

A construction of local points on elliptic curves over modular curves

Douglas L. Ulmer

Department of Mathematics
University of Arizona
Tucson, AZ 85721

January 20, 1996

Let K be the function field of a curve over a finite field of characteristic p , v a place of K , and K_v the completion of K at v . If E is an elliptic curve over K then by the Mordell-Weil theorem $E(K)$ is a finitely generated abelian group. On the other hand $E(K_v)$ is quite large: for example, if E has split multiplicative reduction at v , then $E(K_v)$ has a subgroup of finite index isomorphic as topological group to the direct product of countably many copies of \mathbf{Z}_p , the p -adic integers.

In this paper we study these groups when K is the function field of a modular curve, v is a certain (cuspidal) place, and E is the “universal” elliptic curve over K . We will give an explicit construction using modular forms of a finite rank \mathbf{Z}_p -module S and an injection $\phi : S \rightarrow E(K_v)$; the rank of S is (at most) the order of vanishing of the Hasse-Weil L -function of E over K . The main result (Theorem 5) says that $\phi(S)$ contains a finite index subgroup of the image of the natural inclusion $\iota : E(K) \rightarrow E(K_v)$. (The injection ϕ is constructed using a particularly nice logarithm from a finite index subgroup of $E(K_v)$ to a certain group of formal power series with coefficients in a ring of Witt vectors. That $\phi(S)$ contains a finite index subgroup of $\iota(E(K))$ is proven by exploiting the action of Hecke operators on $E(K)$, on a group closely related to $E(K_v)$, and on a certain cohomology group.)

The very explicit nature of the map ϕ suggests the possibility constructing points in $E(K)$ itself. What is needed is to specify the \mathbf{Z} -module $\phi^{-1}(\iota(E(K)))$ inside the \mathbf{Z}_p -module S . (This construction would be in the same spirit as a result of Rubin [4].) In the last section of the paper we propose a candidate for this module when the L -function of E vanishes to order precisely 1 at the center of its critical strip. We remark that our conjectural construction of global points uses neither Heegner points nor Drinfeld modules.

The main theorem also has an interesting consequence for automorphic forms over \mathbf{Q} which we can state without any further preliminaries.

This research was partially supported by NSF grant DMS 9302976.

THEOREM 1. *Let p be a prime number and N a positive integer not divisible by p . If the conjecture of Birch and Swinnerton-Dyer holds for elliptic curves over function fields of characteristic p , then the Atkin U_p operator acts semi-simply on the space of modular forms of weight 3 and level $\Gamma_1(pN)$.*

(The idea is that the main theorem and a result of Voloch give inequalities $\text{Rank}_{\mathbf{Z}} E(K) \leq \text{Rank}_{\mathbf{Z}_p} S \leq \text{ord}_{s=1} L(E/K, s)$ and the conjecture of Birch and Swinnerton-Dyer implies that we have equalities. But the rank of S is equal to the dimension of a certain space of eigenvectors of U_p , while the order of vanishing of $L(E/K, s)$ is equal to the multiplicity of a certain eigenvalue. Their equality implies the semisimplicity of U_p .)

The conclusion of the theorem (which seems to have been doubted by many experts) is equivalent to the following: if f is a modular form of weight $k = 3$ on $\Gamma_0(N)$ with character ϵ and $T_p f = a_p f$, then the polynomial $T^2 - a_p T + \epsilon(p)p^{k-1}$ has distinct roots. With a mild generalization of the method, one should be able to prove that the Tate conjecture for varieties over finite fields of characteristic p implies the analog of the conclusion of Theorem 1 for modular forms of all odd weights $k \geq 3$. (After this paper was written, Bas Edixhoven proved that the conclusion of Theorem 1 holds unconditionally for modular forms of weight $k = 2$ and level $\Gamma_0(pN)$ with trivial character, if $p > 2$.)

It is a pleasure to thank Barry Mazur for his helpful suggestions on the exposition in this paper.

1. Elliptic curves over modular curves.

Fix a prime number p , a non-negative integer e , a positive integer N prime to p , and a finite field \mathbf{F} of characteristic p . Let $I = Ig_1(p^e N)$ be the modular curve over \mathbf{F} for simultaneous $\Gamma_1(N)$ - and Igusa p^e -structures. (If $e = 0$, this is just $X_1(N)$ over \mathbf{F} .) If we assume, as we always will, that $p^e N \geq 3$, then an open subset of I is a fine moduli space for a suitable moduli problem and we define $\mathcal{E} \rightarrow I$ to be the Néron model of the universal curve. Let K be the function field $\mathbf{F}(I)$ and E/K the generic fiber of the universal curve. This curve was studied in [6].

The Hasse-Weil L -function $L(E/K, s)$ is closely related to the action of Hecke operators on modular forms. For example, when $e = 0$ and $\mathbf{F} = \mathbf{F}_p$, we have

$$\begin{aligned} L(E/K, s) &= \det(1 - T_p p^{-s} + \langle p \rangle_N p^{2-2s} | S_3(\Gamma_1(N))) \\ &= \det(1 - U_p p^{-s} | S_3(\Gamma_1(pN))^{p\text{-old}}). \end{aligned}$$

(The notation here is standard, except perhaps for “ p -old” which stands for the subspace of forms old at p , i.e., coming from level N .) Using this connection, one can exhibit many examples where $L(E/K, s)$ vanishes at $s = 1$. For example:

- (1) If $p^e N = p \equiv 3 \pmod{4}$, $p > 3$, and $\mathbf{F}_{p^2} \subseteq \mathbf{F}$, then $\text{ord}_{s=1} L(E/K, s)$ is at least as large as the class number of $\mathbf{Q}(\sqrt{-p})$. In particular, it is positive.

- (2) A similar statement holds when $p \equiv 1 \pmod{4}$ and $N = 4$.
- (3) Let $N > 4$ be such that $-N$ is the discriminant of an imaginary quadratic field of class number h in which p is inert. Taking $e = 0$, for any \mathbf{F} the order of vanishing of the L -function is bounded below by h and if $\mathbf{F}_{p^2} \subseteq \mathbf{F}$, it is bounded below by $2h$.
- (4) All of the above bounds come from CM modular forms, but there are occasionally more zeroes. For example, if $p = 89$, $e = 0$, and $N = 19$, then Example 3 shows that the order of vanishing is always at least 1 and is at least 2 if $\mathbf{F}_{89^2} \subseteq \mathbf{F}$. In fact, it is precisely 3 if $\mathbf{F}_{89^2} \not\subseteq \mathbf{F}$ and precisely 6 if $\mathbf{F}_{89^2} \subseteq \mathbf{F}$. (This example is due to Atkin.)

(These assertions follow from the L -function calculations of [7] and the construction of CM modular forms (e.g., [2, 4.8.2]); see also [5] where this type of phenomenon was first observed.)

According to the conjecture of Birch and Swinnerton-Dyer, the rank of the Mordell-Weil group $E(K)$ should be equal to the order of vanishing of $L(E/K, s)$ at $s = 1$. Thus in many cases there should be points of infinite order in $E(K)$.

2. Modular forms.

For a positive integer M let $S_k(\Gamma_1(M))$ be the complex vector space of modular forms of weight k on $\Gamma_1(M)$ and let $S_k(\Gamma_1(M); \mathbf{Z})$ be the subgroup of forms all of whose Fourier coefficients at the standard cusps ∞ are integers; this is a \mathbf{Z} -structure on $S_k(\Gamma_1(M))$. For any commutative ring R define $S_k(\Gamma_1(M); R)$ as $S_k(\Gamma_1(M); \mathbf{Z}) \otimes R$. These spaces carry R -linear actions of Hecke operators T_ℓ for $\ell \nmid M$ and U_ℓ for $\ell | M$ as well as ‘‘diamond bracket’’ operators $\langle d \rangle_M$ for $d \in (\mathbf{Z}/M\mathbf{Z})^\times$. For a prime ℓ dividing M , define $S_k(\Gamma_1(M); R)^{\ell\text{-old}}$ to be the submodule spanned by the images of two copies of $S_k(\Gamma_1(M/\ell); R)$ in $S_k(\Gamma_1(M); R)$ under the standard degeneracy maps. This submodule is preserved by the Hecke operators.

We will need later to refer to the following possibility.

HYPOTHESIS 2. *For every $f \in S_3(\Gamma_1(N))$ which is an eigenvector for T_p and $\langle p \rangle_N$ (say $T_p f = a f$ and $\langle p \rangle_N f = \epsilon f$), the polynomial $T^2 - aT + \epsilon p^2$ has distinct roots.*

Let $W = W(\mathbf{F})$ be the ring of Witt vectors over \mathbf{F} and $\sigma : W \rightarrow W$ the automorphism induced by the Frobenius of \mathbf{F} . Then $S_k(\Gamma_1(M); W)$ is a finite rank W -module. In addition to the Hecke action, it carries a \mathbf{Z}_p -linear action of σ . Now define

$$M(R) = \begin{cases} S_3(\Gamma_1(p^e N); R) & \text{if } e > 0 \\ S_3(\Gamma_1(pN); R)^{p\text{-old}} & \text{if } e = 0 \end{cases}$$

and let

$$S = \{f \in M(W) \mid \sigma^{-1} U_p f = p f\}.$$

Clearly S is a free \mathbf{Z}_p -module of finite rank.

PROPOSITION 3.

$$\text{Rank}_{\mathbf{Z}_p} S \leq \text{ord}_{s=1} L(E/K, s)$$

with equality if Hypothesis 2 holds. If Hypothesis 2 fails, then for large enough \mathbf{F} , we have strict inequality.

PROOF: Write $|\mathbf{F}| = p^f$ and $r = \text{ord}_{s=1} L(E/K, s)$. It follows from the computation in [7] of the L -function and basic facts about old and new forms that r is equal to the multiplicity of p^f as an eigenvalue of U_p^f on $M(\mathbf{C})$ or equivalently on $M(\mathbf{Z}_p)$ viewed as a free module over \mathbf{Z}_p . Thus r is also the sum of the multiplicities of ζp as eigenvalue of U_p on $M(\mathbf{Z}_p)$ where ζ runs through μ_f , the f -th roots of unity.

On the other hand, W is a free \mathbf{Z}_p -module of rank f and the \mathbf{Z}_p -linear automorphism σ has eigenvalues $\zeta \in \mu_f$, each occurring with multiplicity one. Since $M(W) = M(\mathbf{Z}_p) \otimes_{\mathbf{Z}_p} W$, the multiplicity of p as an eigenvalue of the \mathbf{Z}_p -linear operator $U_p \otimes \sigma^{-1}$ on $M(W)$ is r . This gives the desired inequality. Moreover, Hypothesis 2 implies U_p is semisimple on its generalized eigenspaces for the eigenvalues ζp ($\zeta \in \mu_f$), so equality holds; for f sufficiently divisible, the converse is true as well.

3. A result on Witt vectors.

For any commutative ring R , let $R[[q]]$ be the ring of formal power series in an indeterminate q and let $\Lambda(R)$ be the multiplicative group $1 + qR[[q]]$ (the additive group of the big Witt vectors over R). Any $u \in \Lambda(R)$ can be written uniquely $u = \prod_{n \geq 1} (1 - c_n q^n)$ with $c_n \in R$. For each positive integer ℓ , define homomorphisms $\mathcal{F}_\ell, \mathcal{V}_\ell : \Lambda(R) \rightarrow \Lambda(R)$ as follows: Let $\mathcal{V}_\ell(u) = \prod (1 - c_n q^{n\ell})$ and for \mathcal{F}_ℓ , let ξ_1, \dots, ξ_ℓ be the formal ℓ -th roots of q . Then $\prod_{i=1}^\ell \prod_{n \geq 1} (1 - c_n \xi_i^n)$ is again a series in q which we define to be $\mathcal{F}_\ell(u)$.

Let $A(R) = qR[[q]]$, the additive group of formal series without constant term. If $\sigma : R \rightarrow R$ is a ring homomorphism, p is a positive integer, and $a \in R$, define

$$A(R)^{(a)} = \left\{ \sum a_n q^n \mid a_{pn} = a \sigma(a_n) \right\}.$$

For each positive integer ℓ , define homomorphisms $F_\ell, V_\ell, \theta : A(R) \rightarrow A(R)$ by the formulae

$$F_\ell \left(\sum a_n q^n \right) = \sum a_{n\ell} q^n \quad V_\ell \left(\sum a_n q^n \right) = \sum a_n q^{n\ell} \quad \theta \left(\sum a_n q^n \right) = \sum n a_n q^n.$$

We have

$$(1) \quad \ell V_\ell \theta = \theta V_\ell \text{ and } F_\ell \theta = \ell \theta F_\ell.$$

and if R is an algebra over the localization $\mathbf{Z}_{(p)}$, then $\theta : A(R)^{(a)} \rightarrow A(R)^{(pa)}$ is an isomorphism.

(All these definitions also make sense if R is replaced by a ring without identity, e.g., an ideal of R .)

Now let p be a prime number, \mathbf{F} a finite field of characteristic p , and $W = W(\mathbf{F})$ the (p -) Witt vectors on \mathbf{F} ; let σ be the automorphism of W induced by the Frobenius of \mathbf{F} . For $u \in \Lambda(W)$, we will write $\bar{u} \in \Lambda(\mathbf{F})$ for the image of u under the map induced by $W \rightarrow \mathbf{F}$ (reduction of coefficients modulo p). For $f = \sum a_n q^n$ in $A(W)$, define a formal series

$$u_f = \exp(-\theta^{-1}f) = \exp\left(-\sum_{n \geq 1} \frac{a_n}{n} q^n\right) = \sum_{i=0}^{\infty} \frac{1}{i!} \left(-\sum_{n \geq 1} \frac{a_n}{n} q^n\right)^i$$

The map $f \mapsto u_f$ is a homomorphism $A(W) \rightarrow \Lambda(\text{Frac } W)$.

The following is the main result of this section. It is undoubtedly well-known to experts, but we are not aware of a suitable reference.

PROPOSITION 4. *For every $f \in A(W)^{(1)}$, u_f lies in $\Lambda(W)$ and $f \mapsto \bar{u}_f$ defines an isomorphism $\varepsilon : A(W)^{(1)} \rightarrow \Lambda(\mathbf{F})$.*

We will write λ for the inverse of ε .

PROOF: Define, for $u = \prod(1 - c_n q^n)$ in $\Lambda(W)$,

$$\begin{aligned} f_u &= -\theta \log u = \theta \sum_{n \geq 1} \sum_{m \geq 1} \frac{c_n^m q^{nm}}{m} \\ &= \sum_{m, n \geq 1} n c_n^m q^{nm} \\ &= \sum_{n \geq 1} a_n q^n \text{ with } a_n = \sum_{d|n} d c_d^{n/d}. \end{aligned}$$

The map $u \mapsto f_u$ is a right inverse to $f \mapsto u_f$ (i.e., $u \mapsto f_u \mapsto u_{f_u}$ is the identity) so it is injective and its image is

$$A' := \left\{ \sum a_n q^n \mid a_{pn} \equiv \sigma(a_n) \pmod{pnW} \right\}.$$

Indeed, f_u lies in A' because

$$\begin{aligned} a_{pn} &= \sum_{d|pn} d c_d^{pn/d} \\ &\equiv \sum_{d|n} d c_d^{pn/d} \pmod{pnW} \\ &\equiv \sum_{d|n} d \sigma(c_d)^{n/d} \pmod{pnW} \\ &= \sigma(a_n). \end{aligned}$$

Conversely, given $f = \sum a_n q^n$ in A' , we can solve inductively for $c_m \in \text{Frac}(W)$ so that $u = \prod(1 - c_m q^m) \mapsto f$. We must have

$$\begin{aligned} mc_m &= a_m - \sum_{\substack{d|m \\ d \neq m}} dc_d^{m/d} \\ &\equiv a_m - \sum_{d|(m/p)} dc_d^{m/d} \pmod{mW} \\ &\equiv a_m - \sigma(a_{m/p}) \pmod{mW} \\ &\equiv 0 \pmod{mW} \end{aligned}$$

since f was in A' . Thus $c_m \in W$. Since $A^{(1)} \subseteq A'$, this proves that for $f \in A^{(1)}$, u_f lies in $\Lambda(W)$, and so $f \mapsto \overline{u_f}$ defines a map $\varepsilon : A^{(1)} \rightarrow \Lambda(\mathbf{F})$.

Similarly, the image of the subgroup $\Lambda(pW)$ under $u \mapsto f_u$ is

$$A'' := \left\{ \sum a_n q^n \mid a_n \equiv 0 \pmod{pnW} \right\}.$$

Thus $\Lambda(\mathbf{F}) \cong \Lambda(W)/\Lambda(pW) \cong A'/A''$. I claim that $A' = A^{(1)} \oplus A''$ and so ε is an isomorphism. Indeed, define $\pi : A' \rightarrow A^{(1)}$ by $\pi(\sum a_n q^n) = \sum b_n q^n$ with $b_n = \lim_{i \rightarrow \infty} \sigma^{-i} a_{p^i n}$. Then π is a projection and $f - \pi(f) \in A''$. On the other hand, if $f = \sum a_n q^n$ is in $A'' \cap A^{(1)}$, then $a_n = \sigma^{-i} a_{p^i n} \equiv 0 \pmod{p^i nW}$ for all $i, n > 0$, so $a_n = 0$ for all $n > 0$ and $f = 0$. This proves the claim and finishes the proof of the proposition.

We leave it as an easy exercise for the reader to check that for every ℓ prime to p we have

$$(2) \quad \lambda \mathcal{F}_\ell = F_\ell \lambda \text{ and } \lambda \mathcal{V}_\ell = \ell V_\ell \lambda.$$

4. Cusps and local points.

Fix once and for all a place v_0 of K corresponding to an unramified cusp of I , i.e., a cusp where j has a simple pole. (Here $j \in K$ is the standard elliptic modular function.) This cusp will play the role of the standard cusp ∞ on $X_1(p^e N)$ over the complex numbers. Let K_{v_0} be the completion of K at v_0 . There is a natural uniformizer at v_0 , namely

$$q = j^{-1} + 744j^{-2} + 750420j^{-3} + \dots$$

Thus $K_{v_0} \cong \mathbf{F}_{v_0}((q))$ where \mathbf{F}_{v_0} is the residue field at v_0 .

Since E is the generic fiber of the universal curve, over K_{v_0} it is canonically isomorphic to a one-sided Tate curve whose period is q . Thus

$$E(K_{v_0}) \cong \mathbf{F}_{v_0}((q))^\times / q^{\mathbf{Z}} \cong F_{v_0}[[q]]^\times$$

and writing $E(K_{v_0})_1$ for the kernel of reduction at v_0 , we have

$$(3) \quad E(K_{v_0})_1 \cong 1 + q\mathbf{F}_{v_0}[[q]] = \Lambda(\mathbf{F}_{v_0}).$$

We will use this description of the local points to construct an injective homomorphism from the module S of Section 2 to $E(K_{v_0})_1$.

5. The main theorem.

Recall the module S of modular forms with coefficients in W defined in Section 2; by Proposition 3 it has \mathbf{Z}_p -rank bounded above by the order of vanishing of $L(E/K, s)$ at $s = 1$. Taking q -expansions at the standard cusps ∞ defines an injection from S into the module $A(W)^{(p)}$ of formal q -expansions studied in Section 3. We have an isomorphism $\theta^{-1} : A(W)^{(p)} \rightarrow A(W)^{(1)}$ and, by Proposition 4, an isomorphism $\varepsilon : A(W)^{(1)} \rightarrow \Lambda(\mathbf{F})$. Finally, we have a natural inclusion $\Lambda(\mathbf{F}) \subseteq \Lambda(\mathbf{F}_{v_0})$ and by Equation 3 an identification $\Lambda(\mathbf{F}_{v_0}) \cong E(K_{v_0})_1$. Composing these maps we have

$$S \xrightarrow{q\text{-expansion}} A^{(p)} \xrightarrow{\theta^{-1}} A^{(1)} \xrightarrow{\varepsilon} \Lambda(\mathbf{F}) \xrightarrow{\text{Equation 3}} E(K_{v_0})$$

$$f = \sum a_n q^n \xrightarrow{\hspace{10em}} \overline{\exp\left(-\sum \frac{a_n}{n^2} q^n\right)}$$

We will write $\phi : S \hookrightarrow E(K_{v_0})$ for this composition. Let $E(K)_1$ denote the set of points in $E(K)$ reducing to the identity at all unramified cusps; it is a subgroup of $E(K)$ of finite, prime-to- p index; let $\iota : E(K) \rightarrow E(K_{v_0})$ be the natural inclusion. Our main result is the following.

THEOREM 5.

$$\iota(E(K)_1) \subseteq \phi(S)$$

REMARKS:

(1) From another point of view, this theorem yields an injection $E(K)_1 \hookrightarrow S$ whose image is a free, finite-rank \mathbf{Z} -module. Knowledge of this \mathbf{Z} -module would yield an explicit construction of points of infinite order in $E(K)$. In Section 9 we will suggest a candidate when $L(E/K, s)$ vanishes simply at $s = 1$.

(2) Since the index $[E(K) : E(K)_1]$ is prime to p , $E(K)_1 \hookrightarrow S$ extends to $E(K) \hookrightarrow S$.

(3) By a theorem of Voloch [9, Theorem 4], the natural map $E(K)_1 \otimes \mathbf{Z}_p \rightarrow E(K_{v_0})_1$ is injective, and therefore so is $E(K)_1 \otimes \mathbf{Z}_p \rightarrow S$. This implies that $\text{Rank}_{\mathbf{Z}} E(K) \leq \text{Rank}_{\mathbf{Z}_p} S$ and so if the conjecture of Birch and Swinnerton-Dyer is true then equality holds in Proposition 3. This proves Theorem 1.

(4) Again assuming the conjecture of Birch and Swinnerton-Dyer, the image of $E(K)_1 \otimes \mathbf{Z}_p \rightarrow S$ has finite index in S . It would be interesting to relate this index to other invariants of E .

Before launching into the proof of Theorem 5, let us explain the main ideas. In Section 6 we define a cycle class map from $E(K)$ to $H^2(M)$, the cohomology of a certain motive related to modular forms of weight 3 and level $\Gamma_1(p^e N)$. In Section 7 we define a ring of Hecke operators acting on $E(K)$, $H^2(M)$, and $E(K_{v_0})_1 \cong \Lambda(\mathbf{F}_{v_0})$. (Actually, they are defined on $\prod_v \Lambda(\mathbf{F}_v)$ where the product extends over all unramified cusps of I .) The maps $E(K) \rightarrow H^2(M)$ and $E(K)_1 \rightarrow \prod_v \Lambda(\mathbf{F}_v)$ are

equivariant and we have detailed information about the Hecke action on $H^2(M)$ from [8].

Now suppose for a moment that on modular forms of weight 3 and level $\Gamma_1(p^e N)$ the eigenvalues of Hecke operators are rational integers and the operators U_ℓ ($\ell|N$) act semi-simply. Then the equivariance of the cycle class map and the results of [8] imply that $E(K) \otimes \mathbf{Q}$ can be written as a direct sum of lines stable under the Hecke algebra and the action on each line is via a known character. The same is thus true of the image of $E(K)_1$ in $\prod_v \Lambda(\mathbf{F}_v)$. But eigenvectors in $\prod_v \Lambda(\mathbf{F}_v)$ are determined up to a scalar by their eigenvalues (this is a multiplicity one statement, or better, a type of q -expansion principle). The vectors coming from $E(K)_1$ are then visibly in the image of $S \rightarrow \prod_v \Lambda(\mathbf{F}_v)$ and this proves the theorem. Of course the suppositions made at the beginning of this paragraph do not hold in general; to handle this we have to extend scalars to $\overline{\mathbf{Q}}_p$ and we have to deal only with forms new at N and deduce the general result by induction on N . The full argument is given in Section 8.

6. Cycle classes.

Recall the universal curve $\mathcal{E} \rightarrow I$ which is an elliptic surface over \mathbf{F} . There are N canonical sections of \mathcal{E} over I whose images are N -torsion points in each fiber. The group $\mathbf{Z}/N\mathbf{Z}$ acts on \mathcal{E} by translation by these sections and μ_2 acts by inversion in each fiber; together we have an action of the semi-direct product $\mathbf{Z}/N\mathbf{Z} \rtimes \mu_2$. Let $\epsilon : \mathbf{Z}/N\mathbf{Z} \rtimes \mu_2 \rightarrow \mu_2$ be the character which is 1 on $\mathbf{Z}/N\mathbf{Z}$ and the identity on μ_2 . Define $H^2(\mathcal{E}) = H_{\text{cris}}^2(\mathcal{E}/W) \otimes_W \text{Frac}(W)$ and $H^2(M) = H^2(\mathcal{E})(\epsilon)$ where (ϵ) means the subspace on which the group $\mathbf{Z}/N\mathbf{Z} \rtimes \mu_2$ acts via the character ϵ . We view $H^2(M)$ as the cohomology of a certain motive which was studied, for example, in [8]. We view the cup product on $H^2(\mathcal{E})$ and its restriction to $H^2(M)$ as a $\text{Frac}(W)$ -valued pairing via the canonical isomorphism $H_{\text{cris}}^4(\mathcal{E}/W) \cong W$. (We could use any other reasonable cohomology theory here, such as ℓ -adic cohomology, but because we will eventually want p -adic coefficients, it is most natural to work with crystalline cohomology.)

We are going to define a homomorphism $E(K) \rightarrow H^2(M)$ which is injective modulo torsion and with respect to which the height pairing and cup product enjoy a certain compatibility. For any point $P \in E(K)$, define \tilde{P} to be the section of \mathcal{E} over I whose generic fiber is P , and let $[\tilde{P}]$ be the cycle class of \tilde{P} in $H^2(\mathcal{E})$. The map $P \mapsto [\tilde{P}]$ is not in general a homomorphism, so we need to make some corrections to it.

Write $\tilde{0}$ for the 0-section, f_1, \dots, f_k for the components of reducible fibers which do not meet the 0-section, and f_0 for one irreducible fiber. As is well known (e.g., [5, §1]), the cycle classes $[\tilde{0}], [f_i]$ ($i = 0, \dots, k$) of these curves are independent in $H^2(\mathcal{E})$ and we let L denote the subspace they generate. The restriction of the cup product to L is non-degenerate. (This follows from the fact that the restriction of cup product to the span of the cycle classes of a given fiber is negative semi-definite

with kernel spanned by the class of the entire fiber.)

PROPOSITION 6.

- (1) The map $P \mapsto [\tilde{P}]$ is a homomorphism $E(K) \rightarrow H^2(\mathcal{E})/L$ which is injective modulo torsion.
- (2) For each $P \in E(K)$ there exists a unique element $\psi(P) \in H^2(\mathcal{E})$ mapping to $[\tilde{P}] \in H^2(\mathcal{E})/L$ such that the cup products $\psi(P) \cup [\tilde{0}]$ and $\psi(P) \cup [f_i]$ ($i = 0, \dots, k$) vanish.
- (3) The map $P \mapsto \psi(P)$ is a homomorphism $E(K) \rightarrow H^2(\mathcal{E})$ whose image lies in $H^2(M)$.
- (4) If $\langle \cdot, \cdot \rangle$ denotes the canonical height pairing on $E(K)$, then

$$\langle P, Q \rangle = -(\psi(P) \cup \psi(Q)) \log |\mathbf{F}|.$$

PROOF: First we note that the assertion of (4) is a well-known property of the global height in the function field case [3]. More generally, $\langle P, Q \rangle = -(\psi(P) \cup [\tilde{Q}]) \log |\mathbf{F}|$, or in other words, we need only “correct” one of P or Q .

For (1), suppose that $P+Q=R$. Then the divisor $(P)+(Q)$ is linearly equivalent to $(Q)+(0)$ on E/K . If $f \in K(E) = \mathbf{F}(\mathcal{E})$ is the rational function on E/K whose divisor is $(P)+(Q)-(R)-(0)$, then the divisor of f on \mathcal{E} is $\tilde{P}+\tilde{Q}-\tilde{R}-\tilde{0}$ plus a sum of curves lying in the fibers of $\mathcal{E} \rightarrow I$. This proves that $P \mapsto [\tilde{P}]$ is a homomorphism. Its injectivity modulo torsion follows from (4) and the non-degeneracy of the height pairing. (Of course one can give a more direct proof!)

The existence and uniqueness in (2) both follow the fact that the restriction of the cup product to L is non-degenerate. (Note that for the existence of $\psi(P)$, we need *rational* coefficients.)

The fact that ψ is a homomorphism follows from (1) and the uniqueness in (2). To show that the image of ψ lies in $H^2(M)$, we have to check that $(-1)^*\psi(P) = -\psi(P)$ and $t^*\psi(P) = \psi(P)$, where (-1) and t are inversion in the fibers and translation by a point of order N respectively. We have that $t^*\psi(P) \cup [\tilde{0}] = \psi(P) \cup [t\tilde{0}]$ which vanishes since $t\tilde{0}$ restricts to a torsion section in the generic fiber and thus is in the kernel of the height pairing. Also, $t^*\psi(P) \cup [f_i] = \psi(P) \cup [tf_i] = 0$ and $t^*\psi(P)$ maps to $[\tilde{P}]$ in $H^2(\mathcal{E})/L$ so by the uniqueness in (2), $t^*\psi(P) = \psi(P)$. Similarly, by the uniqueness in (2), $(-1)^*\psi(P) = \psi(-P)$ which is $-\psi(P)$ since ψ is a homomorphism. This completes the proof of (3) and of the proposition.

With a little more work one can show that $H^2(M) = L^\perp$ and so $H^2(\mathcal{E}) = H^2(M) \oplus L$ (an orthogonal direct sum with respect to cup product).

7. Hecke operators.

We are going to define Hecke operators on $E(K)$, $H^2(M)$, and some related groups. We have already defined endomorphisms $\langle d \rangle_{p^e}$ ($d \in (\mathbf{Z}/p^e\mathbf{Z})^\times$), $\langle d \rangle_N$ ($d \in (\mathbf{Z}/N\mathbf{Z})^\times$), T_ℓ ($\ell \nmid pN$), and U_ℓ ($\ell | N$) on $H^2(M)$ in [8, §2].

To define the relevant operators on $E(K)$, first fix a prime ℓ not dividing pN . Let I_ℓ be the modular curve over \mathbf{F} for simultaneous $\Gamma_0(\ell)$ -, $\Gamma_1(N)$ - and $\text{Ig}(p^e)$ -structures, and let K_ℓ be the function field $\mathbf{F}(I_\ell)$. There are two maps $\pi_1, \pi_2 : I_\ell \rightarrow I$, induced respectively by “forgetting the $\Gamma_0(\ell)$ -structure” and “dividing by the $\Gamma_0(\ell)$ -structure”. These induce two field inclusions $\pi_i^* : K \hookrightarrow K_\ell$, and, defining $E_{\ell,i} = E \times_{\pi_i} \text{Spec } K_\ell$, we have a universal ℓ -isogeny $\Phi : E_{\ell,1} \rightarrow E_{\ell,2}$. Let Φ^\vee be the dual isogeny. Finally, define a Hecke operator $T_\ell : E(K) \rightarrow E(K)$ as the composition

$$E(K) \xrightarrow{\pi_2^*} E_{\ell,2}(K_\ell) \xrightarrow{\Phi^\vee} E_{\ell,1}(K_\ell) \xrightarrow{\text{Tr}_{K_\ell/K}} E(K).$$

(We note that T_ℓ is a group endomorphism of $E(K)$, but is not an endomorphism of E as an algebraic group over K .)

For primes $\ell|N$, write $N = \ell^a N'$ with $\ell \nmid N'$. Then we have a similar construction where I_ℓ is the modular curve for simultaneous $\text{Ig}(p^e)$ -, $\Gamma_1(N')$ -, and $[\Gamma_0(\ell^{a+1}); a, 0]$ -moduli problems. (See [8, §2] for the definition of this last moduli problem and for more details.) This defines an operator U_ℓ for primes $\ell|N$.

Finally, to define endomorphisms $\langle d \rangle_{p^e}$ and $\langle d \rangle_N$ of $E(K)$, we just remark that operators with these names act on I , thus on K ; as E/K is isomorphic to its pull-back via $\langle d \rangle_{p^e}$ and $\langle d \rangle_N$, these operators act naturally on $E(K)$.

We also need the action of Hecke operators on local points. However, the fixed cusp v_0 is not preserved by the Hecke correspondences, so we need to work with $\prod_v E(K_v)$ where the product extends over all unramified cusps. Let $C \subseteq I$ be the reduced subscheme of unramified cusps and let $\mathcal{O} = \Gamma(C, \mathcal{O}_C)$. We have an isomorphism

$$\begin{aligned} \mathcal{O} &\cong \left(\mathbf{F}^{(\mathbf{Z}/p^e\mathbf{Z})^\times} \right) \otimes_{\mathbf{F}} (\mathbf{F}[x]/\Phi_N(x)) \\ &\cong (\mathbf{F}[x]/\Phi_N(x))^{(\mathbf{Z}/p^e\mathbf{Z})^\times} \end{aligned}$$

where $R^{(\mathbf{Z}/p^e\mathbf{Z})^\times}$ means functions from $(\mathbf{Z}/p^e\mathbf{Z})^\times$ to R and Φ_N is the cyclotomic polynomial of order N . There are natural endomorphisms $\langle d \rangle_{p^e}$ and $\langle d \rangle_N$ of \mathcal{O} ; namely $(\langle d \rangle_{p^e} f)(g) = f(dg)$ ($d, g \in (\mathbf{Z}/p^e\mathbf{Z})^\times$, $f \in (\mathbf{F}[x]/\Phi_N(x))^{(\mathbf{Z}/p^e\mathbf{Z})^\times}$) and the action of $\langle d \rangle_N$ is induced by $x \mapsto x^d$.

As in Section 4, we have an identification

$$(4) \quad \prod_v E(K_v)_1 \cong \prod_v \Lambda(\mathbf{F}_v) \cong \Lambda(\mathcal{O}).$$

The operators $\langle d \rangle_{p^e}$ and $\langle d \rangle_N$ act on $\Lambda(\mathcal{O})$ via their action on \mathcal{O} , and thus also on $\prod_v E(K_v)_1$. If $u \in \Lambda(\mathcal{O})$, define $T_\ell u = (\langle \ell \rangle_{p^e} \mathcal{F}_\ell u)^\ell (\langle \ell \rangle_N \mathcal{V}_\ell u)$ and $U_\ell u = (\langle \ell \rangle_{p^e} \mathcal{F}_\ell u)^\ell$ where \mathcal{F}_ℓ and \mathcal{V}_ℓ are the endomorphisms of $\Lambda(\mathcal{O})$ defined in Section 3. We get endomorphisms T_ℓ and U_ℓ of $\prod_v E(K_v)_1$ via Equation 4.

Finally, note that $\langle d \rangle_{p^e}$ and $\langle d \rangle_N$ act on $\prod_v A(W(\mathbf{F}_v))^{(p)} = A(W(\mathcal{O}))^{(p)}$ via their action on \mathcal{O} . Define actions of T_ℓ and U_ℓ on $A(W(\mathcal{O}))^{(p)}$ by the formulae

$$\begin{aligned} T_\ell f &= \langle \ell \rangle_{p^e} F_\ell f + \ell^2 \langle \ell \rangle_N V_\ell f \\ U_\ell f &= \langle \ell \rangle_{p^e} F_\ell f \end{aligned}$$

where F_ℓ and V_ℓ are as in Section 3.

Recall that we have defined maps $\psi : E(K) \rightarrow H^2(M)$ and

$$\theta\lambda_C : \Lambda(\mathcal{O}) \cong \prod_v \Lambda(\mathbf{F}_v) \xrightarrow{\sim} \prod_v A(W(\mathbf{F}_v))^{(p)} \cong A(W(\mathcal{O}))^{(p)}.$$

Write

$$\iota_C : E(K)_1 \hookrightarrow \prod_v E(K_v)_1$$

for the obvious inclusion. (The subscripts C are meant to suggest the product over all unramified cusps.) We have identified $\prod_v E(K_v)_1$ with $\Lambda(\mathcal{O})$ in Equation 4.

PROPOSITION 7. *The maps ψ , $\theta\lambda_C$, and ι_C are equivariant for the actions of $\langle d \rangle_{p^e}$ ($d \in (\mathbf{Z}/p^e\mathbf{Z})^\times$), $\langle d \rangle_N$ ($d \in (\mathbf{Z}/N\mathbf{Z})^\times$), T_ℓ ($\ell \nmid pN$), and U_ℓ ($\ell|N$).*

PROOF: The equivariance of ψ follows from the construction of the operators on $H^2(M)$ in [8]. That of $\theta\lambda_C$ follows from Equations 1 and 2. The equivariance of ι_C follows from a computation which is almost identical to the that giving the action of Hecke operators on q -expansions of modular forms; we will not repeat it here.

8. Proof of Theorem 5.

For every divisor M of N we have an analogue of K (for level $p^e M$) and two embeddings into K . Let $E(K)^{N\text{-old}}$ be the subgroup of $E(K)$ generated by points which are defined over any of these subfields and let $E(K)^{N\text{-new}}$ be the orthogonal complement under the height pairing. Define $H^2(M)^{N\text{-old}}$, $H^2(M)^{N\text{-new}}$, $S^{N\text{-old}}$, and $S^{N\text{-new}}$ similarly.

Fix an algebraic closure $\overline{\mathbf{Q}}_p$ of \mathbf{Q}_p and an embedding $W \hookrightarrow \overline{\mathbf{Q}}_p$. Extending scalars in the cycle map $\psi : E(K)^{N\text{-new}} \rightarrow H^2(M)^{N\text{-new}}$ yields an injection

$$E(K)^{N\text{-new}} \otimes_{\mathbf{Z}} \overline{\mathbf{Q}}_p \rightarrow H^2(M)^{N\text{-new}} \otimes_{\text{Frac}(W)} \overline{\mathbf{Q}}_p$$

and the image lies in the subspace where Frobenius acts by p . To lighten notations, abbreviate this space as H . Applying [8, §2] and the theory of newforms, H breaks up into a direct sum of lines equivariant under the Hecke action. For each of these lines L there is an eigenform $f \in S^{N\text{-new}} \otimes_{\mathbf{Z}_p} \overline{\mathbf{Q}}_p$ such that if the eigenvalues of f are $\{a_\ell\}$ and its character is $\epsilon\eta$ with ϵ of level N , η of level p^e , then the eigenvalues of

T_ℓ and U_ℓ on L are $\{\eta^{-1}(\ell)a_\ell\}$, $\langle d \rangle_{p^e}$ acts on L via $\eta^{-1}(d)$, and $\langle d \rangle_N$ acts via $\epsilon(d)$. Since ψ is Hecke equivariant, the same decomposition holds for $E(K)^{N\text{-new}} \otimes \overline{\mathbf{Q}}_p$.

Let $P = \sum P_i \otimes c_i \in E(K)^{N\text{-new}} \otimes \overline{\mathbf{Q}}_p$ be an eigenvector corresponding to the package of eigenvalues $\{a_\ell\}$ and character $\epsilon\eta$; consider its image $g = \theta\lambda_C \iota_C(P)$ in $A(W(\mathcal{O}))^{(p)} \otimes_{\mathbf{Z}_p} \overline{\mathbf{Q}}_p$. By Proposition 7 we have $\langle d \rangle_{p^e} g = \eta^{-1}(d)g$ and $\langle d \rangle_N g = \epsilon(d)g$. We also have

$$\begin{aligned} \eta^{-1}(\ell)a_\ell g &= T_\ell g \\ &= \langle \ell \rangle_{p^e} F_\ell g + \ell^2 \langle \ell \rangle_N V_\ell g \\ &= \eta^{-1}(\ell) (F_\ell g + \ell^2 \eta \epsilon(\ell) V_\ell g) \end{aligned}$$

for $\ell \nmid pN$ while

$$\begin{aligned} \eta^{-1}(\ell)a_\ell g &= U_\ell g \\ &= \langle \ell \rangle_{p^e} F_\ell g \\ &= \eta^{-1}(\ell) F_\ell g \end{aligned}$$

for $\ell|N$. Now if g_{v_0} is the v_0 component of g , then these equations imply that g_{v_0} is a multiple of the q -expansion of the modular form f with eigenvalues a_ℓ . This in turn implies that $\iota(P) \in E(K_{v_0})_1 \otimes_{\mathbf{Z}_p} \overline{\mathbf{Q}}_p$ actually lies in $\phi(S^{N\text{-new}}) \otimes_{\mathbf{Z}_p} \overline{\mathbf{Q}}_p$. Thus

$$\iota(E(K)^{N\text{-new}}) \otimes_{\mathbf{Z}} \overline{\mathbf{Q}}_p \subseteq \phi(S^{N\text{-new}}) \otimes_{\mathbf{Z}_p} \overline{\mathbf{Q}}_p$$

and so

$$\iota(E(K)^{N\text{-new}}) \otimes_{\mathbf{Z}} \mathbf{Q}_p \subseteq \phi(S^{N\text{-new}}) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p.$$

As

$$E(K) \otimes_{\mathbf{Z}} \mathbf{Q}_p = E(K)^{N\text{-new}} \otimes_{\mathbf{Z}} \mathbf{Q}_p \bigoplus E(K)^{N\text{-old}} \otimes_{\mathbf{Z}} \mathbf{Q}_p,$$

by induction on N we conclude that $\iota(E(K)_1) \otimes_{\mathbf{Z}} \mathbf{Q}_p \subseteq \phi(S) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. Finally since

$$\begin{aligned} \iota(E(K)_1) &\subseteq (\phi(S) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p) \cap E(K_{v_0})_1 \\ &= \phi(S) \end{aligned}$$

we have proven the desired result.

9. The case of analytic rank one.

Recall that e is the power of p occurring in the level of the modular function field K . When $e \leq 1$ and the L -function $L(E/K, s)$ vanishes simply at $s = 1$, one can identify which modular forms $f \in S$ should come from points of infinite order in $E(K)$ and thus give a conjectural construction of these points.

In [1, §1], Coleman defines an inner product on certain spaces of modular forms. More precisely, let $S' \subseteq S_3(\Gamma_1(pN); \overline{\mathbf{Q}}_p)$ be the subspace spanned by p -old forms and by forms whose character has conductor divisible by p . (So S' is a complement

to the subspace of forms new at p but with character of conductor prime to p .) When $e \leq 1$, the \mathbf{Z}_p -module S of modular forms defined in Section 2 is contained in S' . Using a rigid analytic lifting of the Igusa curve, Coleman defines a pairing $(f, g)_C \in \mathbf{C}_p$ for all $f, g \in S'$.

It follows from the construction that this pairing satisfies a certain compatibility with the cup product on $H^2(M)$. Namely, by the remarks after Theorem 5, the composition $\phi^{-1}\iota$ can be viewed as a homomorphism $E(K) \rightarrow S$. Recall also the homomorphism $\psi : E(K) \rightarrow H^2(M)$ of Section 6. The compatibility is that if $P, Q \in E(K)$, then

$$(\phi^{-1}\iota(P), \phi^{-1}\iota(Q))_C = \psi(P) \cup \psi(Q).$$

In fact, $(\cdot, \cdot)_C$ is defined as the pull-back of the cup product under a certain homomorphism from S' to crystalline cohomology. (We note also that both Coleman's pairing and $\phi^{-1}\iota$ depend implicitly on the choice of a cusp; to make the formula correct we have to choose them consistently.)

Now assume that the L -function $L(E/K, s)$ vanishes simply at $s = 1$. Then Proposition 3 implies that $\text{Rank}_{\mathbf{Z}_p} S = 1$. Let $|E(K)_{\text{tor}}|$ be the order of the torsion subgroup of $E(K)$ (which is N in this case) and $\tau(E/K)$ the Tamagawa number of E/K (see [6, §7]). Then the conjecture of Birch and Swinnerton-Dyer for E/K is equivalent to the following statement.

CONJECTURE 8. *There exists a form $f \in S$ satisfying*

$$(f, f)_C = \frac{|E(K)_{\text{tor}}|^2 L'(E/K, 1)}{\tau(E/K)(-\log |\mathbf{F}|)} \in \mathbf{Q}.$$

If the q expansion of f is $\sum a_n q^n$, then there exists $c \in \mathbf{F}^\times$ such that

$$c - \exp\left(\sum_{n=1}^{\infty} \frac{a_n}{n^2} q^n\right) \in \mathbf{F}[[q]]^\times \cong E(K_{v_0})$$

is the image under $E(K) \rightarrow E(K_{v_0})$ of a point of infinite order.

If this conjecture holds, the form f is unique up to a sign and the point in $E(K)$ can be taken to be $\sqrt{|\mathbf{II}(E/K)|}$ times a generator of $E(K)$ modulo torsion.

It is likely that Coleman's pairing can be extended to modular forms of level divisible by higher powers of p . (The relevant space of modular forms should be spanned by newforms such that the conductor of the form and the conductor of its character are exactly divisible by the same power of p , and by all oldforms deduced from these newforms.) If so, we would also have a version of Conjecture 8 when $e > 1$.

BIBLIOGRAPHY

1. Coleman, R., *A p -adic inner product on elliptic modular forms*, Barsotti Symposium in Algebraic Geometry (Cristante, V. and Messing, W., eds.), Academic Press, San Diego, 1994, pp. 125-151.
2. Miyake, T., *Modular Forms*, Springer, Berlin Heidelberg New York, 1989.
3. Néron, A., *Quasi-fonctions et hauteurs sur les variétés abéliennes*, Annals of Math. (2) **82** (1965), 249-331.
4. Rubin, K., *p -adic L -functions and rational points on elliptic curves with complex multiplication*, Invent. Math. **107** (1992), 323-350.
5. Shioda, T., *On elliptic modular surfaces*, Jour. Math. Soc. Japan **24** (1972), 20-58.
6. Ulmer, D.L., *On universal elliptic curves over Igusa curves*, Invent. Math. **99** (1990), 377-391.
7. ———, *L -functions of universal elliptic curves over Igusa curves*, Amer. J. Math. **112** (1990), 687-712.
8. ———, *Slopes of modular forms and congruences*, (Preprint).
9. Voloch, F., *Diophantine approximation on abelian varieties in characteristic p* , (To appear in the American Journal of Mathematics).