F}_p}, \mathcal{F}(k))\right)^{(-1)^{i+1}}$$

where Fr is the Frobenius endomorphism of $\overline{M}(\mathcal{P}, \mathrm{Ig}(p^n)) \otimes \overline{\mathbf{F}_p}$. One knows (using [4], 14.3.4.3) that $H^0(\overline{M}(\mathcal{P}, \mathrm{Ig}(p^n)) \otimes \overline{\mathbf{F}_p}, \mathcal{F}(k)) = 0$ and $H^2(\overline{M}(\mathcal{P}, \mathrm{Ig}(p^n)) \otimes \overline{\mathbf{F}_p}, \mathcal{F}(k)) = 0$ if $k > 0$, and since $\mathcal{F}(0) \cong \mathbf{Q}_\ell$, $H^0(\overline{M}(\mathcal{P}, \mathrm{Ig}(p^n)) \otimes \overline{\mathbf{F}_p}, \mathcal{F}(0)) \cong \mathbf{Q}_\ell$ and $H^2(\overline{M}(\mathcal{P}, \mathrm{Ig}(p^n)) \otimes \overline{\mathbf{F}_p}, \mathcal{F}(0)) \cong \mathbf{Q}_\ell(-1)$. Recall the Hecke polynomials $H_q(k+2, \mathcal{P}, \Gamma_1(p^n), s)$ defined in (6.1). Our main result is then the following calculation of the action of Frobenius on H^1.

Theorem.

$$\det\left(1 - Fr\cdot q^{-s} | H^1(\overline{M}(\mathcal{P}, Ig(p^n)) \otimes \overline{\mathbf{F}_p}, \mathcal{F}(k))\right) = H_q(\mathcal{P}, \Gamma_1(p^n), k+2, s)$$

10. The good reduction theorem From now until the last section we assume that $N \geq 5$ and Γ is the trivial subgroup of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ so $\mathcal{P} = [\Gamma(N)]^{can}$. Let $R = \mathbf{Z}[\zeta_{p^n}, \zeta_N, 1/N]$; the moduli problem $[\mathcal{P}, \mathrm{bal}.\Gamma_1(p^n)^{can}]$ is representable on (Ell/R). To ease notation, let $W(\overline{\mathbf{F}_p})$ be the Witt ring of $\overline{\mathbf{F}_p}$, F its field of fractions, and $\overline{F}$ the algebraic closure. Choose a map $R \to W(\overline{\mathbf{F}_p})(\zeta_{p^n})$ and let $X = \overline{\mathcal{M}}(\mathcal{P}, \mathrm{bal}.\Gamma_1(p^n)^{can})$, $X_s = X \otimes_R \overline{\mathbf{F}_p}$, and $X_{\overline{\eta}} = X \otimes_R \overline{F}$. The curve $X_{\overline{\eta}}$ is smooth over $\overline{F}$ and X_s is a union of Igusa curves as in section 8. Because $\mathcal{P}$ is representable, there is again a universal curve over X and one constructs a sheaf $\mathcal{F}(k)$ as before. The restriction of $\mathcal{F}(k)$ to the various components of X_s is the $\mathcal{F}(k)$ previously constructed on these curves. Recall that we have an action of

$G = (\mathbf{Z}/p^n\mathbf{Z})^\times \times (\mathbf{Z}/p^n\mathbf{Z})^\times$ on the moduli problem [bal.$\Gamma_1(p^n)^{can}$], and thus on the schemes X, X_s and $X_{\overline{\eta}}$. This action commutes with the correspondence U_p and with the action of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$.

For any vector space M on which $(\mathbf{Z}/p^n\mathbf{Z})^\times$ acts semi-simply, let $M(n)$ be the subspace on which it acts via a character of conductor exactly p^n. Let $H \subset (\mathbf{Z}/p^n\mathbf{Z})^\times$ be the subgroup generated by $(1+p^{n-1})$ and $\Delta : (\mathbf{Z}/p^n\mathbf{Z})^\times \to G$ the map $\Delta(a) = (a, a^{-1})$.

Vanishing cycle theory gives an injection

$$H^1(X_s, \mathcal{F}(k)) \hookrightarrow H^1(X_{\overline{\eta}}, \mathcal{F}(k))$$

and the good reduction theorem of Katz-Mazur ([4], 14.5.1) says that this induces an isomorphism

$$H^1(X_s, \mathcal{F}(k))^{1\times H}(n) \cong H^1(X_{\overline{\eta}}, \mathcal{F}(k))(n)$$

where $H^1(X_s, \mathcal{F}(k))^{1\times H}$ is the subspace invariant under $1 \times H \subset G$ and the subspaces $H^1(n)$ are computed with respect to the action of $(\mathbf{Z}/p^n\mathbf{Z})^\times$ via Δ. Using the geometric description of X_s and the action of G, one sees ([4], 14.6.10) that the left hand space is isomorphic to

$$H^1(\overline{\mathcal{M}}((\mathcal{P}\otimes\overline{\mathbf{F}_p})^{\sigma^{-n}}, \mathrm{Ig}(p^n)), \mathcal{F}(k))(n) \bigoplus H^1(\overline{\mathcal{M}}(\mathcal{P}\otimes\overline{\mathbf{F}_p}, \mathrm{Ig}(p^n)), \mathcal{F}(k))(n),$$

and this isomorphism is compatible with the actions of G, U_p and $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$.

Now since $(\mathcal{P}\otimes\overline{\mathbf{F}_p})^{\sigma^{-n}}$ is exotically isomorphic to $\mathcal{P}\otimes\overline{\mathbf{F}_p}$, the two direct summands are isomorphic as $\mathrm{Gal}(\overline{\mathbf{F}_p}/\mathbf{F}_p)$-modules. Furthermore, applying proposition

8.3 and the argument of [1], 4.7, we see that the correspondence U_p acts on the direct sum as Frobenius on the right summand and as the transpose correspondence Ver on the left summand. (This is obvious for $n > 1$; for $n = 1$ we must check that the sum of the V maps from the (0,1) component to the (1,0) component induces zero on $H^1(\overline{\mathcal{M}}(\mathcal{P}\otimes\overline{\mathbf{F}_p}, \mathrm{Ig}(p^n)), \mathcal{F}(k))(n)$. But this is clear, as it is a sum over values of a non-trivial character of $(\mathbf{Z}/p\mathbf{Z})^\times$.) Since transpose correspondences have the same characteristic polynomial, we conclude:

$$\det\left(1 - U_q \cdot q^{-s} | H^1(X_{\overline{\eta}}, \mathcal{F}(k))(n)\right)$$
$$= \det\left(1 - \mathrm{Fr} \cdot q^{-s} | H^1(\overline{\mathcal{M}}(\mathcal{P}, \mathrm{Ig}(p^n)) \otimes \overline{\mathbf{F}_p}, \mathcal{F}(k))(n)\right)^2 \quad 10.1$$

11. The Shimura isomorphism To continue, we choose an imbedding $R = \mathbf{Z}[\zeta_{p^n}, \zeta_N, 1/N] \to \mathbf{C}$. Using this, we get a scheme $X_{\mathbf{C}} = X \otimes_R \mathbf{C}$ over $\mathbf{C}$ (which is independent of the imbedding) and thus an analytic space X^{an} together with a sheaf $\mathcal{F}(k)$. If

$$\mathbf{E}^{\mathrm{an}} \xrightarrow{\pi^{\mathrm{an}}} X^{\mathrm{an}}$$

is the Néron model of the universal curve, then $\mathcal{F}(k) \cong (\mathrm{Sym}^k R^1\pi_*^{\mathrm{an}}\mathbf{Q}) \otimes \mathbf{Q}_\ell$. Thus, using the proper base change theorem (e.g., [5], VI.2.3) and Artin's comparison theorem ([5], III.3.12), we have an isomorphism

$$H^1(X_{\overline{\eta}}, \mathcal{F}(k)) \to H^1(X^{\mathrm{an}}, \mathrm{Sym}^k R^1\pi_*^{\mathrm{an}}\mathbf{Q}) \otimes \mathbf{Q}_\ell.$$

This isomorphism is compatible with the actions of G, U_p and $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ simply because these actions come from actions on $\overline{\mathcal{M}}(\mathcal{P}, \mathrm{bal}.\Gamma_1(p^n)^{can})$ over R. In

particular, since the set of characters of conductor p^n of $(\mathbf{Z}/p^n\mathbf{Z})^\times$ is $\mathbf{Q}$-rational, $H^1(X^{\mathrm{an}}, \mathrm{Sym}^k R^1\pi_*^{\mathrm{an}}\mathbf{Q})(n)$ is a $\mathbf{Q}$-rational subspace of $H^1(X^{\mathrm{an}}, \mathrm{Sym}^k R^1\pi_*^{\mathrm{an}}\mathbf{Q})$ and

$$H^1(X^{\mathrm{an}}, \mathrm{Sym}^k R^1\pi_*^{\mathrm{an}}\mathbf{Q})(n) \otimes \mathbf{Q}_\ell \cong H^1(X_{\overline{\eta}}, \mathcal{F}(k))(n). \tag{11.1}$$

Next we need to bring in modular forms. Let X_o^{an} be the open subset of X^{an} gotten by removing the cusps, and let $j : X_o^{\mathrm{an}} \hookrightarrow X^{\mathrm{an}}$ be the inclusion. Set

$$\tilde{H}^1(X_o^{\mathrm{an}}, j^*\mathrm{Sym}^k R^1\pi_*^{\mathrm{an}}\mathbf{Q})$$
$$= \mathrm{Im}\left(H_c^1(X_0^{\mathrm{an}}, j^*\mathrm{Sym}^k R^1\pi_*^{\mathrm{an}}\mathbf{Q}) \to H^1(X_o^{\mathrm{an}}, j^*\mathrm{Sym}^k R^1\pi_*^{\mathrm{an}}\mathbf{Q})\right)$$

where H_c^1 denotes cohomology with compact supports. Considering $(\mathcal{P}, \Gamma_1(p^n))$ as a moduli problem on (Ell/$\mathbf{C}$), we have the following isomorphism of complex vector spaces, due to Shimura ([7]):

$$\tilde{H}^1(X_o^{\mathrm{an}}, j^*\mathrm{Sym}^k R^1\pi_*^{\mathrm{an}}\mathbf{Q}) \otimes \mathbf{C} \cong S_{k+2}(\mathcal{P}, \Gamma_1(p^n)) \oplus \overline{S_{k+2}(\mathcal{P}, \Gamma_1(p^n))}. \tag{11.2}$$

Again, this is compatible with the actions of G, U_p and $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$.

In order to apply this, we need the following result.

Lemma 11.3. *The restriction map*

$$H^1(X^{\mathrm{an}}, Sym^k R^1\pi_*^{\mathrm{an}}\mathbf{Q}) \to H^1(X_o^{\mathrm{an}}, j^* Sym^k R^1\pi_*^{\mathrm{an}}\mathbf{Q})$$

induces an isomorphism $H^1(X^{\mathrm{an}}, Sym^k R^1\pi_*^{\mathrm{an}}\mathbf{Q}) \cong \tilde{H}^1(X_o^{\mathrm{an}}, j^* Sym^k R^1\pi_*^{\mathrm{an}}\mathbf{Q})$.

Proof: Write $\mathcal{G}$ for $\mathrm{Sym}^k R^1\pi_*^{\mathrm{an}}\mathbf{Q}$ and let $i : Cusps(\mathcal{P}, \Gamma_1(p^n)) \to X^{\mathrm{an}}$ be the inclusion. Recall that $H_c^1(X_o^{\mathrm{an}}, j^*\mathcal{G}) = H^1(X^{\mathrm{an}}, j_!j^*\mathcal{G})$. We have maps

$$H^1(X^{\mathrm{an}}, j_!j^*\mathcal{G}) \to H^1(X^{\mathrm{an}}, \mathcal{G}) \to H^1(X_o^{\mathrm{an}}, j^*\mathcal{G}),$$

and the lemma follows from the fact that the first is surjective and the second is injective. (For the surjectivity, consider the exact sequence

$$H^1(X^{\mathrm{an}}, j_! j^*\mathcal{G}) \to H^1(X^{\mathrm{an}}, \mathcal{G}) \to H^1(X^{\mathrm{an}}, i_* i^*\mathcal{G}) = 0;$$

for the injectivity, consider the exact sequence

$$0 = H^1_{Cusps}(X^{\mathrm{an}}, \mathcal{G}) \to H^1(X^{\mathrm{an}}, \mathcal{G}) \to H^1(X^{\mathrm{an}}_o, j^*\mathcal{G})$$

where H^1_{Cusps} denotes cohomology supported on the cusps.) Q.E.D.

Applying the compatibility of the Shimura isomorphism with U_p and G, we find

$$\det\left(1 - U_q \cdot q^{-s} | H^1(X^{\mathrm{an}}, \mathrm{Sym}^k R^1\pi_*^{\mathrm{an}}\mathbf{Q})(n)\right) = E_q(\mathcal{P}, \Gamma_1(p^n), k+2, s)^2.$$

Finally, using the isomorphisms (11.1-3) and formula (10.1), we find

$$\det\left(1 - \mathrm{Fr} \cdot q^{-s} | H^1(\overline{\mathcal{M}}(\mathcal{P} \otimes \overline{\mathbf{F}_p}, \mathrm{Ig}(p^n)), \mathcal{F}(k))(n)\right) = E_q(\mathcal{P}, \Gamma_1(p^n), k+2, s).$$

12. A dimension count To complete the proof of the theorem for $\mathcal{P} = [\Gamma(N)]^{can}$, we argue by induction on n. The case $n = 0$ is Deligne's result ([1], 5.6). For $n \geq 1$, we have a surjective map of smooth curves:

$$\overline{\mathcal{M}}(\mathcal{P}, \mathrm{Ig}(p^n)) \to \overline{\mathcal{M}}(\mathcal{P}, \mathrm{Ig}(p^{n-1}))$$

which induces an injection

$$i : H^1(\overline{\mathcal{M}}(\mathcal{P}, \mathrm{Ig}(p^{n-1})) \otimes \overline{\mathbf{F}_p}, \mathcal{F}(k)) \to H^1(\overline{\mathcal{M}}(\mathcal{P}, \mathrm{Ig}(p^n)) \otimes \overline{\mathbf{F}_p}, \mathcal{F}(k)).$$

Clearly the image of i intersects the subspace $H^1(\overline{\mathcal{M}}(\mathcal{P}, \mathrm{Ig}(p^n)) \otimes \overline{\mathbf{F}_p}, \mathcal{F}(k))(n)$ only in the zero element. Since the dimension of $H^1(\overline{\mathcal{M}}(\mathcal{P}, \mathrm{Ig}(p^n)) \otimes \overline{\mathbf{F}_p}, \mathcal{F}(k))(n)$ is equal to the degree of $E_q(\mathcal{P}, \Gamma_1(p^n), k+2, s)$, i.e., to

$$\sum_{cond(\chi)=p^n} \dim_{\mathbf{C}} S_{k+2}([\mathcal{P}, \Gamma_1(p^n)], \chi),$$

the theorem is a consequence of the following dimension count.

Proposition 12.1.

$$\dim_{\mathbf{Q}_\ell} H^1(\overline{\mathcal{M}}(\mathcal{P}, Ig(p^n)) \otimes \overline{\mathbf{F}_p}, \mathcal{F}(k)) - \dim_{\mathbf{Q}_\ell} H^1(\overline{\mathcal{M}}(\mathcal{P}, \mathrm{Ig}(p^{n-1})) \otimes \overline{\mathbf{F}_p}, \mathcal{F}(k))$$
$$= \sum_{cond(\chi)=p^n} \dim_{\mathbf{C}} S_{k+2}([\mathcal{P}, \Gamma_1(p^n)], \chi).$$

Proof: We calculate the left hand side using the formula of Grothendieck-Ogg-Shafarevitch and the right hand side using the Riemann-Roch theorem.

Write Y_n for $\overline{\mathcal{M}}(\mathcal{P}, \mathrm{Ig}(p^n)) \otimes \overline{\mathbf{F}_p}$, g_n for its genus, c_n for the number of cusps on Y_n, and let $w = \deg(\mathcal{P})/24$. Since $H^0(Y_n, \mathcal{F}(k))$ and $H^2(Y_n, \mathcal{F}(k))$ are both one dimensional if $k = 0$ and both trivial if $k \geq 1$, the left hand side is equal to $\chi(Y_{n-1}, \mathcal{F}(k)) - \chi(Y_n, \mathcal{F}(k))$ where $\chi(Y_n, \mathcal{F}(k))$ denotes the Euler characteristic of the sheaf $\mathcal{F}(k)$ on the space Y_n. Since $\mathcal{F}(k)$ is lisse of rank $k+1$ away from the cusps, is tamely ramified along the cusps, and is lisse of rank one when restricted to the cusps, by the Grothendieck-Ogg-Shafarevitch formula,

$$\chi(Y_n, \mathcal{F}(k)) = (2 - 2g_n)(k+1) - kc_n.$$

Now according to ([4], 12.9.4), $c_n = \phi(p^n)c_0$ and $2g_n - 2 + c_n = p^n\phi(p^n)w$. After a brief calculation, one finds that the left hand difference is equal to

$$w(k+1)(p^{2n} - p^{2n-1} - (p^{2n-2} - p^{2n-3})) - c_0(p^n - 2p^{n-1} + p^{n-2}). \qquad (12.2)$$

Now the right hand side is equal to

$$\dim_{\mathbf{C}} S_{k+2}(\mathcal{P}, \Gamma_1(p^n)) - \dim_{\mathbf{C}} S_{k+2}(\mathcal{P}, [\Gamma_0(p^n), n-1, n-1])$$

and by the description of modular forms in section 6,

$$S_{k+2}(\mathcal{P}, \Gamma_1(p^n)) = H^0(\overline{\mathcal{M}}(\mathcal{P} \otimes \mathbf{C}, \Gamma_1(p^n)), \Omega^1 \otimes \omega^{k-2})$$

and

$$S_{k+2}(\mathcal{P}, [\Gamma_0(p^n), n-1, n-1]) = H^0(\overline{\mathcal{M}}(\mathcal{P} \otimes \mathbf{C}, [\Gamma_0(p^n), n-1, n-1]), \Omega^1 \otimes \omega^{k-2}).$$

Now the degree of the line bundle ω on $\overline{\mathcal{M}}(\mathcal{P} \otimes \mathbf{C}, \Gamma_1(p^n))$ is $\deg(\mathcal{P} \otimes \mathbf{C}, \Gamma_1(p^n))/24$ (and similarly for $(\mathcal{P} \otimes \mathbf{C}, [\Gamma_0(p^n), n-1, n-1])$), so applying the Riemann-Roch theorem and ([4], 10.13.12), we find that the right hand difference is equal to

$$\frac{(k+1)}{24}\left(\deg(\mathcal{P} \otimes \mathbf{C}, \Gamma_1(p^n)) - \deg(\mathcal{P} \otimes \mathbf{C}, [\Gamma_0(p^n), n-1, n-1])\right)$$
$$- \frac{1}{2}\left(c(\mathcal{P} \otimes \mathbf{C}, \Gamma_1(p^n)) - c(\mathcal{P} \otimes \mathbf{C}, [\Gamma_0(p^n), n-1, n-1])\right)$$

where $c(\mathcal{P})$ is the number of cusps for the moduli problem $\mathcal{P}$. Note that, since $\overline{\mathcal{M}}(\mathcal{P})$ is smooth over $\mathbf{Z}[\zeta_{p^n}, \zeta_N, 1/N]$, we have $c(\mathcal{P} \otimes \mathbf{C}) = c(\mathcal{P}) = c_0$ and $\deg(\mathcal{P} \otimes \mathbf{C}) = \deg(\mathcal{P}) = 24w$. Another computation then yields the fact that the right hand difference is

$$w(k+1)(p^{2n} - p^{2n-1} - (p^{2n-2} - p^{2n-3})) - c_0(p^n - 2p^{n-1} + p^{n-2}).$$

Comparing with (12.2) yields the proposition. Q.E.D.

Finally, it remains to remove the restriction that Γ be the trivial subgroup of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$. But this follows from the facts that if a group Γ acts on a moduli

problem $\mathcal{P}$, then $\overline{M}(\mathcal{P}/\Gamma) \cong \overline{M}(\mathcal{P})/\Gamma$ ([4], 8.1.5) and that the cohomology with rational coefficients of a quotient is gotten by taking invariants. This finishes the proof of the general case of the theorem.

References

1 Deligne, P.: Formes modulaire et représentations ℓ-adiques. In: Seminaire Bourbaki 1968/69 (Lect. Notes in Math. 179.) pp. 139-172 Berlin Heidelberg New York: Springer 1969

2 Deligne, P. and Rapoport, M.: Les schémas de modules de courbes elliptiques. In: Kuyk, W. and Deligne, P. (Eds.) Modular Functions of One Variable II (Lect. Notes in Math. 349.) pp. 143-316 Berlin Heidelberg New York: Springer 1973

3 Grothendieck, A.: Formule de Lefschetz et rationalité des fonctions L, Seminaire Bourbaki 1964/65, exposé 279. In: Grothendieck, A. (Ed.) Dix Exposés sur la Cohomologie des Schemas. pp. 31-45 Amsterdam: North-Holland 1968

4 Katz, N. and Mazur, B.: Arithmetic Moduli of Elliptic Curves. Princeton: Princeton University Press 1985

5 Milne, J.S.: Etale Cohomology. Princeton: Princeton University Press 1980

6 Ogg, A.: On the eigenvalues of Hecke operators. Math. Ann. **179** (1969) 101-108

7 Shimura, G.: Sur les intégrales attachées aux formes automorphes. J. Math. Soc. Japan **11** (1959) 291-311

8 Shimura, G.: On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields. Nagoya Math. J. **43** (1971) 199-208

9 Swinnerton-Dyer, H.P.F.: The conjectures of Birch and Swinnerton-Dyer, and of Tate. In: Springer, T.A. (Ed.) Proceedings of a Conference on Local Fields. pp. 132-157 Berlin Heidelberg New York: Springer 1967

10 Tate, J.: Algebraic cycles and poles of zeta functions. In: Schilling, O.F.G. (Ed.) Arithmetical Algebraic Geometry. pp. 93-110 New York: Harper and Row 1965

11 Ulmer, D.L.: On universal curves over Igusa curves. (To appear in Inv. Math.) (1988)

12 Wiles, A.: Modular curves and the class group of $\mathbf{Q}(\zeta_p)$. Invent. Math. **58** (1980) 1-35