On Universal Elliptic Curves Over Igusa Curves

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

To my parents
in their 50th year

The purpose of this note is to introduce the arithmetic study of the universal elliptic curve over Igusa curves. Specifically, its Hasse-Weil L-function is computed in terms of modular forms and is shown to have interesting zeros. Explicit examples are presented, for which the Birch and Swinnerton-Dyer conjecture is verified.

This paper summarizes part of the author's Ph.D. thesis. He wishes to thank the Sloan Foundation for financial support in the form of a Doctoral Dissertation Fellowship and his advisor, Dick Gross, for mathematical guidance and inspirational enthusiasm.

1. Igusa curves We review some facts about elliptic curves and Igusa curves. For more details, see [4], [8], and [10], chapter 12.

Let k be a field of characteristic p and E an elliptic curve over k. Extending scalars by the absolute Frobenius of k we obtain another elliptic curve $E^{(p)}$ over k and a purely inseparable isogeny $F : E \rightarrow E^{(p)}$ of degree p. The multiplication by p map on E can be factored as $V \circ F$ where $V : E^{(p)} \rightarrow E$ is the dual isogeny of F. One says that E is *ordinary* if it has p points of order p rational over the algebraic closure $\overline{k}$ and that E is *supersingular* if it has only one $\overline{k}$-rational point of order p.

Equivalently, E is ordinary if and only if the isogeny V is étale. The j-invariants of supersingular elliptic curves in characteristic p all lie in the field of p^2 elements and thus form a finite set. We define the *supersingular polynomial* in characteristic p as the monic polynomial in j with simple zeroes at the j-invariants of supersingular curves:

$$f_{ss}(j) = \prod_{E/\overline{\mathbf{F}}_p \ supersingular} (j - j(E)).$$

There is a table of supersingular polynomials for $p \leq 307$ in [1].

Let E be an elliptic curve over a field k of characteristic p and fix an invariant differential 1-form $\omega \in H^0(E, \Omega^1_{E/k})$. Then we can define the Hasse invariant of E with respect to ω: the absolute Frobenius morphism $F_{abs} : E \to E$ defines a p-linear map

$$F^* : H^1(E, \mathcal{O}_E) \to H^1(E, \mathcal{O}_E)$$

of 1 dimensional k vector spaces. The choice of a differential ω defines by Serre duality a generator η of $H^1(E, \mathcal{O}_E)$ and the *Hasse invariant* $A(E, \omega)$ is defined by

$$F^*(\eta) = A(E, \omega)\eta.$$

This is a modular form of weight $p - 1$ in the sense that it depends only on the isomorphism class of the pair (E, ω) and $A(E, a^{-1}\omega) = a^{p-1}A(E, \omega)$ for all $a \in k^\times$. (For any ring R, $R^\times$ will denote the group of invertible elements of R.) The Hasse invariant is zero if and only if E is supersingular.

Lemma 1.1. *Let E be an elliptic curve over a field k of characteristic p. The kernel of $V : E^{(p)} \to E$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ as group scheme over k if and only if* *the Hasse invariant of E is a $(p-1)^{st}$ power in $k^\times$, i.e., if and only if $A(E,\omega)=1$ for some choice of differential ω on E.*

Proof: Consider the finite flat group scheme $\operatorname{Ker} F$. It is a height one group scheme (i.e., $x^p = 0$ for all x in the local ring at the origin) and as such is completely determined by its p-Lie algebra. This algebra is the same as that of E, thus is Abelian with p-power map $v \mapsto v^{(p)} = Av$ where A is the Hasse invariant (Mumford [13], thm. 3 of §15). But the height one group scheme with this p-Lie algebra is $G_{0,A}$ in the notation of Oort-Tate [21]. In particular, $\operatorname{Ker} F \xrightarrow{\sim} \mu_p$ if and only if A is a $(p-1)^{st}$ power; by duality, this is the case if and only if $\operatorname{Ker} V \xrightarrow{\sim} \mathbf{Z}/p\mathbf{Z}$. Q.E.D.

Fix a scheme S in characteristic p and let E be an elliptic curve over S. An *Igusa structure of level* p on E is a point P of order p in $E^{(p)}(S)$ which generates the kernel of V in the sense of Drinfeld. In other words P is such that the subgroup schemes

$$\sum_{a \in \mathbf{Z}/p\mathbf{Z}} [aP]$$

and

$$\operatorname{Ker} V$$

are equal as relative Cartier divisors in $E^{(p)}/S$.

Let Y be the (coarse) moduli space of isomorphism classes of elliptic curves with Igusa structure of level p where $p \geq 3$. This is a smooth open curve over $\mathbf{F}_p$ whose complete model X is obtained by adding $(p-1)/2$ points which we will refer to as *cusps*. X is the *Igusa curve of level* p.

There is an action of $(\mathbf{Z}/p\mathbf{Z})^\times$ on Y given by

$$\langle a\rangle : (E,P) \mapsto (E,aP) \qquad a \in (\mathbf{Z}/p\mathbf{Z})^\times$$

and the elements ± 1 act trivially. This action extends to X and permutes the cusps simply-transitively. If (E,P) represents a point x of Y with E supersingular then x is fixed by all of $(\mathbf{Z}/p\mathbf{Z})^\times$ (since P must be the identity of $E^{(p)}$); if $j(E) = 0$ and E is not supersingular then x has a stabilizer of order 3 in $(\mathbf{Z}/p\mathbf{Z})^\times/\pm 1$ and if $j(E) = 1728$ and E is not supersingular then x has a stabilizer of order 2 in $(\mathbf{Z}/p\mathbf{Z})^\times/\pm 1$. Elsewhere on X, $(\mathbf{Z}/p\mathbf{Z})^\times/\pm 1$ acts freely. The quotient of X by $(\mathbf{Z}/p\mathbf{Z})^\times/\pm 1$ can be naturally identified with the projective j-line; the map $X \to \mathbf{P}^1_j$ away from the cusps is "forget P": $(E,P) \mapsto j(E)$.

For each $p > 2$, define K as the field of functions of X over $\mathbf{F}_p$: $K = \mathbf{F}_p(X)$. Thus when $p = 3$, $K = \mathbf{F}_3(j)$; when $p \geq 5$, let $A(Q,R)$ be the polynomial in two variables over $\mathbf{Q}$ expressing the Eisenstein series E_{p-1} in terms of E_4 and E_6. The polynomial A has p-integral coefficients ([18], p.23), so can be considered as a polynomial over $\mathbf{F}_p$. The following result is due to Serre; see also Katz-Mazur [10], 12.8.8.

Proposition 1.2. *When $p > 3$ an affine model for the curve X is given by the curve in the Q,R-plane over $\mathbf{F}_p$ defined by the equation $A(Q,R) = 1$. Thus the function field $K = \mathbf{F}_p(X)$ is isomorphic to the fraction field of $\mathbf{F}_p[Q,R]/(A(Q,R) - 1)$.*

Remarks: 1) In terms of this model, the supersingular points on X correspond to the points at infinity and the cusps are the points $Q = \zeta^4$ and $R = \zeta^6$ where $\zeta \in {\mathbf{F}_p}^\times$ is a $(p-1)^{st}$ root of unity (so $\Delta(Q,R) = (Q^3 - R^2)/1728 = 0)$. The map to $\mathbf{P}^1_j$ is given by $(Q, R) \mapsto j = Q^3/\Delta = R^2/\Delta + 1728$.

2) Taking the convention that $(\mathbf{Z}/p\mathbf{Z})^\times$ acts on functions on the left, one has $Q^{\langle a \rangle} = a^4 Q$, $R^{\langle a \rangle} = a^6 R$ and $\Delta^{\langle a \rangle} = a^{12}\Delta$.

2. The universal curves Denote by Y^{ord} the curve obtained from Y by removing the supersingular points. When $p \geq 3$, Y^{ord} is a fine moduli space representing the moduli problem "*ordinary* elliptic curves over $\mathbf{F}_p$-algebras together with an Igusa structure of level p." Concretely, this means that there exists a universal curve

$$\mathbf{E} \to Y^{ord} \tag{(2).1}$$

and an Igusa structure of level p on $\mathbf{E}^{(p)}$ such that every family of ordinary elliptic curves with Igusa structure of level p over an $\mathbf{F}_p$-scheme is induced from (2.1) via a unique base change. Let E/K be the generic fibre of the family (2.1). Using the fact that Y^{ord} is a fine moduli space, it is easy to see that E/K is the unique elliptic curve over K with j-invariant j and with an Igusa structure of level p. This characterization allows one to deduce the following result.

Proposition 2.2. *Weierstrass models for the curves E/K are given by the following plane cubics:*

$$y^2 = x^3 + x^2 - 1/j \qquad \textit{when } p = 3$$

$$y^2 = x^3 - \frac{Q}{2^4 3}x + \frac{R}{2^5 3^3} \qquad \textit{when } p \geq 5$$

As noted by Gross in [6], when $p \equiv 3 \pmod 4$, E can be canonically descended to the rational function field $\mathbf{F}_p(j)$. Recall that by lemma (1.1) E/K can be described as the unique elliptic curve with j-invariant j whose Hasse invariant is a $(p-1)^{st}$ power.

Proposition 2.3. *When $p \equiv 3 \pmod 4$ there exists a unique elliptic curve E over $\mathbf{F}_p(j)$ with j-invariant j and whose Hasse invariant is a square. When $p > 3$ a Weierstrass model is given by:*

$$y^2 = x^3 - \frac{c_4}{2^4 3}x - \frac{c_6}{2^5 3^3}$$

with

$$c_4 = j^a (j - 1728)^{a'} \tilde{f}_{ss}(j)^2 \qquad c_6 = -j^b (j - 1728)^{b'} \tilde{f}_{ss}(j)^3$$

where $\tilde{f}_{ss}$ is the supersingular polynomial with any possible factors of j or $(j-1728)$ removed and where a, a', b and b' are given by the following table:

$p \pmod{24}$	a	a'	b	b'
7	3	1	4	2
11	1	3	1	5
19	3	3	4	5
23	1	1	1	2

Remarks: 1) When $p = 3$, $K = \mathbf{F}_p(j)$ and the curve in (2.2) is the unique elliptic curve over $\mathbf{F}_p(j)$ with j-invariant j and square Hasse invariant.

2) In terms of Weil's theory of descent of the base field and the model (2.2), descent data for the curve in (2.3) is given by $f_{\langle a \rangle} : E \to E^{\langle a \rangle}$, $(x, y) \mapsto (a^2 x, \left(\frac{a}{p}\right) a^3 y)$ where $\left(\frac{a}{p}\right)$ is the Legendre symbol.

3) When $p \equiv 1 \pmod 4$, the universal curve over K does not descend to its field of moduli. This can be seen most easily by trying to construct descent data.

Proof: Uniqueness follows from the fact that $(p-1)/2$ is odd: since the j-invariant of E is j, $\mathrm{Aut}(E) = \pm 1$ and E is determined up to a quadratic twist. But the Hasse invariant has weight $p-1$, so twisting by d changes it by $d^{(p-1)/2}$, which is not a square unless d is.

To see that the Weierstrass model above has the required properties, it suffices to check that it becomes isomorphic to the universal curve over K. Indeed, if the Hasse invariant becomes a $(p-1)^{st}$ power after a field extension of degree $(p-1)/2$ it was a square to begin with, and the j-invariant is unchanged by field extensions. Finally, this isomorphism follows from a routine calculation using a result of Hasse ([7], Hilfsatz 3) relating the supersingular polynomial to the Hasse invariant. Q.E.D.

Let E be the model of the universal elliptic curve with square Hasse invariant given by (2.3) and ω the differential $dx/2y$.

Proposition 2.4. *The discriminant and Hasse invariant of $E/\mathbf{F}_p(j)$ are as follows:*

$$\Delta(E,\omega) = j^c(j-1728)^{c'}\tilde{f}_{ss}(j)^6$$

$$A(E,\omega) = j^d(j-1728)^{d'}\tilde{f}_{ss}(j)^{(p+1)/2}$$

where c, c', d and d' are given by the following table:

$p \pmod{24}$	c	c'	d	d'
7	8	3	$(2p-2)/3$	$(p+1)/4$
11	2	9	$(p+1)/6$	$(3p-1)/4$
19	8	9	$(2p-2)/3$	$(3p-1)/4$
23	2	3	$(p+1)/6$	$(p+1)/4$

Proof: The calculation of the discriminant is immediate from (2.3) and the formula $\Delta = (c_4^3 - c_6^2)/1728$. For the Hasse invariant, first assume that $p \equiv 23 \pmod{24}$. Then A is an isobaric polynomial of weight $p-1$ in c_4 and c_6, i.e., a linear combination of the terms

$$c_4 c_6^{(p-5)/6}, \quad c_4^4 c_6^{(p-17)/6}, \quad \ldots, \quad c_4^{(p-7)/4} c_6$$

where

$$c_4 = j(j-1728)\tilde{f}_{ss}(j)^2 \text{ and } c_6 = -j(j-1728)^2\tilde{f}_{ss}(j)^3.$$

Thus A has degree $(p+1)(p-1)/24$ in j and is *a priori* divisible by

$$j^{(p+1)/6}(j-1728)^{(p+1)/4}\tilde{f}_{ss}(j)^{(p-1)/2}.$$

Now $(p+1)/6$ and $(p+1)/4$ are even while $(p-1)/2$ is odd. Since $\tilde{f}_{ss}$ has no repeated roots, the fact that A is a square implies that

$$j^{(p+1)/6}(j-1728)^{(p+1)/4}\tilde{f}_{ss}(j)^{(p+1)/2}$$

divides A. But this expression has the same degree as A, so they differ by a constant. Finally, since E has split multiplicative reduction at ∞ (see section 6) and one knows that the q-expansion of the Hasse invariant of the Tate curve is 1 (Katz-Mazur [10], 12.4.2), this constant must be 1. The other cases are handled similarly. Q.E.D.

3. The L-function Fix a prime $p \equiv 3 \pmod 4$ and let E be the elliptic curve (2.3) over the function field $\mathbf{F}_q(j)$. Fix a separable closure $\overline{\mathbf{F}_q(j)}$ of $\mathbf{F}_q(j)$ and let $G = \mathrm{Gal}(\overline{\mathbf{F}_q(j)}/\mathbf{F}_q(j))$ be the Galois group. For each prime $\ell \neq p$, one has the étale cohomology group $H^1(E \otimes \overline{\mathbf{F}_q(j)}, \mathbf{Q}_\ell)$, which is a 2-dimensional $\mathbf{Q}_\ell$-vector space. The group G acts on $E \otimes \overline{\mathbf{F}_q(j)}$ via the second factor and this provides a linear representation

$$\rho : G \to \mathrm{Aut}_{\mathbf{Q}_\ell}(H^1(E \otimes \overline{\mathbf{F}_q(j)}, \mathbf{Q}_\ell)).$$

For each place v of $\mathbf{F}_q(j)$, let q_v be the number of elements in the residue field, $D_v \subset G$ 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. The *Hasse-Weil L-function* of $E/\mathbf{F}_q(j)$ is the L-function associated to the representation ρ:

$$L(E/\mathbf{F}_q(j), s) = \prod_v \det(1 - \rho(F_v^{-1})q_v^{-s} | H^1(E \otimes \overline{\mathbf{F}_q(j)}, \mathbf{Q}_\ell)^{I_v})^{-1} \qquad (3).1$$

where the product is over all places v of the field $\mathbf{F}_q(j)$. This product converges, as a function of the complex variable s, in the half plane $\operatorname{Re} s > 3/2$, is independent of ℓ, and can be analytically continued to the plane where it satisfies a functional equation (see (8.1)). We will see that this L-function can be computed explicitly in terms of modular forms.

Let N and k be positive integers and χ a Dirichlet character modulo N. Then $S_k(\Gamma_0(N), \chi)$ will denote the complex vector space of modular forms of weight k and character χ for the congruence subgroup $\Gamma_0(N)$ of $SL_2(\mathbf{Z})$. On this space we have operators T_ℓ for primes $\ell \not| N$ and U_p for primes $p|N$ (cf. [17]). We will be interested in the characteristic polynomial of the operators $U_{p^n} = (U_p)^n$. For q a power of p and T a variable, define the Hecke polynomials

$$H_q(T) = H_q(S_k(\Gamma_0(p), \chi), T) = \det(1 - TU_q | S_k(\Gamma_0(p), \chi)).$$

The polynomial $H_q(T)$ has integral coefficients and constant term 1. The L-function result we have in mind is the following.

Proposition 3.2.

$$L(E/\mathbf{F}_q(j), s) = H_q(S_3(\Gamma_0(p), \left(\frac{-}{p}\right)), q^{-s})$$

where $\left(\frac{-}{p}\right)$ *is the Legendre symbol.*

It follows immediately that $L(E/\mathbf{F}_q(j), s)$ is an entire function of s and a theorem of Hecke (see Ogg [14], cor. 1 of thm. 4) implies that the zeroes of the L function lie on the line $\mathrm{Re}\, s = 1$. The existence of modular forms with complex multiplication furnishes such zeroes.

Modular forms with CM by $Q(\sqrt{-p})$ can be constructed as follows: let ϕ be an unramified Hecke character of $Q(\sqrt{-p})$ of infinity type $(2,0)$; there are h such characters where h is the class number of $Q(\sqrt{-p})$. For each ϕ, define a function on the upper half plane by

$$f_\phi(z) = \sum \phi(\mathbf{a}) e^{2\pi i (N\mathbf{a})z} \qquad (3).3$$

where the sum extends over all integral ideals $\mathbf{a}$ of $Q(\sqrt{-p})$ and $N(\mathbf{a})$ is the norm of $\mathbf{a}$. Results of Hecke and Shimura (see [16], lemma 3) assert that f_ϕ is a normalized newform of weight 3 for $\Gamma_1(D)$, where $-D$ is the discriminant of $Q(\sqrt{-p})$; the character χ of f_ϕ is equal to the quadratic character associated to $\mathbf{Q}(\sqrt{-p})$: $\chi(a) = \left(\frac{-D}{a}\right) = \left(\frac{-p}{a}\right)$. Thus the conductor of χ is p and when $p \equiv 3 \pmod 4$, $\chi(a) = \left(\frac{a}{p}\right)$ by quadratic reciprocity. Since the only ideal of $Q(\sqrt{-p})$ of norm p is the principal ideal $(\sqrt{-p})$, we see that that eigenvalue of f_ϕ for U_p is $-p$. Applying this construction, we see that for $p \equiv 3 \pmod 4$, $p > 3$, the L-function $L(E/\mathbf{F}_q(j), s)$ vanishes at $s = 1$ to order (at least) h when $\mathbf{F}_{p^2} \subset \mathbf{F}_q$.

Below is a table of giving the dimension d of $S_3 = S_3(\Gamma_0(p), \left(\frac{-}{p}\right))$, the class number h of the field $\mathbf{Q}(\sqrt{-p})$, and the characteristic polynomial H_p for primes $p \equiv 3 \pmod 4$ with $7 \leq p \leq 71$. The factors are irreducible over $\mathbf{Z}$, and in each case, the only roots of H_p which are roots of unity times $1/p$ (thus giving zeroes of $L(E/\mathbf{F}_q(j), s)$ for some q) are those coming from the CM forms. Whether the CM forms always account for all of the zeroes of the L-function of $E/\mathbf{F}_q(j)$ is an interesting question.

(3.4) Hecke polynomials for small p

p	d	h	H_p
7	1	1	$(1+7T)$
11	1	1	$(1+11T)$
19	3	1	$(1+19T)(1+12T+19^2T^2)$
23	3	3	$(1+23T)^3$
31	5	3	$(1+31T)^3(1+10T+31^2T^2)$
43	7	1	$(1+43T)(1-10T+147T^2+135020T^3$ $+43^2 147T^4-43^4 10T^5+43^6T^6)$
47	7	5	$(1+47T)^5(1-62T+47^2T^2)$
59	9	3	$(1+59T)^3(1-156T+13007T^2-812312T^3$ $+59^2 13007T^4-59^4 156T^5+59^6T^6)$
67	11	1	$(1+67T)(1-154T+11225T^2-332824T^3-29988530T^4$ $+3936691396T^5-67^2 29988530T^6-67^4 332824T^7$ $+67^6 11225T^8-67^8 154T^9+67^{10}T^{10})$
71	11	7	$(1+71T)^7(1-152T+12658T^2-71^2 152T^3+71^4T^4$

The polynomial was determined by finding a basis of S_3 using Ross' simplification of the Hijikata trace formula ([15], thm. 2.1) then calculating the action of U_p on the Fourier coefficients (except for the case $p = 67$, which was supplied by Atkin). The calculations were made using the Lisp language on a Symbolics 3600 computer.

4. Proof of proposition 3.2 The essential idea, which is due to Ihara [9], is to group the terms of the product (3.1) by the values of $a_v = \operatorname{Tr} Fr_v$ and to compare the resulting expression with the Eichler trace formula. We should also mention that p-adic analogues of (3.2) have been considered by various authors; for example, see

[3] and the papers in its bibliography.

Recall that at a place v where $E/\mathbf{F}_q(j)$ has good reduction, the local factor (3.1) is $(1 - a_v q_v^{-s} + q_v^{1-2s}) = (1 - \alpha_v q_v^{-s})(1 - \overline{\alpha}_v q_v^{-s})$ where the reduction of E has $1 - a_v + q$ points over the residue field $\mathbf{F}_{q_v}$ and $|a_v| \leq 2\sqrt{q_v}$. Furthermore, one knows (Manin [11], thm. 1) that a_v is congruent modulo p to the norm from $\mathbf{F}_q$ to $\mathbf{F}_p$ of the Hasse invariant of A. (This is well-defined since the only $(p-1)^{st}$ power in $\mathbf{F}_p$ is 1.) Thus, at a place v of good reduction for $E/\mathbf{F}_q(j)$, a_v is congruent modulo p to a non-zero square.

It will be shown in (6.1) that the universal $E/\mathbf{F}_q(j)$ has additive reduction at 0 and 1728 and the supersingular places and has split multiplicative reduction at the cusp. Christening the other places of $\mathbf{F}_q(j)$ "good," we have

$$\begin{aligned} L(E/\mathbf{F}_q(j)) &= (1-q^{-s})^{-1} \prod_{good\ v} (1 - \alpha_v q^{-deg(v)s})^{-1} (1 - \overline{\alpha}_v q^{-deg(v)s})^{-1} \\ &= \exp\left(\sum_{good\ v} \sum_{m=1}^{\infty} \left(\frac{\alpha_v^m + \overline{\alpha}_v^m}{m} \right) q_v^{-deg(v)ms} \right) \\ &= \exp \sum_{n=1}^{\infty} \left(\sum_{\substack{good\ v \\ deg(v)|n}} deg(v)(\alpha_v^{n/deg(v)} + \overline{\alpha}_v^{n/deg(v)}) \right) \frac{q^{-ns}}{n}. \end{aligned}$$

Now

$$\sum_{\substack{good\ v \\ deg(v)|n}} deg(v)(\alpha_v^{n/deg(v)} + \overline{\alpha}_v^{n/deg(v)}) \qquad (4).1$$

is equal to the sum, over all ordinary places w of degree 1 of $\mathbf{F}_{q^n}(j)$ (except the place $j = 0$ when $p \equiv 7 \pmod{12}$), of a_w (where, as usual, the reduction of $E/\mathbf{F}_{q^n}(j)$ at w has $q^n + 1 - a_w$ rational points over $\mathbf{F}_{q^n}$). We saw above that $|a_w| \leq 2\sqrt{q^n}$ and that a_w is a square modulo p. Conversely, given such an a, we need to know how many times it occurs in the sum (4.1).

Given a negative discriminant d (i.e., $d \equiv 0$ or $1 \pmod 4$)) let $\mathcal{O}_d$ be the unique quadratic order of discriminant d, $h(d)$ the order of its Picard group and $2w(d)$ the number of units in $\mathcal{O}_d$. (One has $w(d) = 3$ when $d = -3$, $w(d) = 2$ when $d = -4$, and $w(d) = 1$ otherwise.) Finally, define the *Hurwitz class number*

$$H(D) = \sum_{df^2 = D} \frac{h(d)}{w(d)}. \tag{4).2}$$

Lemma 4.3. *Given a with $(a, p) = 1$ and $|a| \le 2\sqrt{q}^n$, there are $H(a^2 - 4q^n)$ elliptic curves over $\mathbf{F}_{q^n}$ with $q^n + 1 - a$ points.*

An elliptic curve (up to $\overline{\mathbf{F}_p}$-isomorphism) with $j \neq 0,\ 1728$ has two forms, so contributes to the sum for two different values of a. If $j = 1728$, then there are 4 forms, so we agree to count the curve 1/2, while if $j = 0$, there are 6 forms and we count the curve 1/3. It is with this convention that the lemma holds. The proof, which we omit, is an exercise in applying Deuring's liftings of ordinary elliptic curves in characteristic 0 to characteristic p and in using the correspondence between elliptic curves with complex multiplication and ideal classes in imaginary quadratic orders.

Applying the lemma,

$$\begin{aligned}\sum_{deg(v)|n} deg(v)(\alpha_v^{deg(v)/n} + \overline{\alpha}_v^{deg(v)/n}) &= \sum_{\substack{|a| \le 2\sqrt{q^n} \\ (a/p)=1}} aH(a^2 - 4q^n) \\ &= \frac{1}{2} \sum_a a\left(\tfrac{a}{p}\right) H(a^2 - 4q).\end{aligned}$$

But according to Eichler's version of the trace formula ([5], thm., p. 134), this last expression is just $1 + \operatorname{Tr} U_{q^n}$ where $\operatorname{Tr} U_{q^n}$ is the trace of the Hecke operator U_{q^n}

acting on $S_3(\Gamma_0(p), \left(\frac{\cdot}{p}\right))$. Thus

$$\begin{aligned} L(E/\mathbf{F}_q(j), s)(1-q^{-s}) &= \exp\left(\sum_{n=1}^{\infty}(1+\operatorname{Tr} U_{q^n})\frac{q^{-ns}}{n}\right) \\ &= (1-q^{-s})H_q(q^{-s}). \end{aligned}$$

Since the product expression for the L-function converges absolutely for $\operatorname{Re} s > 3/2$, these formal manipulations are justified and the proof of theorem 3.2 is complete.

5. Torsion The next three sections are devoted to calculating the rest of the invariants of the universal curves which appear in the refined conjecture of Birch and Swinnerton-Dyer. We begin with the torsion points on the universal curve.

Proposition 5.1.

$$E(K \otimes \overline{\mathbf{F}_p})_{tor} \cong 1.$$

$$E^{(p)}(K)_{tor} \cong E^{(p)}(K \otimes \overline{\mathbf{F}_p})_{tor} \cong \mathbf{Z}/p\mathbf{Z}.$$

Proof: The prime-to-p part of these claims follows from the existence of two places of K where the reduction of E has q and $q-1$ points respectively for any sufficiently large power q of p (use lemma 4.3). The p part follows from the definition of K and the fact that the function field of the Igusa curve of level p^2 is a "geometric" extension of that of the Igusa curve of level p (i.e., is not obtained by extending the ground field). Q.E.D.

Recall that $(\mathbf{Z}/p\mathbf{Z})^\times$ acts on X via $\langle a\rangle : (E,P) \mapsto (E,aP)$, ± 1 act trivially, and $\operatorname{Gal}(K/\mathbf{F}_p(j)) = (\mathbf{Z}/p\mathbf{Z})^\times/\pm 1$ acts on functions on the left: $f^{\langle a\rangle}(E,P) = f(E,a^{-1}P)$. With these conventions, we can determine the Galois module structure of the torsion points on the universal curves.

Proposition 5.2. *If $p \equiv 3 \pmod 4$ and $P \in E^{(p)}(K)_{tor}$ then*

$$P^{\langle a\rangle} = \left(\tfrac{a}{p}\right) a^{-1} P$$

for all $\langle a\rangle \in Gal(K/\mathbf{F}_p(j)) \cong (\mathbf{Z}/p\mathbf{Z})^\times / \pm 1$, where $\left(\tfrac{a}{p}\right)$ is the Legendre symbol.

Proof: Tautologically, one has $P^{\langle a\rangle} = \pm a^{-1}P$ for $P \in E^{(p)}(K)_{tor}$. Define a function $\chi : \mathrm{Gal}(K/\mathbf{F}_p(j)) \to \pm 1$ via $P^{\langle a\rangle} = \chi(a)a^{-1}P$. This function is clearly a homomorphism and it is surjective since $\langle -1\rangle$ is trivial in the Galois group. Thus its kernel is exactly the set of squares in $(\mathbf{Z}/p\mathbf{Z})^\times$ and $\chi(a) = \left(\tfrac{a}{p}\right)$. Q.E.D.

In particular, for $p > 3$ the torsion subgroup of $E^{(p)}(\mathbf{F}_q(j))$ is trivial, while for $p = 3$ $E^{(3)}(\mathbf{F}_q(j))_{tor} = E^{(3)}(K)_{tor} \cong \mathbf{Z}/3\mathbf{Z}$. The reader is invited to verify that the sign is correct in proposition 5.2 by computing the action of $(\mathbf{Z}/p\mathbf{Z})^\times$ on the coordinate ring of $\mathrm{Ker}\, V$ using the proof of lemma 1.1 and proposition 2.4.

6. Local invariants

This section is devoted to tabulating the Kodaira-Néron reduction types and conductors of the universal curves. As noted before, the universal curves have good reduction away from the cusps, supersingular points, and places lying over 0 and 1728. At the bad reduction places, the reduction types can be read off from Tate's algorithm [20] and are summarized below (using Kodaira's notation).

When $p = 3$, $E/\mathbf{F}_q(j)$ has split multiplicative reduction at the unique cusp and has reduction type II^* at the unique supersingular point, while $E^{(3)}$ has reduction type IV^* (with all three components of multiplicity one rational over $\mathbf{F}_3$) there. The exponent of the conductor at the supersingular place is 3. When $p > 3$, the reduction types are:

(6.1) Reduction of E over $\mathbf{F}_q(j)$

$p \pmod{24}$	0	1728	$v \in S$
7	IV^*	III	I_0^*
11	II	III^*	I_0^*
19	IV^*	III^*	I_0^*
23	II	III	I_0^*

where S denotes the set of supersingular places not lying over $j = 0$ or 1728.

In order to compute Tamagawa numbers in the next section, we will need the field of rationality of the various components of multiplicity one on the Néron model. The group of connected components on the special fibre of the Néron model of E at a place v of K is isomorphic, as $\mathrm{Gal}(\overline{\mathbf{F}_p}/\mathbf{F}_v)$-module, to the fixed points of the automorphism group of the elliptic curve with additional structure corresponding to v. This group is non-trivial only when v is a supersingular place. In this case, it can be analysed by lifting the curve and its Frobenius endomorphism to characteristic 0 and considering the resulting quadratic order. (For example, the points of order 2 on the special fibre are rational over the residue field if and only if $\pi - 1$ is divisible by 2 in the lifted endomorphism ring, where π is the lift of the Frobenius endomorphism.) Applying this analysis to each place of the ground field yields the following result.

Proposition 6.2. *The product, over all places v of $\mathbf{F}_q(j)$, of the order of the group of components of multiplicity one on the Néron model of $E/\mathbf{F}_q(j)$ at v which are* *rational over the residue field at v is given by the following table.*

$p \pmod{12}$	$\mathbf{F}_{p^2} \not\subseteq \mathbf{F}_q$	$\mathbf{F}_{p^2} \subseteq \mathbf{F}_q$
7	$2^{(p+5)/12+(h-1)/2}$	$2^{(p-1)/6}3$
11	$2^{(p+1)/12+(h-1)/2}$	$2^{(p-5)/6}$

7. Tamagawa numbers Let L be a global function field and $\mathbf{A}_L$ the adèles of L. There is a natural measure $\mu = \prod \mu_v$ on $\mathbf{A}_L$ where μ_v is the Haar measure which assigns measure 1 to the ring of integers $\mathcal{O}_v$ in the completion L_v for a place v of L. The quotient $\mathbf{A}_L/L$ is compact and we set $D_L = \mu(\mathbf{A}_L/L)$. If L is the function field of a curve of genus g with field of constants $\mathbf{F}_q$, then one has (Weil [23], 2.1.3)

$$D_L = q^{g-1}. \tag{(7).1}$$

If A is an elliptic curve over L and ω is a differential on A, for each v ω induces a differential ω_v on the curve A_v over L_v deduced from A; using μ_v we get a measure $|\omega_v|$ on $A_v(L_v)$. When the differential ω_v is a Néron differential, then Tate [20], 5.2 has shown that

$$\int_{A_v(\mathcal{O}_v)} |\omega_v| = \frac{\#A(l_v)}{q} \tag{(7).2}$$

where $\#A(l_v)$ is the number of points on the special fiber of the Néron model of A. Thus if we set

$$\lambda_v = \frac{\#X(l_v)^\circ}{q} \tag{(7).3}$$

where $\#A(l_v)^\circ$ is the number of points on the connected component of the special fiber of the Néron model of A, then $\{\lambda_v\}$ is a set of convergence factors in the sense of Weil [23], 2.3. In this situation, we can form the product measure

$$\Omega = \Omega(L, \omega, (\lambda_v)) = D_L^{-1} \prod_v \lambda_v^{-1} |\omega_v|.$$

By the product formula, this is independent of the choice of ω. Finally, we define the *Tamagawa number* $\tau(A,L)$ to be the measure of the set of $\mathbf{A}_L$ points of A with respect to Ω. Since A is a projective variety, $A(\mathbf{A}_L) = \prod_v A(\mathcal{O}_v)$ and the measure can be computed as a product of local factors: $\Omega = D_L^{-1} \prod_v \lambda_v^{-1} \int_{A_v(\mathcal{O}_v)} |\omega_v|$. Using (7.2) and (7.3), the local factor $\lambda_v^{-1} \int_{A_v(\mathcal{O}_v)} |\omega_v|$ is equal to $q^{f_v} c_v$ where c_v is the number of components of multiplicity 1 on the Néron model at v which are rational over the residue field and f_v is the integer such that $\pi_v^{f_v} \omega_v$ is a Néron differential at v (where π_v is a uniformiser at v).

It is now a simple matter to apply these ideas to the universal curves. The product $C = \prod_v c_v$ of the number of rational components was computed in (6.2) and the valuation of the minimal discriminant, thus the value of f, is an immediate consequence of the Néron model calculation of section 6. Putting all these together, we find the following values for the Tamagawa numbers.

(7.4) Tamagawa numbers of E and $E^{(p)}$ over $\mathbf{F}_q(j)$

$p \pmod{24}$	$\tau(E, \mathbf{F}_q(j))$	$\tau(E^{(p)}, \mathbf{F}_q(j))$
3	1	9
7	$Cq^{-(p-7)/24}$	$Cpq^{-(3p+3)/24}$
11	$Cq^{-(p-11)/24}$	$Cpq^{-(3p-9)/24}$
19	$Cq^{-(p+5)/24}$	$Cpq^{-(3p-9)/24}$
23	$Cq^{-(p-23)/24}$	$Cpq^{-(3p+3)/24}$

8. Application: the functional equation The L-functions of varieties over function fields are known to satisfy a functional equation. In this section we check this directly for the universal curve over $\mathbf{F}_q(j)$. Experts will note that we are merely verifying the formula of Grothendieck-Ogg-Shafarevitch in this special case.

Recall that when $p \geq 5$, the exponent of the conductor of $E/\mathbf{F}_q(j)$ is 2 at the supersingular places and at 0 (because the reduction is additive) and 1 at the cusps (where the reduction is multiplicative). Thus N_E, the norm of the conductor, is q^f where $f = (p+23)/6$ when $p \equiv 7 \pmod{12}$ and $f = (p+19)/6$ when $p \equiv 11 \pmod{12}$; when $p = 3$, $N_E = q^4$. In all cases, the discriminant $D_{\mathbf{F}_q(j)}$ is q^{-1} (7.1). On the other hand, standard formulas (e.g., Cohen-Oesterlé, [2], thm. 1) allow one to compute that the degree in q^{-s} of $L(E/\mathbf{F}_q(j), s)$, namely the dimension of $S_3(\Gamma_0(p), \left(\frac{-}{p}\right))$, is $[p/6]$. Since the inverse roots of the Hecke polynomial $H_q(T)$ have complex absolute value q ([14], cor. 1 of thm. 4), a trivial calculation yields the following.

Proposition 8.1. *Let* $\Lambda(s) = N_E^{s/2} D_{\mathbf{F}_q(j)}^{2s} L(E/\mathbf{F}_q(j), s)$*. Then* $\Lambda(s) = \pm\Lambda(2-s)$*.*

Remark: If n is the number of reciprocal roots of $H_p(T)$ which are negative real numbers and r is the number which are positive real numbers, then the sign in the functional equation is $(-1)^k$ where $k = n([\mathbf{F}_q : \mathbf{F}_p] + 1) + r$.

9. Application: the Tate-Shafarevitch group Recall that the Tate-Shafarevitch group $Ш(K, A)$ of an Abelian variety A over a global field K is defined to be the kernel of the map

$$H^1(K, A) \to \prod_v H^1(K_v, A)$$

where the product is over all places v of K and K_v is the completion of K at v. In this section, we use the explicit calculations of the invariants of the universal curve to obtain information about this group.

Let A be an elliptic curve over a function field K and assume that $\operatorname{ord}_{s=1} L(A/K, s) =$

0. Then by work of Tate ([19], §3), the rank of the Mordell-Weil group $A(K)$ is zero. Furthermore, by Milne [12], 8.1, the equality $\text{ord}_{s=1} L(A/K, s) = \text{Rank } A(K)$ implies the refined Birch and Swinnerton-Dyer conjecture on the leading term of the L-function. Concretely, $\text{Ш}(K, A)$ is finite with order

$$|\text{Ш}(A, K)| = \frac{L(A/K, 1)\,|A(K)_{tor}|^2}{\tau(A, K)} \tag{(9).1}$$

(the regulator term does not appear because the rank is zero).

Applying this to the universal curve $E/\mathbf{F}_q(j)$, one obtains the orders of $\text{Ш}(\mathbf{F}_p(j), E)$ and $\text{Ш}(\mathbf{F}_p(j), E^{(p)})$ for the first few primes $p \equiv 3 \pmod 4$:

(9.2) Order of Ш for E and $E^{(p)}$ over $\mathbf{F}_p(j)$

p	$\lvert\text{Ш}(\mathbf{F}_p(j), E)\rvert$	$\lvert\text{Ш}(\mathbf{F}_p(j), E^{(p)})\rvert$
3	1	1
7	1	1
11	1	1
19	5^2	5^2
23	1	23^2
31	6^2	$6^2 31^2$
43	$2^6 7^2$	$2^6 7^2 43^2$
47	2^4	$2^4 47^4$
59	$2^2 5^2$	$2^2 5^2 59^4$
67	$5^2 7^2$	$5^2 7^2 67^4$
71	17^2	$17^2 71^6$

Of course these orders are all square integers; note that in all cases the order of $\text{Ш}(\mathbf{F}_p(j), E)$ is prime to p.

The only mysterious term on the right hand side of (9.1) can be eliminated by using the fact that the L-functions of isogenous curves are equal. Assuming that

$L(E/\mathbf{F}_q(j),1) \neq 0$, dividing (9.1) for $E^{(p)}/\mathbf{F}_q(j)$ by (9.1) for $E/\mathbf{F}_q(j)$, we find

$$\frac{Ш(\mathbf{F}_q(j),E^{(p)})}{Ш(\mathbf{F}_q(j),E)} = \frac{\tau(E,\mathbf{F}_q(j))}{\tau(E^{(p)},\mathbf{F}_q(j))} = \begin{cases} p^{-1}q^{(p+5)/12} & \text{when } p \equiv 7 \pmod{24} \\ p^{-1}q^{(p+1)/12} & \text{when } p \equiv 11 \pmod{24} \\ p^{-1}q^{(p-7)/12} & \text{when } p \equiv 19 \pmod{24} \\ p^{-1}q^{(p+13)/12} & \text{when } p \equiv 23 \pmod{24} \end{cases}$$

Note that these numbers are squares if and only if q is an *odd* power of p. Moreover, it is possible in some cases to show that $Ш(\mathbf{F}_q(j),E)$ has trivial p-primary component and to explicitly produce the number of elements of $Ш(\mathbf{F}_q(j),E^{(p)})$ predicted by the formula above. (In fact, they are all p-torsion elements.) I hope to report on this in a future paper.

10. Some global points Here are some points of infinite order on the universal curve over $\mathbf{F}_q(j)$:

When $p=7$, the equation of $E/\mathbf{F}_q(j)$ is

$$y^2 = x^3 + j^3(j+1)x + 5j^4(j+1)^2.$$

When $\mathbf{F}_q \supseteq \mathbf{F}_{p^2}$, the Mordell-Weil group $E(\mathbf{F}_q(j))$ is infinite cyclic and a generator is

$$\left(0, \sqrt{5}j^2(j+1)\right);$$

the global height of this point is $\frac{1}{6}\log q$. Since $\tau(E,\mathbf{F}_q(j)) = 6$, the Birch and Swinnerton-Dyer equality implies $|Ш(\mathbf{F}_q(j),E)| = 1$ (which also follows from work of Milne because the elliptic surface over $\mathbf{F}_p$ associated to E is rational).

When $p=11$, the equation of $E/\mathbf{F}_q(j)$ is

$$y^2 = x^3 - 3j(j-1)^3x + 2j(j-1)^5.$$

When $\mathbf{F}_q \supseteq \mathbf{F}_{p^2}$, the Mordell-Weil group $E(\mathbf{F}_q(j))$ is infinite cyclic and a generator is

$$\left(8(j-1)^2, \sqrt{-5}(j-1)^3\right);$$

the global height of this point is $\frac{1}{2}\log q$. Since $\tau(E, \mathbf{F}_q(j)) = 2$, the Birch and Swinnerton-Dyer equality implies $|Ш(\mathbf{F}_q(j), E)| = 1$ (which again also follows from work of Milne).

When $p = 23$, the equation of $E/\mathbf{F}_q(j)$ is

$$y^2 = x^3 - 12j(j-3)(j+4)^2x - 7j(j-3)^2(j+4)^3.$$

When $\mathbf{F}_q \supseteq \mathbf{F}_{p^2}$, the Mordell-Weil group $E(\mathbf{F}_q(j))$ has rank 3; here is a basis:

$$\left((j-3)(j+4), \sqrt{5}(j-3)(j+4)^2\right)$$

$$\left(6(j-3)(j+4), \sqrt{22}(j-3)(j+4)^2\right)$$

$$\left(16(j-3)(j+4), \sqrt{10}(j-3)(j+4)^2\right).$$

In this basis, the matrix of the height pairing has the following interesting form:

$$\begin{pmatrix} \frac{1}{2}\log q & 0 & 0 \\ 0 & \frac{1}{2}\log q & 0 \\ 0 & 0 & \frac{1}{2}\log q \end{pmatrix}$$

Thus the regulator is $\frac{1}{8}(\log q)^3$, and since $\tau(E, \mathbf{F}_q(j)) = 8$, we find $|Ш(\mathbf{F}_q(j), E)| = 1$. This is the expected value as the associated elliptic surface is rational.

References

1 Birch, B.J. and Kuyk, W. (Eds.): Modular Functions of One Variable IV (Lect. Notes in Math. 476.) Berlin Heidelberg New York: Springer 1973

2 Cohen, H. and Oesterlé, J.: Dimensions des espaces de formes modulaires. In: Serre, J.-P. and Zagier, D.B. (Eds.) Modular Functions of One Variable VI (Lect. Notes in Math. 627.) pp. 69-73 Berlin Heidelberg New York: Springer 1977

3 Crew, R.: L-functions of p-adic characters and geometric Iwasawa theory. Invent. Math. **88** (1987) 395-403

4 Deuring, M.: Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abhandlung aus dem Mathematischen Seminar der Hansischen Universität **14** (1941) 197-272

5 Eichler, M.: The basis problem for modular forms and the traces of the Hecke operators. In: Kuyk, W. (Ed.) Modular Functions of One Variable I (Lect. Notes in Math. 320.) pp. 75-151 Berlin Heidelberg New York: Springer 1973

6 Gross, B.: Heegner points and the modular curve of prime level. Jour. Math. Soc. Japan **39** (1987) 345-362

7 Hasse, H.: Existenz separabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade p über elliptischen Funktionenkörpern der Charakteristik p. J. für reine u. ang. Math. **172** (1934) 77-85

8 Igusa, J.: On the algebraic theory of elliptic modular functions. J. Math. Soc. Japan **20** (1968) 96-106

9 Ihara, Y.: Hecke polynomials as congruence ζ-functions in elliptic modular case. Annals of Math. (2) **85** (1967) 267-295

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

11 Manin, J.: The Hasse-Witt matrix of an algebraic curve. Translations of the AMS (2) **45** 245-264

12 Milne, J.S.: On a conjecture of Artin and Tate. Annals of Math. (2) **102** (1975) 517-533

13 Mumford, D.: Abelian Varieties. Oxford: Oxford University Press 1970

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

15 Ross, S.: Hecke operators for $\Gamma_0(N)$, their traces, and applications. Ph.D. Thesis, University of Rochester (1985)

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

17 Shimura, G.: Introduction to the Arithmetic Theory of Automorphic Functions. Princeton: Princeton University Press 1971

18 Swinnerton-Dyer, H.P.F.: On ℓ-adic representations and congruences for coefficients of modular forms. In: Kuyk, W. and Serre, J.-P.(Eds.) Modular Functions of One Variable III (Lect. Notes in Math. 350.) pp. 1-56 Berlin Heidelberg New York: Springer 1973

19 Tate, J.: On the conjecture of Birch and Swinnerton-Dyer and a geometric

analog, Seminaire Bourbaki 1965/66, Exposé 306. In: Grothendieck, A. (Ed.) Dix Exposés sur la Cohomologie des Schemas. pp. 189-214 Amsterdam: North-Holland 1968

20 Tate, J.: Algorithm for determining the type of a singular fiber in an elliptic pencil. In: Birch, B.J. and Kuyk, W. (Eds.) Modular Functions of One Variable IV (Lect. Notes in Math. 476.) pp. 33-52 Berlin Heidelberg New York: Springer 1973

21 Tate, J. and Oort, F.: Group schemes of prime order. Ann. Scient. de l'Ecole Normal Superieur (4) **3** (1970) 1-21

22 Ulmer, D.L.: L-functions of universal curves over Igusa curves. (preprint) (1988)

23 Weil, A.: Adeles and Algebraic Groups. Boston: Birkhäuser 1982