The Arithmetic of Universal Elliptic Modular Curves

by
Douglas L. Ulmer
A.B., Princeton University, 1982

Submitted in partial fulfillment of the requirements for the
Degree of Doctor of Philosophy in the Department of
Mathematics at Brown University

May, 1987

This dissertation by Douglas L. Ulmer is accepted in its present form
by the Department of Mathematics as satisfying the dissertation requirement
for the degree of Doctor of Philosophy

Date . . . . . .

. . . . . .
Benedict H. Gross

Recommended to the Graduate Council

Date . . . . . .

. . . . . .
Joseph Harris

Date . . . . . .

. . . . . .
Michael Rosen

Approved by the Graduate Council

Date . . . . . .

. . . . . .

Vita

Douglas L. Ulmer was born on July 9, 1960 in Nevada, and attended various public schools there. After graduating from Chaparral High School in 1978, he attended Princeton University and was awarded the A.B. degree in Mathematics with High Honors in 1982. He entered the Ph.D. program in Mathematics at Brown University after a brief career as a computer consultant in Cambridge, U.K. Mr. Ulmer held an Alfred P. Sloan Doctoral Dissertation Fellowship during the academic year 1986-87.

Acknowledgements

It is a pleasure to thank the many mathematicians who have generously provided advice and encouragement during this work, including Bill Fulton, Jim Milne, Arthur Ogus, Arnold Pizer, Mike Rosen, Chad Schoen and especially Joe Harris. Discussions with my fellow graduate students, in particular Fernando Cuckierman, were also an invaluable motivation; I thank all these people heartily. Of course a few words would not suffice to express my gratitude for the support and inspiration given to me by Laura Hollengreen. Most importantly, the interest and enthusiasm of my teacher, Dick Gross, provided the stimulation that made the thesis possible.

Contents

Chapter I
Introduction

1. Elliptic Modular Surfaces. In [27], Shioda defined a universal elliptic curve over a class of modular curves by analytic techniques and studied the geometry of the resulting elliptic surface. In particular, he showed that the Néron-Severi group of this surface is generated by components of fibers of the map to the base curve and by the zero section, in other words that there are no other sections. In an appendix, he raised several interesting arithmetic questions related to the reduction of this surface modulo a prime not dividing the level of the modular base curve.

In [7], Gross continued this line of investigation by defining an integral model for one of Shioda's modular surfaces and analyzing the reduction of the resulting arithmetic threefold at various places. When the level of the base curve is a prime p, the reduction modulo p is a reducible surface, one of whose components is a regular elliptic surface with a moduli-theoretic interpretation. The goal of this thesis is to determine whether this moduli interpretation can be exploited to test the Artin-Tate conjectures for these varieties.

2. The Conjectures of Artin and Tate and of Birch and Swinnerton-Dyer. Let $\mathcal{E}$ be a smooth irreducible surface over the finite field $\mathbf{F}_q$ of characteristic p. For $0 \leq i \leq 4$ define $P_i(T)$ as the characteristic polynomial of Frobenius acting on $H^i_{\acute{e}t}(\mathcal{E} \otimes \overline{\mathbf{F}_q}, \mathbf{Q}_\ell)$ for some $\ell \neq p$. The polynomial $P_i(T)$ is known to be independent of ℓ and to have integral coefficients with constant term 1; its roots have absolute value $q^{-i/2}$.

In [31] Tate conjectured that the order of vanishing of $P_2(q^{-s})$ at $s = 1$ is given by

$$\operatorname*{ord}_{s=1} P_2(q^{-s}) = \operatorname{Rank}(NS(\mathcal{E})) = \rho$$

where NS is the Néron-Severi group of $\mathcal{E}$ over $\mathbf{F}_q$, which is Abelian and finitely generated. Furthermore, Artin and Tate [32] conjectured that, if Br denotes the order of the (conjectured to be finite) Brauer group of $\mathcal{E}$, then the leading term of the Taylor expansion of $P_2(q^{-s})$ at $s = 1$ should be

given by

$$\lim_{s\to 1} \frac{P_2(q^{-s})}{(s-1)^\rho} = \frac{\langle D_i, D_j\rangle Br}{|NS_{tor}|^2 q^\alpha}$$

where $\langle D_i, D_j\rangle$ is the absolute value of the discriminant of the intersection pairing on a basis of NS modulo torsion and α is an integer defined in terms of geometric invariants of $\mathcal{E}$. Tate and Milne have shown that in fact the rank assertion implies the leading coefficient assertion. The conjecture has been verified in some special cases, notably for rational surfaces (Milne, [13]), and certain $K3$s. The next interesting case is that of elliptic surfaces.

If $\mathcal{E} \xrightarrow{\pi} X$ is an elliptic surface over $\mathbf{F}_q$ then the generic fiber E/K of the family π is an elliptic curve over the function field $K = \mathbf{F}_q(X)$. In this situation the Tate conjecture for $\mathcal{E}$ is known to be equivalent to the conjecture of Birch and Swinnerton-Dyer for E. (In fact, the latter motivated the former.) Birch and Swinnerton-Dyer conjectured (cf. Tate [32]) that, if E/K is any elliptic curve over a global field K, and if $L(E/K, s)$ is the Hasse-Weil L-function of E over K, the order of vanishing of $L(E/K, s)$ at $s = 1$ is given by

$$\operatorname*{ord}_{s=1} L(E/K, s) = \mathrm{Rank}(E(K)) = r$$

where $\mathrm{Rank}(E(K))$ is the rank of the finitely generated Abelian group of K-rational points of E. Let τ be the Tamagawa measure of E/K, $Ш$ the Tate-Shafarevitch group of E/K and R the absolute value of the discriminant of the height pairing on E with respect to some basis of $E(K)$ modulo torsion. Then Birch and Swinnerton-Dyer also conjectured that $Ш$ is finite and

$$\lim_{s\to 1} \frac{L(E/K, s)}{(s-1)^r} = \frac{\tau R |Ш|}{|E(K)_{tor}|^2}.$$

3. The Main Theorems. Let X_1 be the Igusa curve of level p; this is the moduli space of pairs (E, P) where E is an elliptic curve and P is a point of $E^{(p)}$ which generates the kernel of the Verschiebung. The space X_1 is a smooth complete curve defined over $\mathbf{F}_p$ which is naturally a $(p-1)/2$-sheeted cover of the projective j-line, fully ramified over the supersingular j-invariants. Since X_1 is a fine moduli space away from the supersingular points, we can form a universal curve there and compactify it to a regular relatively minimal surface $\mathcal{E} \to X_1$. When $p \equiv 3 \pmod 4$ we

can descend $\mathcal{E}$ to a surface over $\mathbf{P}^1_j$ which corresponds to a somewhat less natural moduli problem (elliptic curves with square Hasse invariant) but which has the advantage of being fibred over a very simple base. (This is one component of the reduction mentioned in No. 1.) Because of the moduli-theoretic origins of $\mathcal{E}$, it provides a good testing ground for the conjectures of No. 2. For our purposes, it will be more convenient to discuss the conjecture of Birch and Swinnerton-Dyer for the generic fiber $E/\mathbf{F}_q(j)$ of this family. The translation into results about the surface $\mathcal{E}$ and the Tate conjecture is straightforward.

After some preliminaries about X_1 and the geometry of E, our first main theorem is a calculation of the Hasse-Weil L-function of E over $\mathbf{F}_q(j)$. Let $H_q(T)$ be the characteristic polynomial of the Hecke operator T_q acting on the space of cusp forms of weight 3 and quadratric character for the group $\Gamma_0(p)$.

Theorem II.13.1. $L(E/\mathbf{F}_q(j), s) = H_q(q^{-s})$.

Two immediate corollaries are that L is an entire function of s and that it satisfies a functional equation of the usual type. The real benefit, however, of this result is the following: Hecke showed ([8], §13) that, if $h(-p)$ denotes the class number of the imaginary quadratic field $\mathbf{Q}(\sqrt{-p})$, then $h(-p)$ of the eigenvalues of T_p are equal to $-p$. Since $T_{p^n} = {T_p}^n$, over $\mathbf{F}_q(j)$ such that $\mathbf{F}_q \supseteq \mathbf{F}_{p^2}$ the L-function of E will have a zero of order at least $h(-p)$. Thus we have produced elliptic curves whose L-functions vanish to high order and the conjecture of Birch and Swinnerton-Dyer implies that they should have large rank. A further characteristic of these curves as test objects is that they are arithmetically subtle, in the sense that one expects a drastic change in behavior passing from $\mathbf{F}_p$ to $\mathbf{F}_{p^2}$. Clearly, no purely geometric techniques will suffice to understand them.

In Chapter III we make technical preparations for what follows. If R is a complete discrete valuation ring of characteristic p with finite residue field, i.e. $R = \mathbf{F}_q[[t]]$, then we calculate the first cohomology groups of the flat topology on R with coefficients in any finite flat group scheme of order p over R. This explicit calculation allows us to easily deduce an analog of the local flat duality result of Mazur and Roberts.

Chapter IV is an attempt to bound the rank of E from above using the technique of a p-descent.

We develop all the machinery necessary to carry out this calculation based on a knowledge of the reduction type of an elliptic curve at all places and of its Hasse invariant. Applied to the universal curve E this yields the following bound.

Proposition IV.8.6. *Write $q = p^f$ and let $h = h(-p)$ be the class number of the quadratic field $\mathbf{Q}(\sqrt{-p})$. Then*

$$\mathrm{Rank}(E(\mathbf{F}_q(j)) \leq \begin{cases} \frac{p+5}{12}f - \frac{h-1}{2} - 1 & \textit{when } p \equiv 7 \pmod{24} \\ \frac{p+1}{12}f - \frac{h-1}{2} - 1 & \textit{when } p \equiv 11 \pmod{24} \\ \frac{p-7}{12}f - \frac{h-1}{2} - 1 & \textit{when } p \equiv 19 \pmod{24} \\ \frac{p+13}{12}f - \frac{h-1}{2} - 1 & \textit{when } p \equiv 23 \pmod{24} \end{cases}.$$

Finally, in Chapter V we present some tables containing explicit examples of the objects studied here.

Chapter II
The Universal Elliptic Modular Curve

§ Preliminaries on Elliptic Curves

1. Frobenius. Fix a prime number p and let S be a scheme in characteristic p, i.e. an $\mathbf{F}_p$ scheme. Then we have a canonical morphism $F_{abs} : S \to S$, the *absolute Frobenius*. F_{abs} is the identity on points and raises sections of the structure sheaf to the p-th power. Given any S-scheme X, we define the S-scheme $X^{(p)}$ via the Cartesian diagram:

$$\begin{array}{ccc} X^{(p)} & \longrightarrow & X \\ \downarrow & & \downarrow \\ S & \xrightarrow{F_{abs}} & S. \end{array}$$

Then the absolute Frobenius of X factors canonically as

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

where F is the (S-linear) *relative Frobenius*. Given a morphism of S-schemes $f : X \to X'$, we also get $f^{(p)} : X^{(p)} \to X'^{(p)}$. Note that, despite the notation, both $X^{(p)}$ and F depend on the structure of X as S-scheme.

When $X = E$ is an elliptic curve over S, F is an inseperable isogeny of degree p. We denote the dual isogeny by V (for "Verschiebung"). Thus V is also an isogeny of degree p and the composition $V \circ F$ is the multiplication-by-p map in the group of E (Katz-Mazur, [10, 12.1, 12.2]).

2. Supersingular Elliptic Curves. If E is an elliptic curve over a field k of characteristic p, E has either p points of order p over the algebraic closure $\overline{k}$ or it has none. In the first case we say that E is *ordinary*; this is the case if and only if $V : E^{(p)} \to E$ is étale. If E has no p torsion, we say that E is *supersingular* in which case $V : E^{(p)} \to E$ and $p : E \to E$ are purely inseperable. Being

supersingular is a geometric property of E, that is it depends only on the isomorphism class of E over $\overline{k}$, i.e. on the modular invariant $j(E)$. Actually, it depends only on the isogeny class of E; in particular E is supersingular if and only if $E^{(p)}$ is.

If E is supersingular then multiplication by p defines an isomorphism $p : E \xrightarrow{\sim} E^{(p^2)}$, so $j(E)$ lies in $\mathbf{F}_{p^2}$. Thus there are only finitely many j-invariants of supersingular elliptic curves. In characteristics 2 and 3 there is one supersingular j-invariant, namely $j = 0 = 1728$. For $p \geq 5$, there are exactly

$$\begin{aligned}
&(p-1)/12 \quad \text{when } p \equiv 1 \pmod{12} \\
&(p+7)/12 \quad \text{when } p \equiv 5 \pmod{12} \\
&(p+5)/12 \quad \text{when } p \equiv 7 \pmod{12} \\
&(p+13)/12 \quad \text{when } p \equiv 11 \pmod{12}
\end{aligned}$$

supersingular j-invariants and $\frac{1}{2}H(-4p)$ (where $H(-4p)$ is the Hurwitz class number, cf. 15.1) of them are contained in the prime field. A curve with $j = 0$ is supersingular if and only if $p \equiv 2 \pmod 3$ and a curve with $j = 1728$ is supersingular if and only if $p \equiv 3 \pmod 4$. (For this and the next No., the best reference is Robert [19, Chap. IV].)

We define the *supersingular polynomial* in characteristic p as the monic polynomial in j with simple zeroes at the j-invariants of supersingular curves:

$$f_{ss}(j) = \prod_{E \ supersingular} (j - j(E)).$$

Because $E^{(p)}$ is supersingular if and only if E is, this polynomial actually lies in $\mathbf{F}_p[j]$.

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

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

of rank 1 $H^0(S, \mathcal{O}_S)$-modules. 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 of weight $p-1$ in the sense that $A(E, a^{-1}\omega) = a^{p-1}A(E, \omega)$. Thus the Hasse invariant of an elliptic curve E over a field K(without reference to a differential) is defined only up to $(p-1)^{st}$ powers in K; it is zero if and only if E is supersingular.

If $p > 2$ and E is given in Weierstrass form as

$$y^2 = f(x)$$

where $f(x)$ is a cubic polynomial in x and $\omega = dx/2y$ then

$$A(E, \omega) = \text{coefficient of } x^{p-1} \text{ in } f(x)^{p-1/2}.$$

Thus when $p > 3$ and E is given (over say $Spec\ \mathbf{F}_p[Q, R, \left(\frac{Q^3-R^2}{1728}\right)^{-1}]$) as

$$y^2 = x^3 - \frac{Q}{2^4 3}x + \frac{R}{2^5 3^3}$$

then $A(E, dx/2y)$ is a polynomial $A(Q, R)$ in Q and R with coefficients in $\mathbf{F}_p$. In fact if we let $B(Q, R)$ be the polynomial in two variables over $\mathbf{Q}$ such that

$$B(E_4, E_6) = E_{p-1}$$

where E_k is the Eisenstein series of weight k, then B has p-integral coefficients and

$$A(Q, R) \equiv B(Q, R) \pmod{p}.$$

(See for example Swinnerton-Dyer [29] or Robert [19, IV.1].)

Since A vanishes at a pair (Q, R) defining a supersingular curve, it should be related to the supersingular polynomial. In fact, if we denote by $\tilde{f}_{ss}$ the supersingular polynomial with any factors of j or $(j - 1728)$ removed and use the equality $j = Q^3/\Delta$ where $\Delta = Q^3 - R^2/1728$, the following relation holds.

Lemma 3.1. *As polynomials in Q and R over $\mathbf{F}_p$,*

$$A(Q,R) = \begin{cases} \tilde{f}_{ss}(Q^3/\Delta)\Delta^{p-1/12} & \text{when } p \equiv 1 \pmod{12} \\ Q\tilde{f}_{ss}(Q^3/\Delta)\Delta^{p-5/12} & \text{when } p \equiv 5 \pmod{12} \\ R\tilde{f}_{ss}(Q^3/\Delta)\Delta^{p-7/12} & \text{when } p \equiv 7 \pmod{12} \\ QR\tilde{f}_{ss}(Q^3/\Delta)\Delta^{p-11/12} & \text{when } p \equiv 11 \pmod{12} \end{cases}$$

Proof. Note that the exponent of Δ in this expression is just the degree of $\tilde{f}_{ss}$. We do the case $p \equiv 11 \pmod{12}$; the others are similar. Giving Q weight 4 and R weight 6, $A(Q,R)$ is an isobaric polynomial of weight $p-1$. The right hand side also has weight $p-1$ since $\tilde{f}_{ss}(Q^3/\Delta)$ has weight 0. If j_0 is a supersingular invariant $\neq 0$ or 1728 the irreducible polynomial

$$\Delta(j - j_0) = (1 - \frac{j_0}{1728})Q^3 + (\frac{j_0}{1728})R^2$$

divides both sides: this is obvious for the right side and is true for the left because $A(Q,R)$ vanishes along the divisor of points (Q,R) in the plane such that $1728Q^3/(Q^3 - R^2) = j_0$. The functions Q and R also divide both sides. But the sum of the weights of these factors is $p-1$ and thus the two sides differ by a constant. The right side clearly has value 1 at the point $Q = R = 1$ and so does the left, for example by comparing leading coefficients in the q-expansions of the Eisenstein series E_4, E_6 and E_{p-1}. $\square$

We state the following result which is a corollary of the more precise Proposition 2.1 of Chapter IV.

Proposition 3.2. *Let E be an elliptic curve over a scheme S of characteristic p. The kernel of $V : E^{(p)} \to E$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ as group scheme over S if and only if the Hasse invariant of E is a $(p-1)^{st}$ power in $H^0(S, \mathcal{O}_S)^\times$, i.e. if and only if $A(E,\omega) = 1$ for some choice of differential ω on E.*

§ Igusa Structures and Igusa Curves

In this section we define a basic moduli space for elliptic curves in characteristic p, the Igusa curve of level p, and study some of its properties. For a more thorough treatment, we refer to Katz-Mazur [10, Chap. 12].

4. Igusa Structures. 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 $E^{(p)}$ 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

$$Ker\ V$$

are equal as relative Cartier divisors in $E^{(p)}/S$. For example if S is Spec k with k an algebraically closed field, then for ordinary E, P can be any one of the $p-1$ non-trivial points of order p in $E^{(p)}$, while for supersingular E, P is necessarily the origin of $E^{(p)}$.

If (E, P) and (E', P') are two elliptic curves with Igusa structure of level p and $f : E \to E'$ is a morphism of elliptic curves then we say that f is a morphism of Igusa structures if $f^{(p)} : E^{(p)} \to E'^{(p)}$ carries P to P'. Thus it makes sense to speak of isomorphisms of elliptic curves with Igusa structure of level p. For example, (E, P) and $(E, -P)$ are isomorphic via the inverse map of the group scheme E.

5. Igusa Curves. Let Y_1 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_1 is obtained by adding $(p-1)/2$ points which we will refer to as *cusps*. X_1 is the *Igusa curve of level p*.

There is an action of $(\mathbf{Z}/p\mathbf{Z})^\times$ on Y_1 given by

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

and the subgroup $\langle \pm 1 \rangle$ acts trivially. This action extends to X_1 and permutes the cusps simply-transitively. If (E, P) represents a point x of Y_1 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 $(\mathbf{Z}/p\mathbf{Z})^\times/\langle \pm 1 \rangle$ and if $j(E) = 1728$ and E is not supersingular then x has a stabilizer of order 2 in $(\mathbf{Z}/p\mathbf{Z})^\times/\langle \pm 1 \rangle$. Elsewhere on X_1, $(\mathbf{Z}/p\mathbf{Z})^\times/\langle \pm 1 \rangle$ acts freely.

The quotient of X_1 by $(\mathbf{Z}/p\mathbf{Z})^\times/\langle \pm 1 \rangle$ can be naturally identified with the projective j-line; the map $X_1 \to \mathbf{P}^1_j$ away from the cusps is "forget P": $(E, P) \mapsto j(E)$. By the above remarks, $X_1 \to \mathbf{P}^1_j$ is a $(p-1)/2$-sheeted cyclic Galois cover with group $G = (\mathbf{Z}/p\mathbf{Z})^\times/\langle \pm 1 \rangle$; it is totally ramified at the supersingular points and is ramified in triples over $j = 0$ (if not supersingular) and in pairs over $j = 1728$ (if not supersingular). The Riemann-Hurwitz formula yields the expression

$$2g_{X_1} - 2 = \frac{(p-1)(p-11)}{24} - \#\{\textit{supersingular j-invariants}\} \tag{5.1}$$

for the genus g_{X_1} of X_1 when $p \geq 5$; the map $X_1 \to \mathbf{P}^1_j$ is an isomorphism when $p = 3$. Thus for the rest of this section we assume that $p > 3$.

6. A Model for X_1. Recall that $A(Q, R)$ is the reduction mod p of the polynomial in two variables expressing the Eisenstein series E_{p-1} in terms of E_4 and E_6. A is an isobaric polynomial of weight $p-1$ (where Q has weight 4 and R has weight 6). The following result is due to Serre [26]; see also Katz-Mazur [10, 12.8.8].

Proposition 6.1. *When $p > 3$ an affine model for the curve X_1 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 $\mathbf{F}_p(X_1)$ is isomorphic to $\mathbf{F}_p(Q, R)/(A(Q, R) - 1)$.*

Note: In terms of this curve, the supersingular points on X_1 correspond to the points at infinity and the cusps are the points where Q and R satisfy $\Delta(Q, R) = (Q^3 - R^2)/1728 = 0$. The map to $\mathbf{P}^1_j$ is given by $(Q, R) \mapsto j = Q^3/\Delta = R^2/\Delta + 1728$.

Sketch of Proof. If (E, P) is an ordinary elliptic curve with Igusa structure of level p, then P defines an isomorphism of group schemes:

$$\mathbf{Z}/p\mathbf{Z} \to Ker\ V$$

Applying Cartier duality we get an isomorphism

$$Ker\ F \xrightarrow{\phi} \mu_p \hookrightarrow \mathbf{G}_m.$$

Now there exists a unique invariant differential 1-form ω on E such that $\phi^{-1*}(\omega) = \frac{dt}{t}$ where t is the coordinate on $\mathbf{G}_m$ restricted to μ_p. Such a form is invariant under the Cartier operator. Using the differential ω, we can define $Q = c_4(E, \omega)$ and $R = c_6(E, \omega)$ and since ω is fixed by Cartier, we have $A(Q, R) = 1$. Thus we have defined a point of the affine curve above.

Conversely, given Q and R with $A(Q, R) = 1$ we define the curve

$$E = \left\{ y^2 = x^3 - \frac{Q}{2^4 3} x + \frac{R}{2^5 3^3} \right\}$$

Since $A(Q, R) = 1$, E has Hasse invariant 1 so by Proposition 3.2 we have an isomorphism $\psi : \mathbf{Z}/p\mathbf{Z} \to Ker\ V$ and we construct a point of X_1 as $(E, \psi(1))$. This completes the sketch. $\square$

It is easy to describe the action of $(\mathbf{Z}/p\mathbf{Z})^\times$ on this curve: if P corresponds to the differential ω on E then aP corresponds to the differential $a^{-1}\omega$ so we have

$$\langle a \rangle (Q, R) = (a^4 Q, a^6 R).$$

(Here we let $(\mathbf{Z}/p\mathbf{Z})^\times$ act on functions on the left: $f^{\langle a \rangle} = f \circ \langle a^{-1} \rangle .$) Since the polynomial A is isobaric of weight $p - 1$, this new point actually lies on the curve.

7. More on the Galois Action. Let K be the function field $\mathbf{F}_q(X_1) \cong \mathbf{F}_q(Q, R)/(A(Q, R) - 1)$ as in No. 6 and let $\Delta = (Q^3 - R^2)/1728$. If v is a place of K, we say v is supersingular, cuspidal, etc. if the corresponding point of X_1 has those properties. Let S be the set of supersingular places of K not lying over 0 or 1728.

Lemma 7.1. *If v is a supersingular place of K not lying over 0 or 1728 (i.e. $v \in S$) then $ord_v(Q) = -2$, $ord_v(R) = -3$, and $ord_v(\Delta) = -6$. At 0 we have*

$p \pmod 3$	$ord_v(Q)$	$ord_v(R)$	$ord_v(\Delta)$
1	1	0	0
2	$(p-5)/6$	-1	-2

and at 1728 we have

$p \pmod 4$	$ord_v(Q)$	$ord_v(R)$	$ord_v(\Delta)$
1	0	1	0
3	-1	$(p-7)/4$	-3

Proof. Let v be a supersingular place corresponding to j_0. Since $X_1 \to \mathbf{P}^1_j$ is totally ramified over j_0, we have

$$(p-1)/2 = ord_v(j - j_0) = ord_v((Q^3/\Delta) - j_0) = ord_v((R^2/\Delta) + 1728 - j_0).$$

When $j_0 \neq 0$ or 1728, this yields equalities

$$3ord_v(Q) = ord_v(\Delta) = 2ord_v(R)$$

and a local calculation in the (Q, R)-plane shows that $ord_v(\Delta) < 0$. Thus $ord_v(\Delta) = -6a$ where $a = gcd(ord_v(Q), ord_v(R))$. But Q and R generate K over the ground field $\mathbf{F}_q$ so $a = 1$, $ord_v(Q) = -2$, and $ord_v(R) = -3$.

When v lies over 0 or 1728, then $\tilde{f}_{ss}(Q^3/\Delta)$ has valuation 0 and the equality of Lemma 3.1 yields a linear relation among $ord_v(Q)$, $ord_v(R)$ and $ord_v(\Delta)$. We also have

$$ord_v(j - j_0) = \frac{(p-1)}{2},\ 3,\ \text{or } 2$$

according to whether v is supersingular, lies over 0 and is not supersingular, or lies over 1728 and is not supersingular. This yields two more linear relations as above and solving these equations leads to the claims of the lemma. $\square$

We will need a fact about the action of the Galois group of $X_1/\mathbf{P}^1_j$. If $x = (E, P)$ is a point of X_1 with E supersingular, then the cover $X_1 \to \mathbf{P}^1_j$ is totally ramified at x. Thus the Galois group of the cover $G = (\mathbf{Z}/p\mathbf{Z})^\times/\langle \pm 1 \rangle$ acts on the cotangent space at x, i.e. on the 1-dimensional vector space $\mathbf{m}_x/\mathbf{m}_x^2$ where $\mathbf{m}_x \subset \mathcal{O}_x$ is the maximal ideal in the local ring at x. We wish to describe this action as a character of G. There is a natural character $\omega : (\mathbf{Z}/p\mathbf{Z})^\times \to {\mathbf{F}_p}^\times$, namely $\omega(a) = a$. Every other character θ of $(\mathbf{Z}/p\mathbf{Z})^\times$ with values in ${\mathbf{F}_p}^\times$ can be written as a power of ω:

$\theta = \omega^k$ with $0 \leq k \leq p-2$ and θ defines a character of G if and only if k is even. Now let θ be the character of G defined by

$$f^{\langle a \rangle} \equiv \theta(a) f \pmod{\mathbf{m}_x^2} \qquad a \in (\mathbf{Z}/p\mathbf{Z})^\times, \quad f \in \mathbf{m}_x.$$

Proposition 7.2. *The action of G on the tangent space of X_1 at a supersingular point E is given by $\theta = \omega^{-\#Aut(E)}$. So*

$$\theta = \begin{cases} \omega^{-6} & \text{if } j(E) = 0 \\ \omega^{-4} & \text{if } j(E) = 1728 \\ \omega^{-2} & \text{if } j(E) \in S \end{cases}$$

Proof. This is a consequence of Lemma 7.1 and the action of G on Q and R given in No. 6: at 0, $\frac{1}{R}$ is a uniformiser and has weight -6 for G; at 1728, $\frac{1}{Q}$ is a uniformiser with weight -4 for G; finally at the other supersingular points, $\frac{Q}{R}$ is a uniformiser and has weight -2 for G. $\square$

§ The Universal Elliptic Curve

This section is devoted to the definition and study of the first properties of some elliptic curves over global function fields. These curves will be the principal objects of study in the rest of this paper. For simplicity we restrict to the case $p > 3$.

Let us fix some notations for the rest of this section: X_1 is the Igusa curve of level p defined in the previous section and $K = \mathbf{F}_q(X_1)$ is its function field over the field of q elements. Recall that $K \cong \mathbf{F}_q(Q,R)/(A(Q,R)-1)$ where A is the reduction mod p of the polynomial giving E_{p-1} in terms of E_4 and E_6. Let S be the set of supersingular places of K not lying over 0 or 1728.

8. Definitions. Consider the elliptic curve E_1 defined over K by the Weierstrass equation

$$y^2 = x^3 - \frac{Q}{2^4 3} x + \frac{R}{2^5 3^3}.$$

together with the differential $\omega = dx/2y$. E_1 has discriminant $\Delta = \Delta(E,\omega) = (Q^3 - R^2)/1728$ and j-invariant $j = Q^3/\Delta$. Also, $A(E,\omega) = A(Q,R) = 1$. Thus by Proposition 3.2, $E_1^{(p)}$ has a non-trivial K-rational point of order p.

In fact, E_1 is the unique (up to K-isomorphism) curve with these properties. Indeed, any other curve with j-invariant j is $\overline{K}$-isomorphic to E_1 and thus is a quadratic twist of E_1. (Here we use the fact that $j(E_1)$ is transcendental over the prime field so that $Aut_{\overline{K}}(E_1) = \{\pm 1\}$). But twisting by d changes the Hasse invariant by $d^{(p-1)/2}$ so the only twists which leave the Hasse invariant a $(p-1)^{st}$ power are twists where d is a square. Finally, twisting by a square does not change the K-isomorphism class of E_1.

When $p \equiv 3 \pmod 4$, so $(p-1)/2$ is odd, we can canonically descend E_1 to a curve over the rational function field $\mathbf{F}_p(j)$:

Proposition 8.1. *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', etc. are given by the following table:

$p \pmod{24}$	a	a'	b	b'	c	c'
7	3	1	4	2	8	3
11	1	3	1	5	2	9
19	3	3	4	5	8	9
23	1	1	1	2	2	3

This curve has discriminant $\Delta(E, dx/2y) = j^c(j-1728)^{c'}\tilde{f}_{ss}(j)^6$. E becomes isomorphic to E_1 over K_1.

Proof. The uniqueness follows exactly as for E_1: The j-invariant fixes the $\overline{\mathbf{F}_p(j)}$-isomorphism class of E and the only twists which leave the Hasse invariant a square are twists by squares ($(p-1)/2$ is odd).

Let E be the curve defined by the Weierstrass equation above. Then the claims about the j- and Hasse-invariants follow from the assertion that E becomes isomorphic to E_1 over K. Indeed,

that the Hasse invariant of E becomes a $(p-1)^{st}$ power after an extension of degree $(p-1)/2$ shows that it is a square in $\mathbf{F}_p(j)$ and the assertion about the j-invariant is obvious. The assertion about the discriminant follows from a trivial calculation.

It remains to show that E becomes isomorphic to E_1 over K. Here is the case $p \equiv 19 \pmod{24}$:

$$\begin{aligned} E/K &= \left\{ y^2 = x^3 - \frac{j^3(j-1728)^3 \tilde{f}_{ss}(j)^2}{2^4 3} x + \frac{j^4(j-1728)^5 \tilde{f}_{ss}(j)^3}{2^5 3^3} \right\} \\ &= \left\{ y^2 = x^3 - \frac{Q^9 R^6 \tilde{f}_{ss}(Q^3/\Delta)^2}{\Delta^6 2^4 3} + \frac{Q^{12} R^6 \tilde{f}_{ss}(Q^3/\Delta)^3}{\Delta^9 2^5 3^3} \right\} \end{aligned}$$

And by Lemma 3.1, $\tilde{f}_{ss}(Q^3/\Delta) = (R\Delta^{p-7/12})^{-1}$ on X_1. So

$$\begin{aligned} E/K &= \left\{ y^2 = x^3 - \frac{Q^9 R^4}{\Delta^{p+29/6} 2^4 3} x + \frac{Q^{12} R^7}{\Delta^{p+29/4} 2^5 3^3} \right\} \\ &\cong \left\{ y^2 = x^3 - \frac{Q}{2^4 3} x + \frac{R}{2^5 3^3} \right\} \end{aligned}$$

using the change of coordinates

$$(x, y) \mapsto (Q^4 R^2 \Delta^{-(p+29/12)} x, Q^6 R^3 \Delta^{-(p+29/8)} y).$$

The other cases are similar. $\square$

Our main object of study in the rest of this chapter will be E; when necessary we will refer to E_1 as E over K.

9. Local Invariants and Torsion. We know from the expression for Δ that E has good reduction at all places of $\mathbf{F}_p(j)$ away from the cusp ∞, 0, 1728, and the set S of other supersingular points. The fact that $0 < ord_v(\Delta) < 12$ for $v \in S \cup \{0, 1728\}$ implies that the Weierstrass equation (8.1) is minimal except possibly at ∞. The change of coordinates

$$(x, y) \mapsto (j^{2f} x, j^{3f} y) \tag{9.1}$$

(i.e. $\omega \mapsto j^{-f}\omega$) with

$p \pmod{24}$	f
7	$(p+17)/24$
11	$(p+13)/24$
19	$(p+29)/24$
23	$(p+1)/24$

yields a minimal Weierstrass equation at ∞ with $ord_\infty(\Delta) = 1$. Thus E has split multiplicative reduction at ∞. The reduction type at the other places of $\mathbf{F}_p(j)$ can simply be read off from Tate's algorithm [33]. We summarize the results in a table:

(9.2) 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^*

We also need to know about the reduction of $E^{(p)}$ over $\mathbf{F}_q(j)$. Consider the model of $E^{(p)}$ obtained by raising the coefficients of the model (8.1) of E to the p^{th} power, together with the differential $\omega = dx/2y$. This model has good reduction away from 0, 1728, the supersingular points, and the cusp ∞. The following table gives the integer f such that $t_v^{-f}\omega$ is a minimal differential at v (where t_v is a uniformiser at v) and the reduction type at v for the remaining places of $\mathbf{F}_q(j)$.

(9.3) Reduction of $E^{(p)}$ over $\mathbf{F}_q(j)$					
$p \pmod{24}$	0		1728		
7	$(8p-8)/12$	IV^*	$(3p-9)/12$	III^*	
11	$(2p-10)/12$	II^*	$(9p-3)/12$	III	
19	$(8p-8)/12$	IV^*	$(9p-3)/12$	III	
23	$(2p-10)/12$	II^*	$(3p-9)/12$	III^*	

$p \pmod{24}$	$v \in S$		∞	
7	$(6p-6)/12$	I_0^*	$-(p^2+17p)/24$	I_p
11	$(6p-6)/12$	I_0^*	$-(p^2+13p)/24$	I_p
19	$(6p-6)/12$	I_0^*	$-(p^2+29p)/24$	I_p
23	$(6p-6)/12$	I_0^*	$-(p^2+p)/24$	I_p

Finally, for E over K we have:

(9.4) Reduction of E over K				
$p \pmod{12}$	0	1728	$v \in S$	∞
1	I_0	I_0	I_0^*	I_1
5	IV^*	I_0	I_0^*	I_1
7	I_0	III^*	I_0^*	I_1
11	IV^*	III^*	I_0^*	I_1

We will need the conductor of E to study the functional equation of the L-series of E. Recall that the conductor of an elliptic curve E over a global function field K can be described as an

effective divisor on the curve corresponding to K. The support of this divisor is exactly the set of places of K where the curve E has bad reduction and, when $p > 3$, the coefficient of a place is 1 if E has multiplicative reduction there and is 2 if E has additive reduction there. If the field of constants of K has q elements then the norm of a divisor D is just $q^{deg\ D}$. Adding up the local contributions specified in (9.1) and (9.2) yields the following result.

Corollary 9.5. *The norm of the conductor N_E of E over $\mathbf{F}_q(j)$ is*

$$q^{(p+23)/6} \text{ when } p \equiv 7 \pmod{12}$$

$$q^{(p+19)/6} \text{ when } p \equiv 11 \pmod{12}$$

Corollary 9.6. *$E(K\otimes\overline{\mathbf{F}}_p)$ has trivial torsion subgroup. The torsion subgroup of $E^{(p)}(K\otimes\overline{\mathbf{F}}_p)$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$.*

Proof. For the proof we write K instead of $K\otimes\overline{\mathbf{F}}_p$. It follows immediately from Table 9.4 and the fact that the reduction map is injective on prime-to-p torsion that the only possible prime-to-p torsion of E is 2-torsion. That E has reduction type I_1 at the cusps shows that there can be only two points of order 2. But if E had a non-trivial point of order 2 over K, then there would exist a quadratic extension of K which contained the function field of the moduli space of elliptic curves with full level 2 structure. This contradicts the fact that $K/\mathbf{F}_p(j)$ is totally ramified at at least one finite place not lying over 0. Thus there is no prime-to-p torsion. The prime-to-p torsion of $E^{(p)}$ is isomorphic to that of E, thus it is also trivial.

If E had a non-trivial point P of order p rational over K, then the quotient $E/\langle P\rangle$ of E by the group P generates, which is $E^{(1/p)}$, would be rational over K. On the other hand, $j(E^{(1/p)}) = j^{1/p}$ which is not an element of K because K has degree $(p-1)/2$ over $\mathbf{F}_p(j)$. Thus $E(K)$ has no p-torsion. We know by Proposition 3.2 that $E^{(p)}(K)$ has a point of order p; if $P \in E^{(p)}(K)$ had order p^2, $E^{(p)}/\langle P\rangle \cong E^{(1/p)}$ would be rational over K. Thus the torsion subgroup of $E^{(p)}(K)$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$. $\square$

Consider the group scheme $Ker\ V : E^{(p)} \to E$. Since $Ker\ V$ becomes isomorphic to $\mathbf{Z}/p\mathbf{Z}$ over the function field $K = \mathbf{F}_p(X_1)$, the endomorphism ring of $Ker\ V$ is just $\mathbf{Z}/p\mathbf{Z}$. With this

identification, we can describe the action of $G = Gal(K/\mathbf{F}_p(j))$ on $Ker\ V$ by an $\mathbf{F}_p$-valued character χ:

$$P^\sigma = \chi(\sigma)P \qquad P \in Ker\ V(K),\ \sigma \in G.$$

Recall that we defined a character $\omega : (\mathbf{Z}/p\mathbf{Z})^\times \to \mathbf{F}_p{}^\times = (\mathbf{Z}/p\mathbf{Z})^\times$ by $\omega(a) = a$; the characters of $G = (\mathbf{Z}/p\mathbf{Z})^\times/\langle\pm 1\rangle$ are given by even powers of ω.

Proposition 9.7. *The action of $Gal(K/\mathbf{F}_p(j))$ on $Ker\ V$ is given by $\chi = \omega^{(p-3)/2}$.*

Proof. It is enough to calculate the action of G on the K-valued points of $Ker\ V$. Consider K as the function field of the open curve obtained from X_1 by removing the supersingular points, 0, 1728, and the cusps. Then elements of K can be thought of as functions on pairs (E, P) where E is an elliptic curve and P is a non-trivial point of order p on $E^{(p)}$. Also the universal $E^{(p)}$ defines a family of elliptic curves over the open curve, each with a non-trivial point of order p. Choose a non-trivial K-valued point $\mathbf{P} \in E^{(p)}(K)_p$; this gives an isomorphism

$$E^{(p)}(K)_p \cong \mathbf{Z}/p\mathbf{Z}$$

and similarly for all the fibers of the family defined by $E^{(p)}$ (thinking of $\mathbf{P}$ as a section of the family). Assume that $\mathbf{P}$ has the property that $\mathbf{P}(E, P) = \pm P$. (Such a $\mathbf{P}$ exists because the open curve is a fine moduli space.) Using the identification on the fibers as above, we can distinguish between (E, P) and $(E, -P)$ and we always choose the representative such that P corresponds to a square in $(\mathbf{Z}/p\mathbf{Z})^\times$. With this convention we have $\mathbf{P}(E, P) = P$. Now G acts on the left, so

$$\begin{aligned}
\mathbf{P}^{\langle a\rangle}(E, P) =& \mathbf{P}(\langle a^{-1}\rangle(E, P)) \\
=& \mathbf{P}(E, a^{-1}P) \\
=& \pm\, a^{-1}P \quad \text{(according to whether } a \text{ is a square or not)} \\
=& a^{(p-3)/2}P \\
=& a^{(p-3)/2}\mathbf{P}(E, P)
\end{aligned}$$

□

It is also possible (and a good check on the signs) to calculate the action of G directly on the coordinate ring of $Ker\ V$ using Propositions IV.2.1 and 10.1.

10. The Hasse Invariant of E. Let E be the elliptic curve over $\mathbf{F}_p(j)$ whose equation is given in (8.1) and let ω be the differential $dx/2y$. We use the fact that $A(E/\mathbf{F}_p(j), \omega)$ is a square to give a more explicit description of it.

Proposition 10.1.

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

where d and d' are given by:

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

Proof. We do the case $p \equiv 23 \pmod{24}$: 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 ∞ and one knows that the q-expansion of the Hasse invariant of the Tate curve begins with 1 (Katz-Mazur [10, 12.4.2]), this constant must be 1. $\square$

11. Tamagawa Numbers. Let L be a global function field and $\mathbf{A}_L$ the adèles of L, i.e. the restricted direct product

$$\prod_{\mathcal{O}_v} L_v$$

where $\mathcal{O}_v$ is the ring of integers in the completion L_v for a place v of L. There is a natural measure

$$\mu = \prod \mu_v$$

where μ_v is the Haar measure for which $\mu_v(\mathcal{O}_v) = 1$. L imbeds diagonally in $\mathbf{A}_L$ and the quotient $\mathbf{A}_L/L$ is compact. Let $D_L = \mu(\mathbf{A}_L/L)$; if L is the function field of a curve of genus g with field of constants $\mathbf{F}_q$, then (cf. Weil [35, 2.1.3])

$$D_L = q^{g-1}.$$

In particular,

$$D_{\mathbf{F}_q(j)} = q^{-1}. \tag{11.1}$$

If X is an elliptic curve over L and ω is a differential on X, for each v ω induces a differential ω_v on the curve X_v over L_v deduced from X; using μ_v we get a measure $|\omega_v|$ on $X_v(L_v)$. When the differential ω_v is a Néron differential (i.e. is the differential corresponding to a minimal Weierstrass equation), then Tate [33] has shown that

$$\int_{X_v(\mathcal{O}_v)} |\omega_v| = \frac{\#X(l_v)}{q}$$

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

$$\lambda_v = \frac{\#X(l_v)^\circ}{q}$$

where $\#X(l_v)^\circ$ is the number of points on the connected component of the closed fiber of the Néron model of X then $\{\lambda_v\}$ is a set of convergence factors in the sense of Weil [35, 2.3]. In this situation, we can form the product measure

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

Finally, we define the *Tamagawa number* $\tau(X, \omega, L)$ to be the measure of the set of $\mathbf{A}_L$ points of X with respect to Ω.

Proposition 11.2. *Let $C = \prod_{v \neq \infty} c_v$ be the product over all finite places v of the order of the group of geometric components of the special fiber of the Néron model of E at v which are rational over $\mathbf{F}_q$. Then the Tamagawa numbers of E and $E^{(p)}$ are given by*

$$\tau(E, dx/2y, \mathbf{F}_q(j)) = \begin{cases} Cq^{-(p-7)/24} & \text{when } p \equiv 7 \pmod{24} \\ Cq^{-(p-11)/24} & \text{when } p \equiv 11 \pmod{24} \\ Cq^{-(p+5)/24} & \text{when } p \equiv 19 \pmod{24} \\ Cq^{-(p-23)/24} & \text{when } p \equiv 23 \pmod{24} \end{cases}$$

and

$$\tau(E^{(p)}, dx/2y, \mathbf{F}_q(j)) = \begin{cases} Cpq^{-(3p+3)/24} & \text{when } p \equiv 7 \pmod{24} \\ Cpq^{-(3p-9)/24} & \text{when } p \equiv 11 \pmod{24} \\ Cpq^{-(3p-9)/24} & \text{when } p \equiv 19 \pmod{24} \\ Cpq^{-(3p+3)/24} & \text{when } p \equiv 23 \pmod{24} \end{cases}$$

Proof. Because E is a projective variety, $E(\mathbf{A}_{\mathbf{F}_q(j)}) = \prod_v E(\mathbf{F}_q(j)_v)$ and we need only compute local integrals. Let k_v be the residue field of $\mathbf{F}_q(j)$ at v. We have already observed that $\omega = dx/2y$ is a minimal differential away from ∞ so at these places

$$\int_{E(\mathbf{F}_q(j)_v)} \lambda_v^{-1} |\omega_v| = \frac{\#E(k_v)}{\#E(k_v)^\circ} = c_v$$

where c_v is the number of geometric components of the closed fiber at v which are rational over k_v. At ∞, the differential ω is not minimal; using the change of coordinates and notation of (9.1) we find

$$\int_{E(\mathbf{F}_q(j)_\infty)} \lambda_\infty^{-1} |\omega_\infty| = q^{-f} c_\infty.$$

Putting this together, we see that

$$\begin{aligned} \tau &= D_L^{-1} \prod_v \int_{E(\mathbf{F}_q(j)_v)} \lambda_v^{-1} |\omega_v| \\ &= q \left(\prod_{v \neq \infty} c_v \right) q^{-f} \end{aligned}$$

which proves the first assertion.

The proof of the second assertion is exactly the same, once one has established that, away from ∞, the number of rational components on the special fiber of the Néron model of E is equal to that of $E^{(p)}$. This follows, for example, from the fact that this number is prime to p. $\square$

We record the following result for later use.

Corollary 11.3.

$$\frac{\tau(E, dx/2y, \mathbf{F}_q(j))}{\tau(E^{(p)}, dx/2y, \mathbf{F}_q(j))} = \begin{cases} p^{-1}q^{(p+5)/12} & \text{when } p \equiv 7 \pmod{24} \\ p^{-1}q^{(p+1)/12} & \text{when } p \equiv 11 \pmod{24} \\ p^{-1}q^{(p-7)/12} & \text{when } p \equiv 19 \pmod{24} \\ p^{-1}q^{(p+13)/12} & \text{when } p \equiv 23 \pmod{24} \end{cases}$$

It will be useful in considering the fine conjectures of Birch and Swinnerton-Dyer to evaluate the constant C of Proposition 11.2.

Proposition 11.4. *Let $C = \prod_{v \neq \infty} c_v$ be as in Proposition 11.2, H=H(-4p) be the Hurwitz class number of the quadratic order of discriminant $-4p$, and $h = h(-p)$ be the class number of the quadratic order of discriminant $-p$. Then the value of C 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	$2^{(H+h-1)/2}$	$3 \cdot 2^{(p-1)/6}$
11	$2^{(H+h-3)/2}$	$2^{(p-5)/6}$

Proof. Consider a supersingular elliptic curve E defined over the field of p^2 elements. If π denotes the Frobenius map, then π^2 is an endomorphism of E and as elements of $End(E)$, $\pi^2 = \pm p$. Thus π^2 fixes all the points of order 2 on E, i.e. they are rational over $\mathbf{F}_{p^2}$. Now assume that E is defined over the field $\mathbf{F}_p$ and consider the action of π on the non-trivial points of order 2 on E. Since these points are rational over $\mathbf{F}_{p^2}$, π^2 fixes them, which implies that the image of π in the automorphism group of these points is of order 2. Therefore, at least one non-trivial point of order 2 on E is rational over $\mathbf{F}_p$. They are all rational over $\mathbf{F}_p$ if and only if the endomorphism $\pi - 1$ annihilates these points. But this is equivalent to 2 dividing $\pi - 1$ as an endomorphism of E, i.e. that $\frac{\pi-1}{2} \in End(E)$. Now when this is the case, E can be lifted to an elliptic curve in characteristic 0 with complex multiplication

by the ring of integers in $\mathbf{Q}(\sqrt{-p})$ (cf. the proof of Lemma 15.2). Such curves are parameterized by the class group of $\mathbf{Q}(\sqrt{-p})$ which has order $h(-p)$ and class field theory shows that $E_{\mathcal{P}}$ reduces to the same curve as $E_{\mathcal{P}'}$ if and only if $\mathcal{P}' = \mathcal{P}^{\pm 1}$ in the class group. Thus since $h(-p)$ is odd (by genus theory), there are $(h(-p)+1)/2$ elliptic curves (up to $\overline{\mathbf{F}_p}$-isomorphism) defined over $\mathbf{F}_p$ all of whose points of order 2 are rational over $\mathbf{F}_p$. Note that when $p \equiv 3 \pmod 4$ some curve with $j = 1728$ always has 4 points of order 2 rational over $\mathbf{F}_p$ and any curve with $j = 0$ always has only 2 points of order 2 rational over $\mathbf{F}_p$.

Now the proposition follows from this discussion applied to the Néron model of E at the various places v of $\mathbf{F}_q(j)$: for $v \in S$, there exists a ramified quadratic extension over which E obtains good reduction. Furthermore, the components of the Néron model correspond to the points of order 2 on this curve, and their rationality is independent of the choice of extension. The cases $v = 0$ and $v = 1728$ can be checked directly and the proposition now follows from some arithmetic using the fact that there are $\frac{1}{2}H(-4p)$ supersingular j-invariants over the field $\mathbf{F}_p$. $\square$

§ The L-function of E

12. Definitions. Let A be an elliptic curve over a global field L. If v is a non-archimedean place of L where A has good reduction then let A_v be the curve obtained by reducing A mod v and let q_v be the cardinality of the residue field at v. We define $a_{v,n}$ by

$$\#A_v(\mathbf{F}_{q_v^n}) = q_v^n + 1 - a_{v,n}.$$

The a_v satisfy $|a_{v,n}| \leq 2\sqrt{q_v^n}$ and in fact $a_v = a_{v,1}$ determines all the $a_{v,n}$: if we define a function of a complex variable s by $L_v(s) = (1 - a_v q^{-s} + q_v^{1-2s})$, then

$$L_v(s) = exp\left(\sum_n \frac{1}{n} a_{v,n} q_v^{-ns}\right) \tag{13.1}$$

where the latter converges. If A has bad reduction at v, we set $L_v(s)$ to be

$$1, \qquad 1 - q^{-s} \quad \text{or} \quad 1 + q^{-s}$$

as A has additive, split multiplicative or non-split multiplicative reduction at v.

We define the *Hasse-Weil L-function* of A over L as

$$L(A/L,s) = \prod_{non-archimedean\ v} L_v(s)^{-1}.$$

This converges for Re $s>\frac{3}{2}$ and is conjectured to have an analytic continuation to an entire function which satisfies a functional equation for $s \mapsto 2-s$. The goal of this section is to compute the L-function of the curve E over the global field $\mathbf{F}_q(j)$.

13. Statement. Consider the space of modular forms of weight 3 and quadratic character for the group

$$\Gamma_0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) | c \equiv 0 \pmod{p} \right\}.$$

This space, which we denote by $S_3 = S_3(\Gamma_0(p), \left(\frac{-}{p}\right))$, is a complex vector space of dimension $d = [p/6]$ consisting of holomorphic functions on the upper half plane for which

$$f(\gamma z) = \left(\frac{d}{p}\right)(cz+d)^3 f(z) \qquad \text{for } \gamma \in \Gamma_0(p)$$

and which satisfy a growth condition at infinity. On this space we have Hecke operators T_q for all $q = p^n$ whose effect on Fourier expansions is:

$$T_q : \sum a_n e^{2\pi i n z} \mapsto \sum a_{qn} e^{2\pi i n z}.$$

Note that $T_{p^n} = (T_p)^n$. Let $H_q(T)$ be the characteristic polynomial of this operator:

$$H_q(T) = det(1 - T \cdot T_q|_{S_3}).$$

The principal result of this chapter is:

Theorem 13.1. $L(E/\mathbf{F}_q(j), s) = H_q(q^{-s})$.

It should be emphasized that the right hand side of this equality is a quantity which can be explicitly calculated. See V.2 for some examples.

We will give the proof in No. 15, but first let us derive some consequences. One knows that $H_p(T)$ has integral coefficients and a factorization

$$H_p(T) = \prod_{\alpha} (1 - \alpha T)$$

where the eigenvalues α all have absolute value p (cf. Li [11, Thm. 3]).

Corollary 13.2. *$L(E/\mathbf{F}_q(j), s)$ is an entire function.*

Recall that the norm of the conductor N_E of E is q^f where $f = (p-23)/6$ if $p \equiv 7 \pmod{12}$ and $f = (p+19)/6$ if $p \equiv 11 \pmod{12}$ (cf. 9.5), and the discriminant $D_{\mathbf{F}_q(j)} = q^{-1}$ (cf. 11.1).

Corollary 13.3. *Let $\Lambda(s) = N_E^{s/2} D_{\mathbf{F}_q(j)}^{2s} L(E/\mathbf{F}_q(j), s)$. Then $\Lambda(s) = \pm\Lambda(2-s)$.*

Proof. Since H_q has integral, thus real, coefficients of absolute value q, the reciprocal roots $\{\alpha_i\}$ of H_q satisfy $\{\alpha_i\} = \{\overline{\alpha_i}\} = \{q/\alpha_i\}$. When $p \equiv 7 \pmod{12}$ we have

$$N_E^{s/2} D_{\mathbf{F}_q(j)}^{2s} = \left(q^{p-1/6}\right)^{s/2}$$

and

$$\begin{aligned}
\Lambda(s) &= \left(q^{(p-1)/6}\right)^{s/2} \left(\prod_{i=1}^{p-1/6} (1 - \alpha_i q^{-s}) \right) \\
&= \pm \left(q^{(p-1)/6}\right)^{(2-s)/2} \left(q^{(p-1)/6}\right)^{s-1} \left(\frac{q^{(p-1)/6}}{\prod \alpha_i} \right) \prod_i (1 - \alpha_i q^{-s}) \\
&= \pm \left(q^{(p-1)/6}\right)^{(2-s)/2} \prod_i \left(\frac{q^s}{\alpha_i} - 1 \right) \\
&= \pm \left(q^{(p-1)/6}\right)^{(2-s)/2} \prod_i \left(q^{s-2} \overline{\alpha_i} - 1 \right) \\
&= \pm\Lambda(2-s).
\end{aligned}$$

The proof for $p \equiv 11 \pmod{12}$ is similar. □

If $\{\alpha\}$ are the reciprocal roots of $H_p(T)$, the sign is given by $(-1)^k$ where

$$k = \#\{\alpha \in \mathbf{R} | \alpha < 0\} [\mathbf{F}_q : \mathbf{F}_p] + 1.$$

14. Consequences for the Conjecture of Birch and Swinnerton-Dyer. Hecke showed that, if $h(-p)$ denotes the number of classes of positive definite quadratic forms of discriminant $-p$, then $h(-p)$ of the α's are equal to $-p$. Since $T_{p^n} = {T_p}^n$, $H_{p^n}(T) = \prod_\alpha (1 - \alpha^n T)$ and so over $\mathbf{F}_q(j)$ with $\mathbf{F}_q \supseteq \mathbf{F}_{p^2}$, H_q has q as a reciprical root of multiplicity at least $h(-p)$. Thus the conjecture of Birch and Swinnerton-Dyer predicts that the rank of the Mordell-Weil group of E is at least $h(-p)$ over $\mathbf{F}_{p^2}(j)$. On the other hand, experimental evidence suggests that over the field $\mathbf{F}_p(j)$, E has rank 0, and when this is the case we can evaluate the order of the Tate-Shafarevitch group Ш. (See IV.1 for the definition.)

Proposition 14.1. *If $H_q(q^{-1}) \neq 0$ then the rank of the Mordell-Weil groups of E and $E^{(p)}$ are 0 and both $Ш(\mathbf{F}_q(j), E)$ and $Ш(\mathbf{F}_q(j), E^{(p)})$ have finite order. The orders of these groups are as follows:*

$$|Ш(\mathbf{F}_q(j), E)| = H_q(q^{-1})\tau(E, dx/2y, \mathbf{F}_q(j))$$
$$|Ш(\mathbf{F}_q(j), E^{(p)})| = H_q(q^{-1})\tau(E^{(p)}, dx/2y, \mathbf{F}_q(j)).$$

(We use $|G|$ to denote the order of a finite group G.)

Proof. It follows from the work of Tate [32, §3] and the equivalence of the conjectures of Birch and Swinnerton-Dyer and of Tate that

$$\mathrm{Rank}(E/\mathbf{F}_q(j)) \leq \operatorname*{ord}_{s=1} L(E/\mathbf{F}_q(j), s).$$

But by the hypothesis and Theorem 13.1, $\mathrm{ord}_{s=1}\, L(E/\mathbf{F}_q(j), s) = \mathrm{ord}_{s=1}\, H_q(q^{-s}) = 0$. Furthermore, by Milne [14, 8.1] the equality $\mathrm{Rank}(E/\mathbf{F}_q(j)) = \mathrm{ord}_{s=1}\, L(E/\mathbf{F}_q(j), s)$ implies the refined conjecture of Birch and Swinnerton-Dyer on the leading coefficient of the Taylor expansion of $L(E/\mathbf{F}_q(j), s)$ at $s = 1$. Applied to $E/\mathbf{F}_q(j)$, this says

$$|Ш(\mathbf{F}_q(j), E)| = \frac{L(E/\mathbf{F}_q(j), 1)\,|E_{tor}|^2}{\tau(E, dx/2y, \mathbf{F}_q(j))\,R}$$

where R is the regulator, i.e. the determinant of the height pairing on E. But $|E_{tor}| = 1$ and $R = 1$ because the rank is 0, which proves the proposition for E. Finally, $E^{(p)}$ is isogenous to E over $\mathbf{F}_q(j)$, so they have the same rank and the same L-function and the same arguments apply. □

For the reader's amusement we calculate the orders of $Ш(\mathbf{F}_p(j), E)$ and $Ш(\mathbf{F}_p(j), E^{(p)})$ for

$3 < p < 60$ using the table in V.2:

p	$\lvert Ш(\mathbf{F}_p(j), E)\rvert$	$\lvert Ш(\mathbf{F}_p(j), E^{(p)})\rvert$
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	$2^2 5^2$	$2^2 5^2 59^4$

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

Unfortunately, there are still many questions to be answered here. First one should have a better understanding of the Hecke polynomial H_p. One knows that all of its inverse roots have absolute value p and that $-p$ occurs at least $h(-p)$ times. Are other roots equal to $\pm p$ (thereby leading one to expect E to have higher rank in those cases) or more generally do other roots differ from p by a root of unity? If not, one would have $\mathrm{Rank}(E(\overline{\mathbf{F}_p}(j))) \leq h(-p)$.

More importantly, and probably much more difficult, is the issue of constructing in some natural way the $h(-p)$ points of infinite order on E over $\mathbf{F}_{p^2}(j)$ that the conjectures predict. This enterprise would probably be considerably complicated by the existence of extra roots of H_{p^2} equal to p^{-2}. If one had these points and an understanding of the polynomial H_q, a calculation of the height pairing on a basis of the points of infinite order would yield a formula for the order of $Ш$ analogous to 14.1.

15. The Calculation. The essence of the proof given here seems to go back to Ihara [9]; a more conceptual proof along the lines of Deligne [4] should also be possible.

If A is an elliptic curve over a finite field $\mathbf{F}_q$ of characteristic p and if A has $q+1-a$ points then a is congruent mod p to the norm from $\mathbf{F}_q$ to $\mathbf{F}_p$ of the Hasse invariant of A (cf. the last page of

Demazure [4] where this result is attributed to Manin). (This makes sense because the only $(p-1)^{st}$ power in $\mathbf{F}_p$ is 1.) In particular, A is supersingular if and only if $a = 0$. If $j(A) \neq 0$ or 1728 so $Aut_{\overline{\mathbf{F}_p}}(A) = \pm 1$ then A has one other form over $\mathbf{F}_q$, and this twisted curve has $q+1+a$ points. Thus when $p \equiv 3 \pmod 4$, so -1 is not a square mod p and $(p-1)/2$ is odd, the j-invariant ($\neq 0,\ 1728$) of a curve A together with the condition that its Hasse invariant be a square completely determines the number of points on A. (If $j = 0$ and the Hasse invariant is a square there are two possibilities for a and if $j = 1728$ there are three.) Conversely, given a with $|a| \leq 2\sqrt{q}$ and $\left(\frac{a}{p}\right) = 1$, we would like to know how many curves have $q + 1 - a$ points over $\mathbf{F}_q$.

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 $\mathcal{O}_d$ (= 2 if $d < -4$). Finally, define the *Hurwitz class number*

$$H(D) = \sum_{df^2 = D} \frac{h(d)}{w(d)}. \tag{15.1}$$

Lemma 15.2. *Assume $p \equiv 3 \pmod 4$. Given a with $|a| \leq 2\sqrt{q}$ and $\left(\frac{a}{p}\right) = 1$ there are $H(a^2 - 4q)$ elliptic curves over $\mathbf{F}_q$ with $q + 1 - a$ points.*

Here we are making the convention that a curve with $j = 0$ should count only 1/3 (as it will be counted with two other values of a) and a curve with $j = 1728$ should count 1/2 (it will be counted with one other a).

Proof. This is a consequence of Deuring's lifting theory. Deuring [5, §4] showed that, given an ordinary elliptic curve in characteristic p and a place $\mathcal{P}$ of $\overline{\mathbf{Q}}$ above p, there exists a unique elliptic curve in characteristic zero with the same endomorphism ring and reducing modulo $\mathcal{P}$ to the given curve. Furthermore the reduction map gives an isomorphism of the endomorphism rings. Thus counting curves in characteristic p amounts to counting curves with complex multiplication by an order in an imaginary quadratic field. Such curves correspond to ideal classes in the order.

If $A/\mathbf{F}_q$ has $q + 1 - a$ points then its Frobenius endomorphism satisfies the equation

$$X^2 - aX + q = 0$$

so the endomorphism ring $\mathcal{O}$ of the lift contains an element π satisfying the same equation. This implies that $d = discriminant(\mathcal{O})$ and $discriminant(\pi) = a^2 - 4q$ satisfy $df^2 = a^2 - 4q$ for some f. Then recalling our counting convention, we have

$$\#\{\text{curves with } q+1-a \text{ points}\} = \sum_{\substack{\mathcal{O}_d \\ d|a^2-4q}} \frac{h(d)}{w(d)} = H(a^2-4q)$$

□

The other ingredient we need is:

Theorem (Eichler Trace Formula). *The trace of T_q acting on*

$$S_3(\Gamma_0(p), \left(\frac{-}{p}\right))$$

is

$$-1 - \frac{1}{2}\sum_{|a|\leq 2\sqrt{q}} a\left(\frac{a}{p}\right) H(a^2-4q).$$

See Eichler [6] for the proof.

Proof of Theorem 13.1. First some notation. Let us call a place v of $\mathbf{F}_q(j)$ *good* if E has good reduction at v. For a good place v of $\mathbf{F}_q(j)$ let $deg(v)$ be its degree, so the residue field at v has $q_v = q^{deg(v)}$ elements, and let $q_v^n - a_{v,n} + 1$ be the number of $\mathbf{F}_{q_v^n}$-rational points on the reduction of E at v. Fix an integer m; given $x \in \mathbf{F}_{q^m}$, let a_x be the a defined above for a curve of j-invariant x and square Hasse-invariant. Then the crux of the matter is:

$$\begin{aligned}
\sum_{\substack{\text{good } v \\ deg(v)|m}} deg(v) a_{v,m/deg(v)} &= \sum_{x\in\mathbf{F}_{q^m}} a_x \\
&= \sum_{\substack{|a|\leq 2\sqrt{q^m} \\ \left(\frac{a}{p}\right)=1}} a(\#\ x \text{ such that } a_x = a) \\
&= \sum_{\substack{|a|\leq 2\sqrt{q^m} \\ \left(\frac{a}{p}\right)=1}} aH(a^2-4q) \\
&= \frac{1}{2}\sum_{|a|\leq 2\sqrt{q^m}} a\left(\frac{a}{p}\right) H(a^2-4q) \\
&= -1 - Tr\ T_{q^m}
\end{aligned}$$

Using the fact that the local factors L_v at the supersingular points are 1 and $L_\infty = (1 - q^{-s})$, we find

$$\begin{aligned}
L(s)^{-1}\left(\frac{1}{1-q^{-s}}\right) &= \prod_{good\ v} (1 - a_v q_v^{-s} + q_v^{1-2s}) \\
&= \prod_v exp\left(\sum_{n=1}^{\infty} \frac{1}{n} a_{v,n} q_v^{-ns}\right) \\
&= exp \sum_v \sum_n \frac{1}{n} a_{v,n} q_v^{-ns} \\
&= exp \sum_m \left(\sum_{deg(v)|m} \frac{deg(v)}{m} a_{v,m/deg(v)}\right) q^{-ms} \\
&= exp \sum_m \left(-1 - Tr\ T_{q^m}\right) q^{-ms} \\
&= \left(\frac{1}{1-q^{-s}}\right) \frac{1}{H(q^{-s})}
\end{aligned}$$

And the theorem is proved. $\square$

Chapter III
Flat Cohomology

The goal of this chapter is to compute the flat cohomology groups of the spectrum of a complete discrete valuation ring of residue characteristic p with coefficients in the sheaf defined by a group scheme of order p. This calculation yields a local flat duality result as a simple corollary. For ease of exposition (and because this is all we need) we restrict to the equal characteristic case; however, the arguments presented here extend readily to the mixed characteristic case first studied by Roberts [20].

§ Background and Statement

1. Topological and Cohomological Definitions. We summarize some concepts about the flat topology, its sheaves and its cohomology in order to establish notation. The basic reference is Milne [15].

There are several variants of the flat topology, but by Milne [15, III.3] they are essentially equivalent from the point of view of cohomology. We work with the faithfully flat quasi-finite site: for any scheme V, we call a V-scheme $U \to V$ an (fpqf) *open set* of V if $U \to V$ is locally of finite type, flat and quasi-finite. If $\{U_i \to V\}$ is a collection of open sets such that the (set-theoretic) union of the images of the $U_i \to V$ is all of V, then we call $\{U_i \to V\}$ an (fpqf) *open cover* of V. That the union of the images be all of V is equivalent to $\coprod_i U_i \to V$ being faithfully flat. Given two open sets $\{U_i \to V\}$ and $\{U_j \to V\}$, the role of their intersection is played in this theory by the fiber product $U_i \times_V U_j$; when there will be no confusion about the base of the product in question, we will denote this by U_{ij}.

Fix a scheme X. The category of open sets of X together with the collection of all coverings of open sets of X satisfies three properties:

(1) An isomorphism $U \xrightarrow{\sim} V$ is a covering.

(2) If $\{U_i \to V\}_i$ is a covering and $\{U_{i,j} \to U_i\}_j$ are coverings for all i then $\{U_{i,j} \to V\}_{i,j}$ is a covering.

(3) If $\{U \to X\}$ is an open set and $\{U_i \to X\}$ is a covering then $\{U_i \times_X U \to U\}$ is a covering.

Thus we have defined a *Grothendieck topology* in the sense of Artin [2].

A *sheaf* (of abelian groups) for the flat topology on X is a contravariant functor from the open sets of X to abelian groups which satisfies the usual sheaf axioms. If S is a sheaf on X and $U \to X$ is an open set we call the value of S at $U \to X$ the group of *sections* of S over U and denote it (rather ambiguously as the value in general depends on the map $U \to X$) by $S(U)$. Two fundamental examples of sheaves are $\mathbf{G}_a$ and $\mathbf{G}_m$. Let $\Gamma(U, \mathcal{O}_U)$ denote the global sections of the structure sheaf of U; then $\mathbf{G}_a(U) = \Gamma(U, \mathcal{O}_U)$ (as additive group) and $\mathbf{G}_m(U) = \Gamma(U, \mathcal{O}_U)^\times$ (the invertible elements of this ring).

Let G be a group scheme over X. Then for every open set $U \to X$, we have the group of U-valued points of G: $G(U) = Hom_X(U, G)$. In fact (Milne, [15, II.1.7]) when G is flat over X this association gives us a sheaf in the flat topology on X. A sheaf that arises in this way is said to be *representable* and to be *represented* by G and the sheaf determines the group scheme. For example, $\mathbf{G}_a$ is represented by the X-group scheme

$$X \times_{\mathbf{Z}} Spec\ \mathbf{Z}[T]$$

and $\mathbf{G}_m$ is represented by

$$X \times_{\mathbf{Z}} Spec\ \mathbf{Z}[T, T^{-1}]/(TT^{-1} = 1).$$

All of the sheaves we consider will be representable, and we will use the same notation for a group scheme over X and the sheaf it defines. A map of schemes $i : X \to Y$ induces a map from sheaves on Y to sheaves on X: $G \mapsto i^*G$. In particular, if $i : U \to X$ is an open set and G is a representable sheaf on X then i^*G is represented by $G \times_X U$.

One verifies that the category of sheaves on the flat topology of a scheme is Abelian and possesses enough injectives. Thus we can define the cohomology groups $H^i(X, G)$ of X with coefficients in

a sheaf G as the right derived functors of the global sections functor $G \mapsto G(X)$. All of the usual formalism holds; in particular, associated to a short exact sequence of sheaves

$$0 \to G' \to G \to G'' \to 0$$

on X one has a long exact sequence of cohomology groups

$$\cdots \to H^i(X, G') \to H^i(X, G) \to H^i(X, G'') \to H^{i+1}(X, G') \to \cdots$$

Also, a map of schemes $i : X \to Y$ induces a map of cohomology groups $H^i(Y, G) \to H^i(X, i^*G)$.

2. Group Schemes of Order p. We review the Oort-Tate classification of finite flat group schemes of order p [18]. This classification holds over a fairly general (mixed characteristic) base, but for our purposes it suffices to work only in characteristic p. It is the fact that these group schemes have such an explicit description that allows us to make our cohomological calculations by elementary means.

Fix an affine scheme $S = Spec\ A$ in characteristic p. Then to any two elements a and b of A such that $ab = p = 0$, Oort and Tate associate a group scheme $G_{a,b}/S = G_{a,b}$. As a scheme, $G_{a,b}$ is

$$Spec\ A[X]/(X^p - aX)$$

and its group structure is defined by the comultiplication

$$\delta : X \mapsto X \otimes 1 + 1 \otimes X + b \sum_{i+j=p} c_{i,j} X^i \otimes X^j$$

where $c_{i,j}$ are universal constants which can be defined in terms of Jacobi sums. In fact, since S is of characteristic p, one has

$$c_{i,j} = \frac{1}{i!}\frac{1}{j!}.$$

There is a map from $G_{a,b}$ to $G_{a',b'}$ if and only if $\gamma^{p-1}a = a'$ and $b = \gamma^{p-1}b'$ with $\gamma \in A$, in which case the map is given by

$$G_{a',b'} \leftarrow G_{a,b}$$

$$X \mapsto \gamma X.$$

This is an isomorphism if and only if γ is invertible in A. When S is integral, one of a or b must be zero; $G_{a,b}$ is étale as a scheme over S if and only if a is a unit of A.

Here are some basic examples:

(1) $G_{1,0} = Spec\ A[X]/X^p - X \cong \mathbf{Z}/p\mathbf{Z}/A$ the constant group scheme:

$$\mathbf{Z}/p\mathbf{Z}(B) = \mathbf{Z}/p\mathbf{Z}$$

(with the obvious group structure) if B is a connected A-scheme.

(2) $G_{0,0} = Spec\ A[X]/X^p \cong \alpha_p$

$$\alpha_p(Spec\ B) = \{b \in B | b^p = 0\}$$

which is a group under addition because the A-algebra B has characteristic p.

(3) $G_{0,1} = Spec\ A[X]/X^p \cong \mu_p$.

$$\mu_p(Spec\ B) \cong \{b \in B^\times | b^p = 1\}$$

with multiplicative group structure.

Note that the description of μ_p as $G_{0,1}$ is not the naive one; let us make the isomorphism explicit. If

$$\mu_p = Spec\ A[Y]/(Y^p - 1)$$

with comultiplication

$$Y \mapsto Y \otimes Y,$$

and

$$G_{0,1} = Spec\ A[X]/X^p$$

with comultiplication

$$X \mapsto X \otimes 1 + 1 \otimes X + \sum_{i+j=p} c_{i,j} X^i \otimes X^j$$

then the isomorphism $\mu_p \cong G_{0,1}$ is given by

$$X \mapsto \sum_{i=1}^{p-1} -i^{-1} Y^i$$

$$Y \mapsto \sum_{i=0}^{p-1} X^i/(i!). \tag{2.1}$$

Given any finite flat group scheme G over S, we get another, $\tilde{G}$ the *Cartier dual* of G as

$$\tilde{G} = Hom(G, \mathbf{G}_m)$$

the homomorphisms being as S-group schemes. One has canonically $\tilde{\tilde{G}} \cong G$. In terms of the Oort-Tate classification, $\widetilde{G_{a,b}} = G_{b,a}$. Thus, $\widetilde{\mathbf{Z}/p\mathbf{Z}} = \mu_p$ and α_p is self-dual.

These three basic examples define sheaves on S and fit into exact sequences

$$0 \to \mathbf{Z}/p\mathbf{Z} \to \mathbf{G}_a \xrightarrow{\wp} \mathbf{G}_a \to 0$$

$$0 \to \mu_p \to \mathbf{G}_m \xrightarrow{F} \mathbf{G}_m \to 0$$

$$0 \to \alpha_p \to \mathbf{G}_a \xrightarrow{F} \mathbf{G}_a \to 0$$

where $\wp(x) = x^p - x$ and $F(x) = x^p$. (Note that these last two sequences are exact in the flat—or any finer—topology, but <u>not</u> in the étale topology).

Finally, in the case where A is a local ring with field of fractions K, we say that $G = G_{a,b}$ over A is *generically split* if $G \otimes K = G \times_{Spec\ A} Spec\ K$ is isomorphic to either μ_p or $\mathbf{Z}/p\mathbf{Z}$. This is the case if and only if a and b are $(p-1)^{st}$ powers in A (and one of them is non-zero).

3. Facts About the Base. Let R be the power series ring $\mathbf{F}_q[[t]]$ and K the field of finite-tailed Laurent series $\mathbf{F}_q((t))$. R is a discrete valuation ring with valuation induced by $ord(t) = 1$ and K is its field of fractions. Let $\wp : K \to K$ be the map

$$\wp(x) = x^p - x.$$

We want to define filtrations on and pairings between the discrete group $K/\wp(K)$ and the compact group $K^\times/K^{\times p}$. Most of the facts that we need are in Weil [34] and Serre [25].

The map $\wp$ is $\mathbf{F}_p$-linear; first consider it restricted to $\mathbf{F}_q$. The kernel of $\wp : \mathbf{F}_q \to \mathbf{F}_q$ is $\mathbf{F}_p$ and the image is exactly the kernel of the trace map

$$Tr : \mathbf{F}_q \to \mathbf{F}_q$$

$$x \mapsto x^p + x^{p^2} + \ldots x^q.$$

Thus $\mathbf{F}_q/\wp(\mathbf{F}_q) \xrightarrow{\sim} \mathbf{F}_p$ via Tr. If $x \in K$ has $ord(x)>0$ then x is in $\wp(\mathbf{F}_q)$. Indeed, let $y = x + x^p + x^{p^2} + \dots$ (which converges because $ord(x)>0$). Then $\wp(y) = x$. If $x \in K$ has $ord(x) = i<0$, then $ord(\wp(x)) = pi$, and any $y \in K$ with $ord(y) = pj<0$ can be written as $\wp(y') + y''$ with $ord(y') = j$ and $ord(y'') \geq pj + 1$. Thus if we define $P^{[i]}$ as the image in $K/\wp(K)$ of the set

$$\{x \in K | ord(x) \geq -i\}$$

then the $P^{[i]}$ form an increasing exhaustive filtration of $K/\wp(K)$ such that $P^{[0]} \cong R/\wp(R)$ has order p and $P^{[i]}/P^{[i-1]}$ has order q if $p \not| \, i$ and is trivial if $p|i$. We can summarize all this as

$$\{0\} \underset{p}{\subseteq} P^{[0]} \underset{q}{\subseteq} P^{[1]} \underset{q}{\subseteq} \dots \underset{q}{\subseteq} P^{[p-1]} = P^{[p]} \underset{q}{\subseteq} P^{[p+1]} \underset{q}{\subseteq} \dots \subseteq K/\wp(K).$$

Now consider the multiplicative group $K^\times$. The choice of a uniformizer t gives a splitting

$$K^\times = t^{\mathbf{Z}} \times {\mathbf{F}_q}^\times \times U^{(1)}$$

where ${\mathbf{F}_q}^\times$, the multiplicative group of $\mathbf{F}_q$, is cyclic of order $q-1$ and $U^{(1)} = \{x \in K | ord(1-x)>0\}$ is the set of *principal units*. As for $U^{(1)}$, one knows (Weil [34, Chap. II, §3]) that it is a free $\mathbf{Z}_p$-module (written exponentially) on generators

$$(1 + \alpha_i t^j) \qquad 1 \leq i \leq [\mathbf{F}_q : \mathbf{F}_p] \quad 1 \leq j \quad p \not| j$$

where $\alpha_1, \dots \alpha_{[\mathbf{F}_q:\mathbf{F}_p]}$ are a set of coset representatives of $\mathbf{F}_p$ in $\mathbf{F}_q$. Letting $U^{[i]}$ $(i \geq 0)$ be the image in $K^\times/K^{\times p}$ of

$$\{x \in K | ord(1-x) \geq i\}$$

we find that the $U^{[i]}$ form a decreasing exhaustive filtration of $K^\times/K^{\times p}$ where $U^{[0]} \cong R^\times/R^{\times p}$ has index p in $K^\times/K^{\times p}$ and $U^{[i]}/U^{[i+1]}$ has order q when $p \not| \, i$ and is trivial if $p|i$. All this is summarized by

$$\{1\} \subseteq \dots \underset{q}{\subseteq} U^{[p+1]} = U^{[p]} \underset{q}{\subseteq} U^{[p-1]} \underset{q}{\subseteq} \dots \underset{q}{\subseteq} U^{[1]} = U^{[0]} \underset{p}{\subseteq} K^\times/K^{\times p}.$$

If K is given the topology induced from the valuation, $K/\wp(K)$ is a discrete group and $K^\times/K^{\times p}$ is compact. In fact, these topological groups are Pontrjagin dual. First we define the *Artin-Schreier pairing*

$$[\ ,\ ) : K/\wp(K) \times K^\times/K^{\times p} \to \mathbf{F}_p$$

by the formula

$$[f,g) = Tr_{\mathbf{F}_q/\mathbf{F}_p}\left(Res\ f\frac{dg}{g}\right) \tag{3.1}$$

where the differential dg is calculated formally:

$$d(\sum a_i t^i) = (\sum i a_i t^{i-1})dt$$

and Res is the residue (i.e. the coefficient of $t^{-1}dt$). Composing [,) with

$$\mathbf{Z}/p\mathbf{Z} \to \mathbf{Q}/\mathbf{Z}$$

$$a \mapsto a/p$$

yields the map which puts the two groups in duality (Serre, [25, Chap. XIV, Prop. 14]). It is clear from the explicit form of [,) that $P^{[i]}$ and $U^{[i+1]}$ are orthogonal complements under this pairing.

4. Statement of the Theorem. As before, let $R = \mathbf{F}_q[[t]]$ and $K = \mathbf{F}_q((t))$. Then we have maps

$$Spec\ K \overset{i}{\hookrightarrow} Spec\ R \overset{j}{\hookleftarrow} Spec\ \mathbf{F}_q$$

where i is an open immersion and j is a closed immersion. If G is a sheaf for the flat topology on $Spec\ R$ (e.g. coming from a group scheme over R) then i^*G is a sheaf on the flat topology of $Spec\ K$ which we will sometimes refer to as $G|_{Spec\ K}$, $G\otimes K$ or even G. Also, to simplify typography, we will write $H^i(R,G)$ and $H^i(K,G)$ for the cohomology groups $H^i(Spec\ R,G)$ and $H^i(Spec\ K, i^*G)$.

Consider the following exact sequences of sheaves for the flat topology on $Spec\ K$:

$$0 \to \mathbf{Z}/p\mathbf{Z} \to \mathbf{G}_a \overset{\wp}{\to} \mathbf{G}_a \to 0$$

$$0 \to \mu_p \to \mathbf{G}_m \overset{F}{\to} \mathbf{G}_m \to 0$$

$$0 \to \alpha_p \to \mathbf{G}_a \overset{F}{\to} \mathbf{G}_a \to 0$$

where as before $\wp(x) = x^p - x$ and $F(x) = x^p$. Then a piece of the corresponding long exact cohomology sequence reads:

$$H^0(K,\mathbf{G}_a) \to H^0(K,\mathbf{G}_a) \to H^1(K,\mathbf{Z}/p\mathbf{Z}) \to H^1(K,\mathbf{G}_a)$$

$$H^0(K, \mathbf{G}_m) \to H^0(K, \mathbf{G}_m) \to H^1(K, \mu_p) \to H^1(K, \mathbf{G}_m)$$

$$H^0(K, \mathbf{G}_a) \to H^0(K, \mathbf{G}_a) \to H^1(K, \alpha_p) \to H^1(K, \mathbf{G}_a).$$

But one knows (Serre [25, Chap. X, §1]) that $H^1(K, \mathbf{G}_a) = H^1(K, \mathbf{G}_m) = 0$ (Satz 90 and its additive analog), that $H^0(K, \mathbf{G}_a) = K$ (as additive group) and that $H^0(K, \mathbf{G}_m) = K^\times$. Thus the coboundary maps induce isomorphisms

$$H^1(K, \mathbf{Z}/p\mathbf{Z}) \cong K/\wp(K)$$

$$H^1(K, \mu_p) \cong K^\times/K^{\times p}$$

$$H^1(K, \alpha_p) \cong K/K^p.$$

A similar calculation, using the same exact sequence of sheaves on *Spec* R and the facts that $H^1(R, \mathbf{G}_a) = H^1(R, \mathbf{G}_m) = 0$ and that $H^0(R, \mathbf{G}_a) = R$ and $H^0(R, \mathbf{G}_m) = R^\times$ yields isomorphisms

$$H^1(R, \mathbf{Z}/p\mathbf{Z}) \cong R/\wp(R)$$

$$H^1(R, \mu_p) \cong R^\times/R^{\times p}$$

$$H^1(R, \alpha_p) \cong R/R^p.$$

Our goal is to calculate $H^1(R, G_{a,b})$ for any finite flat group scheme $G_{a,b}$ of order p. We start with the generically split case. Recall that a group scheme $G_{a,0}$ over R is said to be generically split if $G_{a,0} \otimes K \cong \mathbf{Z}/p\mathbf{Z}$. This occurs if and only if a is a $(p-1)^{st}$ power in $K^\times$. Similarly, $G_{0,b}$ is generically split if $G_{0,b} \otimes K \cong \mu_p$ which occurs if and only if b is a $(p-1)^{st}$ power in $K^\times$. In this situation we have maps

$$H^1(R, G_{a,0}) \to H^1(K, G_{a,0}) \cong H^1(K, \mathbf{Z}/p\mathbf{Z}) \cong K/\wp(K)$$

and

$$H^1(R, G_{0,b}) \to H^1(K, G_{0,b}) \cong H^1(K, \mu_p) \cong K^\times/K^{\times p}$$

where the first maps are induced from $i : Spec\ R \to Spec\ K$. Our first main result is

Theorem 4.1. *Let $G_{a,0}$ and $G_{0,b}$ be generically split group schemes over R. Then the maps*

$$H^1(R, G_{a,0}) \to K/\wp(K)$$

$$H^1(R, G_{0,b}) \to K^\times/K^{\times p}$$

are injections which induce isomorphisms

$$H^1(R, G_{a,0}) \cong P^{[i]}$$

$$H^1(R, G_{0,b}) \cong U^{[j]}$$

where $i = \frac{ord(a)p}{(p-1)}$ and $j = \frac{ord(b)p}{(p-1)} + 1$.

The condition that $G_{a,0}$ and $G_{0,b}$ be generically split insures that $\frac{ord(a)}{(p-1)}$ and $\frac{ord(b)}{(p-1)}$ are integers. Note that the theorem is in agreement with our calculation of $H^1(R, \mathbf{Z}/p\mathbf{Z})$ and $H^1(R, \mu_p)$ above when $a = 1$ and $b = 1$ respectively.

5. Duality Results. The explicit calculation of Theorem 4.1 allows one to give a particularly elementary proof of a duality result analogous to that of Mazur and Roberts. (For another proof in our context, see Milne [16, III.6].) Let G be a finite flat group scheme over a scheme X. Then the general theory of cohomology provides us with cup-product pairings:

$$H^i(X, G) \times H^j(X, \tilde{G}) \to H^{i+j}(X, \mathbf{G}_m)$$

(where, as before, $\tilde{G}$ is the Cartier dual of G) (Milne, [15, V.1.17]).

Theorem (Tate Duality). *Let K be a complete discrete valuation ring with finite residue field and let G be a finite flat commutative group scheme over K (of any order) with Cartier dual $\tilde{G}$. Then the cup product pairing*

$$H^1(K, G) \times H^1(K, \tilde{G}) \to H^2(K, \mathbf{G}_m) \cong \mathbf{Q}/\mathbf{Z} \tag{5.1}$$

is a perfect pairing. Furthermore, when $G \cong \mathbf{Z}/p\mathbf{Z}$ this cup product is computed by the Artin-Schreier pairing (3.1).

This is due to Tate [30] when the order of G is prime to the characteristic of K (and thus G is étale); the general result was obtained by Schatz, cf. [22].

If $K = \mathbf{F}_q((t))$ and $R = \mathbf{F}_q[[t]]$ and G is a group scheme over R, then the cup products are compatible with restriction maps, in the sense that the diagram

$$\begin{array}{ccc} H^1(K,G)\times H^1(K,\tilde{G}) & \longrightarrow & H^2(K,\mathbf{G}_m) \\ \uparrow \qquad\quad \uparrow & & \uparrow \\ H^1(R,G)\times H^1(R,\tilde{G}) & \longrightarrow & H^2(R,\mathbf{G}_m) \end{array}$$

commutes. (The vertical maps being induced from $i : Spec\ K \hookrightarrow Spec\ R$). If $G = G_{a,0}$ is a generically split group scheme of order p over R, then this reads

$$\begin{array}{ccc} H^1(K,\mathbf{Z}/p\mathbf{Z})\times\ H^1(K,\mu_p) & \longrightarrow & H^2(K,\mathbf{G}_m) \\ \uparrow \qquad\quad \uparrow & & \uparrow \\ H^1(R,G_{a,0})\ \times H^1(R,G_{0,a}) & \longrightarrow & H^2(R,\mathbf{G}_m) \end{array} .$$

The following corollary is now an immediate consequence of Theorem 4.1 and the form of the pairing (3.1).

Corollary 5.2. *For a generically split finite flat group scheme G of order p, the images*

$$H^1(R,G_{a,0}) \to H^1(K,\mathbf{Z}/p\mathbf{Z}) \xrightarrow{\sim} K/\wp(K)$$

and

$$H^1(R,G_{0,a}) \to H^1(5,\mu_p) \xrightarrow{\sim} K^\times/K^{\times p}$$

are orthogonal complements under the cup product pairing (5.1).

In fact, as we will see in No. 8, the analogous result is true for any group scheme of order p over R. Finally, using this basic case, the analogous result for group schemes of order prime to p, and a standard dévissage, one proves Corollary 5.2 for <u>any</u> finite flat group scheme G.

One knows (Milne, [15, IV.1.6]) that $H^2(R,\mathbf{G}_m) = 0$ because R is a complete local ring. Therefore the images of $H^1(R,G)$ and $H^1(R,\tilde{G})$ for any G annihilate each other under the Artin-Schreier pairing. Thus the proof of Theorem 4.1 will follow from the inequality

$$\#H^1(R,G_{a,0}) \geq pq^{ord(a)} \geq [K^\times/K^{\times p} : H^1(R,G_{0,a})]$$

which will be established in the next section.

§ The Proofs

6. Cech Cohomology and Torsors. The proof of Theorem 4.1 will involve the explicit construction of cohomology classes. In order to do this, we introduce Cech cohomology, which suffices for our purposes because it always agrees with derived functor cohomology on H^1 (Milne, [15, III.2.10]).

Let X be a scheme and G a sheaf of Abelian groups for the flat topology on X. Recall that to give a class in $\check{H}^1(X, G)$ is to give a covering $\{U_i \to X\}$ and, for each pairwise intersection $U_{ij} = U_i \times_X U_j$, a section $g_{ij} \in G(U_{ij})$ satisfying the *cocycle condition*:

$$g_{ij}g_{jk} = g_{ik} \qquad \text{all } i, j, k.$$

Two such collections of data $(\{U_i \to X\}, (g_{ij}))$ and $(\{U_i' \to X\}, (g_{ij}'))$ determine the same class if and only if, after passing to a suitable refinement $\{U_i'' \to X\}$, they differ by a coboundary:

$$g_{ij} - g_{ij}' = b_i - b_j$$

with $b_i \in G(U_i)$. (Here and henceforth we religiously avoid writing in all the appropriate restrictions and refinement maps).

Let us illustrate this explicitly by writing down the isomorphisms

$$K/\wp(K) \xrightarrow{\sim} H^1(K, \mathbf{Z}/p\mathbf{Z})$$

$$K^\times/K^{\times p} \xrightarrow{\sim} H^1(K, \mu_p)$$

in terms of Cech 1-cocycles. Given $x \in K$, we solve (in some algebraic closure of K) the equation $\wp(y) = x$. Then $U_1 = Spec\ K(y) \to Spec\ K$ is a finite faithfully flat morphism, i.e. a cover of *Spec* K. We form the $K(y) \otimes_K K(y)$-valued point

$$g_{11} = 1 \otimes y - y \otimes 1$$

of the group scheme $\mathbf{Z}/p\mathbf{Z}$. This is a point of $\mathbf{Z}/p\mathbf{Z}$ because:

$$\begin{aligned}
\wp(1 \otimes y - y \otimes 1) &= (1 \otimes y - y \otimes 1)^p - (1 \otimes y - y \otimes 1) \\
&= 1 \otimes (y^p - y) - (y^p - y) \otimes 1 \\
&= 1 \otimes x - x \otimes 1 \\
&= 0.
\end{aligned}$$

It is easy to check that this satisfies the cocycle condition. Indeed, let $p_{12},\ p_{13}$ and p_{23} denote the various projections

$$U_1 \times_{Spec\ K} U_1 \times_{Spec\ K} U_1 \to U_1 \times_{Spec\ K} U_1.$$

Then

$$p_{12}^*(g_{11}) = 1 \otimes y \otimes 1 - y \otimes 1 \otimes 1$$

$$p_{23}^*(g_{11}) = 1 \otimes 1 \otimes y - 1 \otimes y \otimes 1$$

and

$$p_{13}^*(g_{11}) = 1 \otimes 1 \otimes y - y \otimes 1 \otimes 1$$

Thus $p_{12}^*(g_{11}) + p_{23}^*(g_{11}) = p_{13}^*(g_{11})$, which is exactly the cocycle condition, and we have defined a class in $\check{H}^1(K, \mathbf{Z}/p\mathbf{Z})$.

Similarly given $x \in K^\times$, we solve $y^p = x$ and consider the cover $U_1 = Spec\ K(y) \to Spec\ K$, which is finite and faithfully flat. Forming the $K(y) \otimes_K K(y)$-valued point of μ_p

$$g_{11} = \frac{1 \otimes y}{y \otimes 1} = (1 \otimes y)(y^{-1} \otimes 1) = y^{-1} \otimes y$$

we get a class in $\check{H}^1(K, \mu_p)$.

We next define torsors (or principal homogeneous spaces) and relate them to Cech cohomology. Fix a scheme X and let G be a sheaf of Abelian groups on X and S a sheaf of sets with a G-action (i.e. for every $U \to X$, an action in the usual sense $G(U) \times S(U) \to S(U)$ compatible with restrictions). S is a *torsor* for G on X (or a *G-torsor*) if there exists a covering of X for the flat topology $\{U_i \to X\}$ such that for each i $S|_{U_i}$ is isomorphic, as sheaf with G-action, to $G|_{U_i}$ acting on itself by left translation. Such an isomorphism amounts to a section $s \in S(U_i)$. Indeed, given s, we have $G|_{U_i} \xrightarrow{\sim} S|_{U_i}$ by $g \to gs$. Conversely, if $G|_{U_i} \xrightarrow{\sim} S|_{U_i}$, let s be the image of the identity of $G(U_i)$. We say that the covering $\{U_i \to X\}$ *trivializes* S. A torsor S is trivial if it is isomorphic to G acting on itself by left translation i.e. if $S(X)$ is non-empty. When G is representable by a finite flat group scheme, S is representable by a scheme, which we will also call S, and this scheme is finite and flat over X (Milne, [15, III.4.2, 4.3]).

Given a torsor S for G over X, we can define a class in $\check{H}^1(X, G)$: choose a trivializing cover $\{U_i \to X\}$ for S. Then for each pairwise intersection, $U_i \times U_j$, we have an isomorphism of sheaves with G-action:

$$(S|_{U_i})|_{U_i \times U_j} \xrightarrow{\sim} (S|_{U_j})|_{U_i \times U_j}$$

which is given by translation by an element g_{ij} of $G(U_i \times U_j)$. Then one checks (Milne [15, III.4.6]) that the covering $\{U_i \to X\}$ and the sections (g_{ij}) define an element of $\check{H}^1(X, G)$ and that this element does not depend on the choices made. In fact, this correspondence induces an isomorphism between the set (actually group, cf. Milne [15, III.4.8]) of G-torsors on X and $\check{H}^1(X, G)$. For example, the class in $K/\wp(K)$ represented by $z \in K$ corresponds to the $\mathbf{Z}/p\mathbf{Z}$-torsor represented by the scheme

$$Spec\ K[X]/(X^p - X - z)$$

with $\mathbf{Z}/p\mathbf{Z}$-action

$$K[X]/(X^p - X - z) \to K[X]/(X^p - X) \otimes K[X]/(X^p - X - z)$$

$$X \mapsto X \otimes 1 + 1 \otimes X.$$

Simlarly, the class in $K^\times/K^{\times p}$ represented by $z \in K^\times$ corresponds to the μ_p-torsor represented by

$$Spec\ K[X]/(X^p - z)$$

with action

$$K[X]/(X^p - z) \to K[X]/(X^p - 1) \otimes K[X]/(X^p - z)$$

$$X \mapsto X \otimes X.$$

This correspondence provides the most convenient way of proving the following result.

Lemma 6.1. *Let $K = \mathbf{F}_q((t))$, $R = \mathbf{F}_q[[t]]$ and let G be a finite flat group scheme over R. Then the restriction map:*

$$\check{H}^1(R, G) \to \check{H}^1(K, G)$$

is injective.

Proof. Let $T = Spec\ A$ be the scheme representing a G-torsor on $Spec\ R$ and assume this torsor is trivial over $Spec\ K$. Thus we have a diagram

$$\begin{array}{ccc} T & \xleftarrow{\tilde{i}} & T \times_{Spec\ R} Spec\ K \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle f} \\ Spec\ R & \xleftarrow[i]{} & Spec\ K \end{array}$$

where $T \times_{Spec\ R} Spec\ K$ is assumed to have a K-valued point, i.e. a section of the map f. Writing the corresponding diagram of rings:

$$\begin{array}{ccc} A & \xrightarrow{\tilde{i}^*} & A \otimes K \\ {\scriptstyle g^*}\uparrow & & \uparrow{\scriptstyle f^*} \\ R & \xrightarrow[i^*]{} & K \end{array}$$

the fact that the torsor is trivial over K implies that there exists a section of the map f^*, i.e. a homomorphism $A \otimes K \to K$ which is a right inverse to f^*. Composing with $\tilde{i}^*$ gives a homomorphism from A to K. But A is finite, thus integral, over R and R is integrally closed in K. This implies that the image of the composed map actually lies in R, i.e. we have a section of g^*. But this provides an R-valued point of T, so T is trivial over R. $\square$

From now on we drop the checks over H^1 as H^1 defined as a derived functor is isomorphic to the Cech group $\check{H}^1$

7. Construction of Classes. We combine the Cech cohomology of No. 6 with our knowledge of maps between group schemes of order p to construct some cohomology classes. Recall that for generically split groups $G_{a,0}$ and $G_{0,b}$ we have maps

$$H^1(R, G_{a,0}) \to H^1(K, G_{a,0}) \cong H^1(K, \mathbf{Z}/p\mathbf{Z}) \cong K/\wp(K)$$

and

$$H^1(R, G_{0,b}) \to H^1(K, G_{0,b}) \cong H^1(K, \mu_p) \cong K^\times/K^{\times p}$$

which are injections by Lemma 6.1.

Proposition 7.1. *Let $G_{a,0}$ and $G_{0,b}$ be generically split group schemes over R. Then*

(1) *The image of $H^1(R, G_{a,0}) \to K/\wp(K)$ contains $P^{[i]}$ where $i = \frac{ord(a)p}{p-1}$.*

(2) *The image of $H^1(R, G_{0,b}) \to K^\times/K^{\times p}$ contains $U^{[j]}$ where $j = \frac{ord(b)p}{p-1}$.*

Corollary 7.2. *$\#H^1(R, G_{a,0}) \geq pq^{ord(a)}$ and $[K^\times/K^{\times p} : H^1(R, G_{0,b})] \leq pq^{ord(b)}$*

Note that this, together with No. 5, completes the proof of Theorem 4.1

Proof. We construct cohomology classes which map to a given class in $P^{[i]}$ or $U^{[j]}$. Choose $\alpha \in R$ such that $\alpha^{p-1} = a$. Given $\overline{x} \in P^{[i]}$, with i as in the statement, $\overline{x}$ is represented by $x \in K$ with $ord(x) \geq -i = -\frac{ord(a)p}{p-1}$. Solve $\wp(y) = x$. Then $ord(y) \geq -\frac{ord(a)}{p-1} = -ord(\alpha)$. Thus αy is integral over R and so $U_1 = Spec\, R[\alpha y] \to Spec\, R$ is finite and faithfully flat. Form the $R[\alpha y] \otimes_R R[\alpha y]$-valued point of $G_{a,0}$

$$g_{11} = 1 \otimes \alpha y - \alpha y \otimes 1.$$

The datum $(\{U_1 \to Spec\, R\}, (g_{11}))$ satisfies the cocycle condition and so define a class in $H^1(R, G_{a,0})$. Under the maps

$$H^1(R, G_{a,0}) \to H^1(K, G_{a,0}) \xrightarrow{\sim} H^1(K, \mathbf{Z}/p\mathbf{Z})$$

this class first goes to

$$1 \otimes_K \alpha y - \alpha y \otimes_K 1 = \alpha \otimes_K y - \alpha y \otimes_K 1$$

and then to

$$1 \otimes y - y \otimes 1$$

which, as we saw in no. 6, corresponds to the class $\overline{x} \in K/\wp(K)$. This proves (1).

(2) is similar but a little more messy. Choose $\beta \in R$ such that $\beta^{p-1} = b$. Take a class $w \in U^{[j]}$ represented by $(1 - x) \in K$ with $ord(x) \geq \frac{ord(b)p}{p-1}$. Let y be such that $(1 - y)^p = 1 - x$. Then $ord(y) \geq \frac{ord(b)}{p-1} = ord(\beta)$. The class in $H^1(K, \mu_p)$ corresponding to w is represented by

$$\left(\{U_1 = Spec\, K(y) \to Spec\, K\}, g_{11} = (1 - y)^{-1} \otimes (1 - y)\right)$$

and the corresponding element of $H^1(K, G_{0,1})$ is represented by

$$\left(\{U_1 \to Spec\, K\}, g_{11} = \sum_{j=1}^{p-1} -j^{-1} \left((1 - y)^{-1} \otimes (1 - y)\right)^j\right)$$

(using the isomorphism $\mu_p \xrightarrow{\sim} G_{0,1}$ (2.1)). We rewrite:

$$\begin{aligned} g_{11} &= \sum_j -j^{-1}((1+y+y^2+\dots)\otimes(1-y))^j \\ &= \sum_j -j^{-1}(1\otimes 1-(1+y+y^2+\dots)\otimes y+(y+y^2+\dots)\otimes 1)^j \end{aligned}$$

Let $z = -(1+y+y^2+\dots)\otimes y+(y+y^2+\dots)\otimes 1$. Then

$$\begin{aligned} g_{11} &= \sum_j -j^{-1}(1\otimes 1+z)^j \\ &= \sum_j -j^{-1}(1\otimes 1+jz+\dots+z^j) \\ &= \sum_j -j^{-1}(jz+\dots+z^j) \end{aligned}$$

Now $ord(y) \geq ord(\beta)$, so $R[y/\beta]$ is integral and thus finite and flat over R. Furthermore y, and thus z, is divisible by β in $R[y/\beta]\otimes_R R[y/\beta]$. If we let $U_1' = Spec\ R[y/\beta]$ and

$$g_{11}' = \frac{1}{\beta}g_{11} = \sum_j -j^{-1}(j(\frac{z}{\beta})+\dots+\beta^{j-1}(\frac{z}{\beta})^j)$$

then $(\{U_1' \to Spec\ R\}, (g_{11}'))$ defines a class in $H^1(R, G_{0,b})$ which maps to the class w we started with. Thus we have established (2). $\square$

Note that the maps $H^1(R, G_{a,0}) \to H^1(K, G_{a,0})$ and $H^1(K, \mathbf{Z}/p\mathbf{Z}) \to K/\wp(K)$ are canonical, while the map $H^1(K, G_{a,0}) \to H^1(K, \mathbf{Z}/p\mathbf{Z})$ depends on the isomorphism $G_{a,0} \to \mathbf{Z}/p\mathbf{Z}$ which is determined by a choice of α such that $\alpha^{p-1} = a$. Replacing α by $\alpha' = \delta\alpha$ with $\delta \in (\mathbf{Z}/p\mathbf{Z})^\times$ composes the isomorphism determined by α with multiplication by δ. Similarly, the maps $H^1(R, G_{0,b}) \to H^1(K, G_{0,b})$ and $H^1(K, \mu_p) \to K^\times/K^{\times p}$ are canonical, while the map $H^1(K, G_{0,b}) \to H^1(K, \mu_p)$ depends on the isomorphism $G_{0,b} \to \mu_p$ which is determined by a choice of β such that $\beta^{p-1} = b$. Replacing β by $\beta' = \delta\beta$ with $\delta \in (\mathbf{Z}/p\mathbf{Z})^\times$ composes the isomorphism determined by β with raising to the δ^{-1} power.

8. Non-Split Group Schemes and Local Flat Duality. We now turn to the non-split case. Let G be a finite flat group scheme of order p over $R = \mathbf{F}_q[[t]]$. Then there is a ring S, integral over R of degree dividing $p-1$, such that G splits over S. (If $G = G_{a,0}$, let $S = R(a^{1/p})$ and if $G = G_{0,b}$, let $S = R(b^{1/p})$.) The map

$$Spec\ S \to Spec\ R$$

is a Galois cover with group H a quotient of $(\mathbf{Z}/p\mathbf{Z})^\times$. This Galois group acts on the S-valued points of G, so the cohomology groups $H^i(S,G)$ are H-modules. The exact sequence of terms of low degree of the Hochschild-Serre spectral sequence reads

$$0 \to H^1(H, G(S)) \to H^1(R,G) \to H^1(S,G)^H \to H^2(H, G(S)) \to \dots$$

But $G(S)$ has order p, which is relatively prime to the order of H, so the end terms vanish and we find

$$H^1(R,G) \cong H^1(S,G)^H.$$

Similarly, the field of fractions L of S is Galois over K with group H and

$$H^1(K,G) \cong H^1(L,G)^H.$$

Note that the actions of H on the groups $H^1(S, G_{a,0}) \cong S/\wp(S)$ and $H^1(S, G_{0,a}) \cong S^\times/S^{\times p}$ are not the standard ones (because the isomorphisms $G_{a,0} \cong \mathbf{Z}/p\mathbf{Z}$ and $G_{0,a} \cong \mu_p$ are not in general defined over R). Let α be such that $\alpha^{p-1} = a$ and form the character $\chi : H \to {\mathbf{F}_p}^\times$, $\sigma \mapsto \sigma(\alpha)/\alpha$ (which does not depend on the choice of α). Then the action of H on $P^{[i]} \subseteq S/\wp(S)$ ($i = ord(a)p/(p-1)$) is

$$s^\sigma = \chi(\sigma)\sigma(s) \tag{8.1}$$

(where $\sigma(s)$ denotes the usual Galois action) and the action on $U^{[i]} \subseteq S^\times/S^{\times p}$ is given by

$$s^\sigma = (\sigma(s))^{\chi(\sigma)^{-1}}. \tag{8.2}$$

One proves this by simply tracing through the isomorphisms, noting that the Galois action on 1-cocycles is given by the action on the coefficients.

It is possible to use these results to give a more explicit description of $H^1(R,G)$ for non-split G (at least for the G that become isomorphic to $\mathbf{Z}/p\mathbf{Z}$) but we will not do that here. Instead, let us use the results we have to prove a more general duality result.

Theorem 8.3. *Let $K = \mathbf{F}_q((t))$, $R = \mathbf{F}_q[[t]]$ and let G be a finite flat group scheme of order p over R with Cartier dual $\tilde{G}$. Then the image of the restriction maps*

$$H^1(R, G) \to H^1(K, G)$$

and

$$H^1(R, \tilde{G}) \to H^1(K, \tilde{G})$$

are exact annihilators under the pairing induced by Tate duality:

$$H^1(K, G) \times H^1(K, \tilde{G}) \to \mathbf{Q}/\mathbf{Z}.$$

Proof. If $G = \alpha_p$, this is obvious from the formula for the pairing $H^1(K, \alpha_p) \times H^1(K, \alpha_p) \to \mathbf{Q}/\mathbf{Z}$ given in, e.g., Schatz [22, Chap. V, §5]. Thus, reversing the roles of G and $\tilde{G}$ if necessary, we can assume that G is of the form $G_{a,0}$. Let $S = R(a^{1/p})$ and $L = K(a^{1/p})$, so G is generically split over S. L is Galois and cyclic over K of degree n where n divides $p-1$; let H be the Galois group. Consider the digram

$$\begin{array}{ccc} H^1(L, G) \times H^1(L, \tilde{G}) & \longrightarrow & \mathbf{Q}/\mathbf{Z} \\ \uparrow \quad \uparrow & & \uparrow \\ H^1(K, G) \times H^1(K, \tilde{G}) & \longrightarrow & \mathbf{Q}/\mathbf{Z}. \end{array}$$

We have just seen that the groups $H^1(K, G)$ and $H^1(K, \tilde{G})$ are exactly the H-invariants of $H^1(L, G)$ and $H^1(L, \tilde{G})$ so the vertical maps on the left are inclusions. The diagram commutes where the map on the right is multiplication by n (Serre [25, Chap. XIII, Prop. 7]). But all the H^1 groups are killed by p, thus are $\mathbf{F}_p$-vector spaces and the pairing is bilinear for this structure. This implies that the pairings factor through $\mathbf{Z}\frac{1}{p}/\mathbf{Z} \cong \mathbf{F}_p$ and multiplication by n is an isomorphism of this group. Thus for the purposes of calculating orthogonal complements, we can assume that the pairing

$$H^1(K, G) \times H^1(K, \tilde{G}) \to \mathbf{F}_p$$

is the restriction of

$$H^1(L, G) \times H^1(L, \tilde{G}) \to \mathbf{F}_p.$$

We also know that this restriction is a perfect pairing and it follows from general considerations or the form of the action of H in (8.1-2), that H acts orthogonally in the sense that

$$\langle x^\sigma, \tilde{x}^\sigma \rangle = \langle x, \tilde{x} \rangle \qquad x \in H^1(L, G), \quad \tilde{x} \in H^1(L, \tilde{G}), \quad \sigma \in H.$$

Now the assertion of the theorem is exactly that

$$H^1(R, \tilde{G})^\perp \cap H^1(K, G) = H^1(R, G)$$

where we use $\perp$ to denote orthogonal complement in $H^1(L, G)$. The inclusion $\supseteq$ follows from linear algebra, or from the fact that $H^2(R, \mathbf{G}_m) = 0$. To show equality, take $x \in H^1(L, \tilde{G})$ such that $\langle x, y \rangle = 0$ for all $y \in H^1(R, \tilde{G})$ and such that $x^\sigma = x$ for all $\sigma \in H$. For any $z \in H^1(S, \tilde{G})$ we have

$$\langle x, \sum_\sigma z^\sigma \rangle = 0$$

because $\sum_\sigma z^\sigma$ is H-invariant, thus in $H^1(R, \tilde{G})$. But

$$\begin{aligned} \langle x, \sum_\sigma z^\sigma \rangle &= \sum_\sigma \langle x, z^\sigma \rangle \\ &= \sum_\sigma \langle x, z \rangle \\ &= |H| \langle x, z \rangle \end{aligned}$$

Thus, $\langle x, z \rangle = 0$ because the order of H is prime to p. Therefore, $x \in H^1(S, \tilde{G})^\perp = H^1(S, G)$ by Corollary 5.2. Finally, $x \in H^1(S, G) \cap H^1(K, G) = H^1(R, G)$ and the proof is complete. $\square$

§ Extensions of $\mathbf{Z}/p\mathbf{Z}$ by μ_p

9. Extensions. Fix a field K of characteristic p. We want to consider extensions of $\mathbf{Z}/p\mathbf{Z}$ by μ_p in the category of finite flat group schemes over K, in other words diagrams

$$0 \to \mu_p \to G \to \mathbf{Z}/p\mathbf{Z} \to 0 \tag{9.1}$$

of group schemes over K. Let $Ext^1_K(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ be the group of isomorphism classes of such objects.

Lemma 9.2. *If K is a field of characteristic p, there is a canonical isomorphism*

$$Ext^1_K(\mathbf{Z}/p\mathbf{Z}, \mu_p) \cong H^1(K, \mu_p) \cong K^\times/K^{\times p}.$$

Proof. The exact sequence of constant group schemes

$$0 \to \mathbf{Z} \xrightarrow{p} \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z} \to 0$$

induces an exact sequence of Exts:

$$\to Ext^0_K(\mathbf{Z}, \mu_p) \to Ext^1_K(\mathbf{Z}/p\mathbf{Z}, \mu_p) \to Ext^1_K(\mathbf{Z}, \mu_p) \xrightarrow{p} Ext^1_K(\mathbf{Z}, \mu_p).$$

But for any group scheme G over K, $Ext^i_K(\mathbf{Z}, G) = H^i(K, G)$. Since $H^0(K, \mu_p) = 0$ and $H^1(K, \mu_p)$ is killed by p, we have

$$Ext^1_K(\mathbf{Z}/p\mathbf{Z}, \mu_p) \cong H^1(K, \mu_p)$$

which completes the proof. □

It is clear from the definitions that the class of the extension (9.1) in $H^1(K, \mu_p)$ is exactly the image of $1 \in \mathbf{Z}/p\mathbf{Z}$ under the coboundary map

$$H^0(K, \mathbf{Z}/p\mathbf{Z}) \to H^1(K, \mu_p)$$

induced by (9.1). In other words, the image is the μ_p-torsor which is the inverse image of 1 in (9.1).

10. Cohomology. Let K be a local field of characteristic p with finite residue field: $K \cong \mathbf{F}_q((t))$. We want to analyze part of the long exact cohomology sequence associated to the extension (9.1). Let $a \in K^\times$ represent the class of (9.1) in $H^1(K, \mu_p) \cong K^\times/K^{\times p}$. Thus a is the image of 1 under δ_0 in

$$H^0(K, \mathbf{Z}/p\mathbf{Z}) \xrightarrow{\delta_0} H^1(K, \mu_p) \to H^1(K, G) \to H^1(K, \mathbf{Z}/p\mathbf{Z}) \xrightarrow{\delta_1} H^2(K, \mu_p).$$

It follows from the formalism of the Yoneda pairing (cf. Altman-Kleiman [1, IV.1]) that the map δ_1 is just the cup product

$$H^1(K, \mathbf{Z}/p\mathbf{Z}) \times Ext^1_K(\mathbf{Z}/p\mathbf{Z}, \mu_p) \to H^2(K, \mu_p)$$

defined by the class of a. This, however, is nothing but the Artin-Schreier pairing:

$$\delta_1(b) = [b, a) \in H^2(K, \mu_p) \cong H^2(K, \mathbf{G}_m)_p$$

for $b \in H^1(K, \mathbf{Z}/p\mathbf{Z}) \cong K/\wp(K)$. Thus we have an exact sequence

$$0 \to K^\times/a^{\mathbf{Z}}K^{\times p} \to H^1(K, G) \xrightarrow{\phi} \{b \in H^1(K, \mathbf{Z}/p\mathbf{Z}) | [b, a) = 0\} \to 0.$$

Since $H^1(K, \mathbf{Z}/p\mathbf{Z})$ is the set of $\mathbf{Z}/p\mathbf{Z}$-torsors over K, an element b of this group is just a Galois extension L of K together with a generator σ of $Gal(L/K) = \mathbf{Z}/p\mathbf{Z}$. Fix b in the image of ϕ and let (L, σ) be the corresponding data.

Lemma 10.1. *The fiber $\phi^{-1}(b)$ is the quotient of*

$$\left\{x \in L^\times/L^{\times p} | \sigma(x) \equiv ax\right\}$$

by multiplication by powers of a. Thus $\phi^{-1}(b)$ is a non-empty principal homogeneous space for $K^\times/a^{\mathbf{Z}}K^{\times p}$ if and only if $[b, a) = 0$.

Proof. This follows from the interpretation of $H^1(K, G)$ as the set of G-torsors over K. □

It would be interesting to have an explicit expression for the cup product pairing on $H^1(K, G)$ in terms of this description.

Chapter IV
A Bound on the Rank of E

Let K be the function field $\mathbf{F}_q(X_1)$ and E the universal curve introduced in Chapter II. The purpose of this chapter is to bound from above the ranks of the Mordell-Weil groups $E(K)$ and $E(\mathbf{F}_q(j))$. We use the classical technique of a first p-descent invented by Fermat and refined by Mordell and Weil; the main local tool is the cohomology calculation of Chapter III, while globally we use class field theory and generalized Jacobians as exposed in Serre [24].

§ Preliminaries

1. The Formalism of Descent. Let L be a global field and $F : A_1 \to A_2$ an isogeny of elliptic curves defined over L. We seek to bound from above the cokernel

$$A_2(L)/F(A_1(L))$$

by cohomological techniques. The isogeny F yields an exact sequence of finite flat group schemes (and thus of sheaves for the flat topology on $Spec\ L$):

$$0 \to Ker\ F \to A_1 \xrightarrow{F} A_2 \to 0$$

part of whose long exact (flat) cohomology sequence reads

$$0 \to A_2(L)/F(A_1(L)) \xrightarrow{\lambda_F} H^1(L, Ker\ F) \to H^1(L, A_1)_F \to 0$$

(where we have used a subscript to denote the kernel of a map). In general the group $H^1(L, Ker\ F)$ is infinite so we need to do more: for each place v of L, let L_v be the completion. We have similar exact sequences for each L_v:

$$0 \to A_2(L_v)/F(A_1(L_v)) \xrightarrow{\lambda_{v,F}} H^1(L_v, Ker\ F) \to H^1(L_v, A_1)_F \to 0;$$

let the *local Selmer group of F at v*, $Sel_v(L,F)$, be the image of $\lambda_{v,F}$. There is also a commutative diagram induced by the restriction maps $H^i(L,\cdot) \to H^i(L_v,\cdot)$

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_2(L)/F(A_1(L)) & \xrightarrow{\lambda_F} & H^1(L, Ker\ F) & \longrightarrow & H^1(L,A_1)_F & \longrightarrow & 0 \\ & & \downarrow & & \downarrow r_v & & \downarrow s_v & & \\ 0 & \longrightarrow & A_2(L_v)/F(A_1(L_v)) & \xrightarrow{\lambda_{v,F}} & H^1(L_v, Ker\ F) & \longrightarrow & H^1(L_v,A_1)_F & \longrightarrow & 0 \end{array}$$

Define the *Selmer group for F over L*, $Sel(L,F) \subseteq H^1(L, Ker\ F)$, to be the set

$$\{x \in H^1(L, Ker\ F) |\ r_v(x) \in Sel_v(L,F) \text{ for all } v\}.$$

Clearly, $Sel(L,F)$ contains the image of λ_F; this group will turn out to be finite and give an upper bound. As a measure of the failure of this bound, let $Ш(L,A_1) = Ker\ (H^1(L,A_1) \to \prod_v H^1(L_v,A_1))$. Then $Ш(L,A_1)_F = Ker\ \prod_v s_v$, and we have an exact sequence

$$0 \to A_2(L)/F(A_1(L)) \to Sel(L,F) \to Ш(L,A_1)_F \to 0.$$

We are going to apply these ideas to the Frobenius isogeny $F : E \to E^{(p)}$ of the universal curve E and its dual $V : E^{(p)} \to E$. We work over the field $K = \mathbf{F}_q(X_1)$, where the group schemes $Ker\ F$ and $Ker\ V$ are very simple and then use the Galois group $G = Gal(K/\mathbf{F}_q(j))$ to get results over $\mathbf{F}_q(j)$.

2. Some Lemmas. We collect here some technical results that will be needed in the sequel. Let L be a field of characteristic p and A an elliptic curve over L. The kernel of the relative Frobenius morphism

$$F : A \to A^{(p)}$$

is a finite flat group scheme of order p over L, thus can be described in terms of the Oort-Tate group schemes $G_{a,b}$ (cf. Chapter III). Let $H \in L$ be the Hasse invariant of A with respect to some differential ω defined over L.

Proposition 2.1. *As group schemes over L,*

$$Ker\ F \cong G_{0,H}.$$

Note that this makes sense independently of the differential ω: changing ω changes H by multiplication by an element of $L^{\times(p-1)}$ which does not change the isomorphism class of $G_{0,H}$ over L.

Proof. The group scheme $Ker\ F$ has the property that, for every point $P \in Ker\ F$ and any x in the local ring $\mathcal{O}_{Ker\ F,P}$ at P, $x^p = 0$. In other words, $Ker\ F$ is a *height one group scheme*. Such group schemes are completely classified by their p-Lie algebras (Mumford, [17, Theorem, §14]) and the p-Lie algebra of $Ker\ F$ is isomorphic to that of E (Mumford, [17, §11]). Since $Ker\ F$ is commutative and one-dimensional, its p-Lie algebra is completely determined by its p-power map. According to Mumford [17, Theorem 3, §15] this map is identified with the Frobenius acting on $H^1(A, \mathcal{O}_A)$ (using the fact that elliptic curves are self dual). But this is exactly the definition of the Hasse invariant: choosing a basis η of the one dimensional L vector space $H^1(A, \mathcal{O}_A)$, one defines H by $F^*(\eta) = H\eta$. Now let $\mathbf{g}$ be the p-Lie algebra defined by the one dimensional vector space $L \cdot v$ with trivial bracket and with p-power map $v \mapsto v^{(p)} = Hv$. Then Mumford shows by construction ([17, §14, Proof of Theorem]) that the unique height one group scheme with p-Lie algebra $\mathbf{g}$ is $G_{0,H}$. Thus $Ker\ F \cong G_{0,H}$ as was to be proved. □

In fact, the same proof shows that the theorem holds over a more general base scheme, for example over the ring of integers in L when L is a local field.

Since the Verschiebung $V : E^{(p)} \to E$ is the dual isogeny of F, $Ker\ V$ is the Cartier dual of $Ker\ F$ (Mumford, [17, §15, Thm. 1]). Recalling that as group schemes $\mathbf{Z}/p\mathbf{Z} \cong G_{1,0}$, we have a result first announced as Proposition 3.2 of Chapter II.

Corollary 2.2. *Let A be an elliptic curve over a scheme S of characteristic p. The kernel of $V : A^{(p)} \to A$ is isomorphic to $\mathbf{Z}/p\mathbf{Z}$ as a group scheme over S if and only if the Hasse invariant of A is a $(p-1)^{st}$ power in $H^0(S, \mathcal{O}_S)$.*

We will need some results about Galois invariants. Let $L = \mathbf{F}_q((t))$, and let L'/L be a Galois extension with Galois group H of order prime to p. Consider an isogeny $F : A_1 \to A_2$ of degree p

between two elliptic curves defined over L. Then we have a commutative diagram:

$$\begin{array}{ccc} A_2(L')/F(A_1(L')) & \xrightarrow{\lambda'} & H^1(L', Ker\ F) \\ \uparrow & & \uparrow \\ A_2(L)/F(A_1(L)) & \xrightarrow{\lambda} & H^1(L, Ker\ F). \end{array}$$

H acts on the the groups in the top row and the map λ' is H-equivariant.

Proposition 2.4. *The restriction map*

$$H^1(L, Ker\ F) \to H^1(L', Ker\ F)$$

induces an isomorphism

$$Image\ \lambda \cong [Image\ \lambda']^H.$$

Proof. Since $Ker\ F$ is a group scheme of order p and the order of H is prime to p, the Hochschild-Serre spectral sequence shows that the restriction map induces an isomorphism

$$H^1(L, Ker\ F) \xrightarrow{\sim} H^1(L', Ker\ F)^H.$$

Because λ and λ' are injections, the proposition is implied by the following.

Lemma 2.5. *The natural map*

$$A_2(L) = A_2(L')^H \to [A_2(L')/F(A_1(L'))]^H$$

is surjective.

Proof. We have an exact sequence of H-modules

$$0 \to F(A_1(L')) \to A_2(L') \to A_2(L')/F(A_1(L')) \to 0;$$

forming the associated long exact sequence of Galois cohomology groups, the assertion of the lemma is equivalent to the claim that

$$H^0(H, A_2(L')/F(A_1(L'))) \to H^1(H, F(A_1(L')))$$

is the zero map. But $A_2(L')/F(A_1(L'))$ is a p-group (since, e.g., it imbeds in $H^1(L', Ker\ F)$) thus so is $H^0(H, A_2(L')/F(A_1(L')))$. On the other hand, the group $H^1(H, F(A_1(L')))$ is annihilated by

the order of H, which is prime to p (Serre [25], Chap. VIII, Cor. 1 to Prop. 4). Thus the map is zero and the lemma, as well as the proposition, is proved. $\square$

Now let L'/L be a Galois extension of global function fields of characteristic p with $H = Gal(L'/L)$ of order prime to p. If $F : A_1 \to A_2$ is a p-isogeny of elliptic curves over L, we have:

Proposition 2.6. *The restriction map*

$$H^1(L, Ker\ F) \to H^1(L', Ker\ F)$$

induces an isomorphism

$$Sel(L, F) \cong Sel(L', F)^H.$$

Proof. Again we have an isomorphism

$$H^1(L, Ker\ F) \cong H^1(L', Ker\ F)^H$$

and we will identify $H^1(L, Ker\ F)$ with its image. Then

$$Sel(L', F)^H = Sel(L', F) \cap H^1(L, Ker\ F).$$

Clearly, $Sel(L, F) \subset Sel(L', F)^H$; we must show equality. Let $x \in Sel(L', F)^H$; because x is invariant, it lies in $H^1(L, Ker\ F)$ and it remains to show that x satisfies the local conditions, i.e. that $r_v(x) \in H^1(L_v, Ker\ F)$ actually lies in $Sel_v(L, F)$ (in the notation of No. 1) for all places v of L. But since $x \in Sel(L', F)$ we have

$$r_w(x) \in Sel_w(L', F) \subseteq H^1(L'_w, Ker\ F)$$

for all places w of L'. If H_w is the decomposition group at w, so $H_w = Gal(L'_w/L_v)$ for $w|v$, then since x is H-invariant, $r_w(x)$ is H_w-invariant. Then Proposition 2.6 shows that $r_w(x)$ actually lies in $Sel_v(L, F) = Sel_w(L', F)^{H_w}$. Thus the local conditions are satisfied and the proof is complete. $\square$

§ The Local Descent

3. Statement. Let K be the function field $\mathbf{F}_q(X_1)$ and let E be the universal elliptic curve of Chapter II. Let $F : E \to E^{(p)}$ be the Frobenius isogeny and $V : E^{(p)} \to E$ its dual the Verschiebung. Recall that over K we have isomorphisms of group schemes:

$$Ker\ V \cong \mathbf{Z}/p\mathbf{Z}$$

$$Ker\ F \cong \mu_p.$$

For each place v of K let K_v be the completion of K at v. We saw in III.4 that there are canonical isomorphisms

$$H^1(K_v, \mathbf{Z}/p\mathbf{Z}) \cong K_v/\wp(K_v)$$

and

$$H^1(K_v, \mu_p) \cong K_v^\times/K_v^{\times p}.$$

The latter groups have filtrations

$$P^{[i]} \subseteq K_v/\wp(K_v)$$

$$U^{[j]} \subseteq K_v^\times/K_v^{\times p}$$

(where $P^{[i]}$ is the image of $\{x \in K_v | ord(x) \geq -i\}$ in $K_v/\wp(K_v)$ and $U^{[j]}$ is the image of $\{x \in K_v^\times | ord(1-x) \geq j\}$ in $K_v^\times/K_v^{\times p}$.) We want to describe the images of the coboundary maps

$$E(K_v)/V(E^{(p)}(K_v)) \xrightarrow{\lambda_{v,V}} H^1(K_v, Ker\ V) \cong K_v/\wp(K_v)$$

$$E^{(p)}(K_v)/F(E(K_v)) \xrightarrow{\lambda_{v,F}} H^1(K_v, \mu_p) \cong K_v^\times/K_v^{\times p}$$

in terms of these filtrations.

Proposition 3.1. *Let S be the set of supersingular places of K not lying over 0 or 1728. The images of the coboundary maps $\lambda_{v,V}$ and $\lambda_{v,F}$ are given by the following table:*

Place v of K	*Image of $\lambda_{v,V}$*	*Image of $\lambda_{v,F}$*
v ordinary	$P^{[0]}$	$U^{[0]}$
$v \in S$	$P^{[(p-1)/2]}$	$U^{[(p+1)/2]}$
$v = 1728$	$P^{[(p-3)/4]}$	$U^{[(p+1)/4]}$
$v = 0$	$P^{[(p-5)/6]}$	$U^{[(p+1)/6]}$
v over ∞	0	$K^\times/K^{\times p}$

(When 0 is not supersingular the $(p-1)/6$ places of K over $j=0$ fall into the first category. Similarly, if 1728 is not supersingular the $(p-1)/4$ places of K over $j=1728$ are in the first category.) We will prove this result in the next No.

4. Computation of the Local Images. We begin with a general result. Let L be a complete local ring of characteristic p with finite residue field and let S be its ring of integers. If $F: A \to A'$ is an isogeny of degree p of elliptic curves defined over L, then $Ker\ F$ is a finite flat group scheme of order p over L and we have a coboundary map $\lambda: A'(L) \to H^1(L, Ker\ F)$. The following is the basic result on local images.

Lemma 4.1. *If A (and thus A') has good reduction over S (so F extends to an isogeny of abelian schemes over Spec S) then the image of λ is equal to the image of the restriction map*

$$H^1(S, Ker\ F) \to H^1(L, Ker\ F).$$

Proof. We choose models of A and A' with good reduction over S (these are automatically the Néron models) and denote these again by A and A'. We then have a commutative diagram induced by the restriction maps:

$$\begin{array}{ccccc} A'(L) & \xrightarrow{\lambda} & H^1(L, Ker\ F) & \longrightarrow & H^1(L, A) \\ \uparrow & & \uparrow r & & \uparrow \\ A'(S) & \longrightarrow & H^1(S, Ker\ F) & \longrightarrow & H^1(S, A). \end{array}$$

By the characteristic property of Néron models, $A'(L) = A'(S)$. On the other hand, $H^1(S, A) = 0$ (using the interpretation of H^1s as principal homogeneous spaces, the fact that every curve of genus 1 over a finite field has a rational point, and Hensel's lemma). Thus, the image of λ is equal to the image of r and the lemma is proved. □

We return to the situation $K = \mathbf{F}_q(X_1)$ and E is the universal elliptic curve over K of Chapter II. Let v be a place of K, K_v the completion, and R_v its ring of integers.

Proposition 4.2. *If v is an ordinary place of K (i.e. not a supersingular place or a cusp) then the maps $\lambda_{v,V}$ and $\lambda_{v,F}$ have images:*

$$Image\ \lambda_{v,V} = P^{[0]} = R_v/\wp(R_v)$$

and

$$Image\ \lambda_{v,F} = U^{[0]} = R_v^\times / R_v^{\times p}.$$

Proof. The models II.8.1 of the curves E and $E^{(p)}$ have good reduction at these places so the lemma applies. As group schemes over R_v, $Ker\ V \cong G_{A,0}$ and $Ker\ F \cong G_{0,A}$ where A is the Hasse invariant of E (by Proposition 2.1). But the explicit expression II.10.1 shows that $ord_v(A) = 0$ and the cohomology calculation Theorem III.4.1 finishes the proof. □

Proposition 4.3. *Let v be a supersingular place of K not lying over 0 or 1728. Then the images of the coboundary maps are*

$$Image\ \lambda_{v,V} = P^{[(p-1)/2]}$$

and

$$Image\ \lambda_{v,F} = U^{[(p+1)/2]}$$

Proof. The curves E and $E^{(p)}$ have reduction type I_0^* over K_v (Table II.9.4), so there exists a totally ramified quadratic extension L/K_v over which they obtain good reduction. Let w be a normalized valuation in L. A trivial calculation shows that for a model of E with good reduction over the ring of integers of L, we have $ord_w(A(E)) = p - 1$. Thus applying the lemma and Theorem III.4.1, we see that the images of

$$E(L) \to H^1(L, \mathbf{Z}/p\mathbf{Z})$$

and

$$E^{(p)}(L) \to H^1(L, \mu_p)$$

are equal to $P_L^{[p]} = P_L^{[p-1]}$ and $U_L^{[p]} = U_L^{[p+1]}$. If $H = Gal(L/K_v)$, applying Proposition 2.4 we have:

$$Image\ \lambda_{v,V} = {P_L^{[p-1]}}^H = P_{K_v}^{[(p-1)/2]}$$

and

$$Image\ \lambda_{v,F} = {U_L^{[p+1]}}^H = U_{K_v}^{[(p+1)/2]}$$

□

Similar arguments apply at the other supersingular places and we have the following.

Proposition 4.4. *If v is a supersingular place of K lying over $j = 0$ then Image $\lambda_{v,V} = P^{[(p-5)/6]}$ and Image $\lambda_{v,F} = U^{[(p+1)/6]}$. If v is supersingular and lies over $j = 1728$ then Image $\lambda_{v,V} = P^{[(p-3)/4]}$ and Image $\lambda_{v,F} = U^{[(p+1)/4]}$.*

(If 0 or 1728 is not supersingular then E has good reduction and $ord_v(A) = 0$, so these v are handled by the arguments of Proposition 4.2.)

It remains to check what happens over the cusps. Here E and $E^{(p)}$ have split multiplicative reduction (Table II.9.4), so we have analytic parameterizations

$$E(K_v) \cong K_v^\times / q^{\mathbf{Z}}$$

and

$$E^{(p)}(K_v) \cong K_v^\times / q^{p\mathbf{Z}}$$

for some $q \in K_v^\times$ with $ord_v(q) = ord_v(\Delta) = 1$. The Frobenius $F : E \to E^{(p)}$ is induced by $K_v^\times \to K_v^\times$ $x \mapsto x^p$ and the Verschiebung is induced by the identity $K_v^\times \to K_v^\times$ $x \mapsto x$. Thus,

$$E^{(p)}(K_v)/F(E(K_v)) \cong K_v^\times / K_v^{\times p}$$

and

$$E(K_v)/V(E^{(p)}(K_v)) = \{0\}.$$

Proposition 4.5. *For v a cusp of K, the image of $\lambda_{v,V}$ is trivial and the image of $\lambda_{v,F}$ is isomorphic to $K_v^\times / K_v^{\times p}$.*

This completes the verification of the claims made in Proposition 4.2.

§ The Global Descent

5. The multiplicative descent. Our goal is to find the subgroup $Sel(K, F)$ of $H^1(K, \mu_p)$ consisting of those elements whose images under the restriction maps $H^1(K, \mu_p) \to H^1(K_v, \mu_p)$ lie in the image of $\lambda_{v,F}$ for all v. Let $f \in K^\times$ be a non-zero function on X_1. We can form the global differential 1-form $\frac{df}{f}$ on X_1 (calculating df formally); it has at worst simple poles and the residue

at a point of X_1 is equal to the valuation of f at that point. In the classical terminology, $\frac{df}{f}$ is a *differential of the third kind*. Furthermore, $\frac{df}{f}$ is zero if and only if f is a p^{th} power, i.e. if $f \in K^{\times p}$. Thus we have an injection

$$K^\times/K^{\times p} \to \{\text{differentials of the third kind}\}$$

$$f \mapsto \frac{df}{f}.$$

Now let $\overline{f} \in K^\times/K^{\times p}$ be represented by $f \in K^\times$, and assume that $\overline{f} \in Sel(K,F)$. If v is a cusp of X_1, this imposes no condition on f, thus $\frac{df}{f}$ may have a simple pole with residue in the prime field. If v is an ordinary place of K, then $f \in U^{[0]}$, i.e. $f = g^p u$ in K_v where u is a unit in the ring of integers of K_v. Thus $\frac{df}{f}$ is regular at v. If $v \in S$, i.e. v is a supersingular place of K not lying over 0 or 1728, then $f \in U^{[(p+1)/2]}$, i.e. $f = g^p u$ in K_v where $ord_v(1-u) \geq (p+1)/2$. A local computation then shows that $\frac{df}{f}$ has a zero of order at least $(p-1)/2$ at v. Similarly, if 1728 or 0 is supersingular then $\frac{df}{f}$ has a zero of order at least $(p-3)/4$ or $(p-5)/6$. Thus,

$$\begin{aligned} div(\frac{df}{f}) \geq D = &- \sum_{cuspidal\ v} [v] \\ &+ \frac{p-1}{2} \sum_{v \in S} [v] \\ &+ \left(\frac{p-3}{4} [1728] \text{ if } p \equiv 3 \pmod 4 \right) \\ &+ \left(\frac{p-5}{6} [0] \text{ if } p \equiv 2 \pmod 3 \right). \end{aligned} \tag{5.1}$$

But comparing with the expression II.5.1 for the genus of X_1, we find $deg(D) = 2g_{X_1} - 2$! Thus if $\overline{f} \in Sel(K,F)$ then either $f \in K^{\times p}$ and $\frac{df}{f} = 0$, or $div(\frac{df}{f}) = D$. But the set of differentials with divisor D is (at most) a one-dimensional $\mathbf{F}_q$-vector space and the set of those whose residues lie in the prime field is at most a one-dimensional $\mathbf{F}_p$-vector space. In fact, Serre's theory of reduction modulo p of modular forms [26] shows that such differentials actually do exist: in terms of the isomorphism $K \cong \mathbf{F}_q(Q,R)/(A(Q,R)-1)$ of II.6.1, a differential with divisor D is given by

$$\omega = \frac{3RdQ - 2QdR}{Q^3 - R^2}.$$

(This is the reduction mod p of the Eisenstein series E_{p-1}.) Thus we have proved the following.

Proposition 5.2. *The order of $Sel(K, F)$ is p.*

Now since $G = Gal(K/\mathbf{F}_q(j))$ acts on $Ker\ V$ by $\chi = \omega^{(p-3)/2}$ (Proposition II.9.7), it must act on the Cartier dual, $Ker\ F$, by $\chi^{-1} = \omega^{(p+1)/2}$. Thus

$$H^1(K, Ker\ F)^G = (K^\times/K^{\times p})^\chi$$

(where we use a χ superscript to indicate the χ-eigencomponent of this $\mathbf{F}_p$-vector space). Now the map $f \mapsto \frac{df}{f}$ is obviously G-equivariant, so we can compute eigencomponents on the differentials. But the explicit form of the differential ω above (together with the fact that Q is of weight 4 and R is of weight 6) makes it clear that ω is of weight $-2 \equiv p-3 \pmod{p-1}$ with respect to G, i.e. that

$$\langle a \rangle^* \omega = a^{p-3}\omega.$$

Thus ω does not lie in the χ-eigenspace and we have the following result.

Theorem 5.3. *If $p \equiv 3 \pmod 4$ and $p > 3$ then for all q, the group $Sel(\mathbf{F}_q(j), F)$ is trivial. Thus*

$$F : E(\mathbf{F}_q(j)) \to E^{(p)}(\mathbf{F}_q(j))$$

is an isomorphism for all q.

(Recall that for $p = 3$ $K = \mathbf{F}_p(j)$.)

Proposition 2.1 shows that as group schemes over K,

$$Ker\ F \cong \mu_p$$

and

$$Ker\ V \cong \mathbf{Z}/p\mathbf{Z}. \tag{5.4}$$

Fixing these isomorphisms, E_p, the kernel of p acting on E over K, is an extension of the type considered in III.9:

$$0 \to \mu_p \to E_p \to \mathbf{Z}/p\mathbf{Z} \to 0. \tag{5.5}$$

In fact, the proof of Proposition 5.2 allows us to determine the class of the extension (5.5) in $Ext^1_K(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ which according to Lemma III.9.2 is isomorphic to $K^\times/K^{\times p}$: (5.5) induces a coboundary map

$$H^0(K, \mathbf{Z}/p\mathbf{Z}) \xrightarrow{\delta} H^1(K, \mu_p).$$

But the torsion calculation II.9.6 shows that

$$H^0(K, \mathbf{Z}/p\mathbf{Z}) \cong E^{(p)}(K)/F(E(K))$$

so that the image of δ is non-zero in $Sel(K, F)$. Since the latter group has order p, we have an isomorphism

$$H^0(K, \mathbf{Z}/p\mathbf{Z}) \cong Sel(K, F)$$

and the class of the extension (5.5) is just the image of 1, i.e. of the point $P \in H^0(K, Ker\ V)$ which maps to 1 using (5.4). Note that under the map from $K^\times/K^{\times p}$ to differentials of the third kind the class of the extension (5.5) maps to the ω given above Proposition 5.2. This comment also provides another proof of Proposition 5.3, namely that the elements of $Sel(K, F)$ do not descend to $\mathbf{F}_q(j)$: Proposition 2.3 shows that the points of order p in $E^{(p)}$, i.e. $Ker\ V$, do not descend.

6. Etale Descent. Now we turn to the subgroup $Sel(K, V)$ of $H^1(K, \mathbf{Z}/p\mathbf{Z})$ consisting of those elements whose image under the restriction maps $H^1(K, \mathbf{Z}/p\mathbf{Z}) \to H^1(K_v, \mathbf{Z}/p\mathbf{Z})$ lie in the images of the $\lambda_{v,V}$. First we note that, for any field L of characteristic p, by Artin-Schreier theory $H^1(L, \mathbf{Z}/p\mathbf{Z}) \cong L/\wp(L)$ parametrizes Galois extensions of L with group $\mathbf{Z}/p\mathbf{Z}$: given $\overline{f} \in L/\wp(L)$ represented by $f \in L$ we solve $\wp(x) = f$ and let $L' = L(x)$. L' is Galois over L with $Gal(L'/L) = \mathbf{Z}/p\mathbf{Z}$, acting by translation: $a : f \mapsto f + a$. In the language of Chapter III, a Galois extension of L with group $\mathbf{Z}/p\mathbf{Z}$ is just a $\mathbf{Z}/p\mathbf{Z}$-torsor over $Spec\ L$.

Now let $\overline{f} \in Sel(V) \subseteq K/\wp(K)$ be represented by $f \in K$ and let K' be the extension deduced from f as above. The local restrictions at each v (i.e. that f lie in the image of λ_v) give a bound on the possible pole of f at v modulo $\wp(K_v)$. But this implies a bound on the local term of the conductor of the extension at v (cf. Serre [24, Chap. VI, No. 12]). More precisely, if f has a pole at v of order n with n prime to p (which we can always arrange by modifying f by an element of $\wp(K)$),

the conductor of the extension K'/K at v is $n+1$. Thus if S is the set of supersingular places of K not lying over 0 or 1728, then the conductor of the extension K'/K is bounded by

$$\begin{aligned}\mathbf{m} = \sum_v \mathbf{m}_v[v] = \frac{p+1}{2}\sum_{v\in S}[v] \\ + \left(\frac{p+1}{4}[1728] \quad \text{if } p \equiv 3 \pmod 4\right) \\ + \left(\frac{p+1}{6}[0] \quad \text{if } p \equiv 2 \pmod 3\right).\end{aligned}$$

Furthermore, the condition that $f \in \wp(K_v)$ for the cusps, i.e. for those v lying over $j = \infty$, implies that the extension K'/K is completely split at these places.

Choose a cusp c of X_1. Since c is rational over $\mathbf{F}_q$, class field theory identifies the Galois group of the maximal abelian extension of K whose conductor is bounded by $\mathbf{m}$ and which is split at c with $J_{\mathbf{m}}(\mathbf{F}_q)$, the $\mathbf{F}_q$-valued points of the generalized Jacobian of X_1 for the modulus $\mathbf{m}$. Thus $\mathbf{Z}/p\mathbf{Z}$-extensions of K with conductor bounded by $\mathbf{m}$ are parameterized by

$$Hom(J_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z})$$

(homomorphisms as Abelian groups, not as algebraic groups). That K' be completly split at all the cusps is equivalent to the condition that the homomorphism to $\mathbf{Z}/p\mathbf{Z}$ vanish on the group of divisor classes generated by the cusps. Let $\langle cusps\rangle$ denote this subgroup. All this is summarized by the following statement.

Proposition 6.1.

$$\begin{aligned}Sel(K,V) &= \{x \in Hom(J_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z}) | x(\langle cusps\rangle) = 0\} \\ &\cong Hom(J_{\mathbf{m}}(\mathbf{F}_q)/\langle cusps\rangle, \mathbf{Z}/p\mathbf{Z}).\end{aligned}$$

By Proposition 2.6, $Sel(\mathbf{F}_q(j), V) = Sel(K,V)^G$, so we need to explicate the action of G on this group. Recall that the action of G on $(Ker\ V)(K) \cong \mathbf{Z}/p\mathbf{Z}$ was given by the character $\chi = \omega^{(p-3)/2}$. Thus the action of G on $H^1(K, Ker\ V) \cong K/\wp(K)$ is the usual action of G on $K/\wp(K)$ twisted by χ:

$$\overline{x}^\sigma = \chi(\sigma)\overline{\sigma(x)} \qquad \overline{x} \in K/\wp(K),\ \sigma \in G,$$

and $H^1(K, Ker\ V)^G \cong K/\wp(K)^{\chi^{-1}}$ where we use a superscript to indicate an eigencomponent. Therefore,

$$Sel(\mathbf{F}_q(j), V) \cong Hom(J_{\mathbf{m}}(\mathbf{F}_q)/\langle cusps\rangle, \mathbf{Z}/p\mathbf{Z})^{\chi^{-1}}.$$

Finally, if $\phi \in Hom(J_{\mathbf{m}}(\mathbf{F}_q)/\langle cusps\rangle, \mathbf{Z}/p\mathbf{Z})$ and $\sigma \in G$, then $(\sigma\phi)(x) = \phi(\sigma^{-1*}(x))$ where σ^{-1*} : $J_{\mathbf{m}} \to J_{\mathbf{m}}$ is the map induced on Jacobians by the map $\sigma^{-1} : X_1 \to X_1$.

7. Analysis of $J_{\mathbf{m}}$. We analyze $Hom(J_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z})$, ignoring for the moment the cusp condition. Recall that $J_{\mathbf{m}}$ is an extension of algebraic groups

$$0 \to L_{\mathbf{m}} \to J_{\mathbf{m}} \to J \to 0 \tag{7.1}$$

where J is the ususal Jacobian of X_1 and $L_{\mathbf{m}}$ is the group

$$\frac{\{div(f) | f \in K^\times\}}{\{div(f) | f \in K^\times,\ f \equiv 1 \pmod{\mathbf{m}}\}}.$$

Since $L_{\mathbf{m}}$ is linear (or even connected as we are over a finite field), one has

$$0 \to L_{\mathbf{m}}(F) \to J_{\mathbf{m}}(F) \to J(F) \to 0$$

for all finite fields F containing $\mathbf{F}_q$.

The group $L_{\mathbf{m}}$ can be written as a product of local groups

$$L_m \cong \left(\prod_{v \in\ Support(\mathbf{m})} \mathbf{G}_m \times U_v^{(1)}/U_v^{(\mathbf{m}_v)} \right) \Big/ \mathbf{G}_m$$

where $U_v^{(i)} = \{f \in K^\times | ord_v(1-f) \geq i\}$ and where the $\mathbf{G}_m$ in the denominator imbeds diagonally into the product. Now for the $\mathbf{m}$ under consideration, $m_v < p$ for all v, so according to Serre [24, Chap. V, Prop. 9] we have

$$U_v^{(1)}/U_v^{(\mathbf{m}_v)} \cong {\mathbf{G}_a}^{\mathbf{m}_v - 1}$$

via

$$(a_1, \ldots, a_{\mathbf{m}_v - 1}) \mapsto \prod_{i=1}^{\mathbf{m}_v - 1} E(a_i t_v^i)$$

where E is the Artin-Hasse exponential and t_v is a uniformizer at V. If we choose t_v to be a uniformizer which is an eigenfunction for G, Proposition II.7.2 gives the action of G and the expression above makes it trivial to compute eigencomponents. Let χ be the character giving the action of G on $Ker\ V$ i.e. $\chi = \omega^{(p-3)/2}$.

Proposition 7.2. *$L_{\mathbf{m}}(\mathbf{F}_q)\otimes\mathbf{Z}_p \cong {\mathbf{F}_q}^{\sum(\mathbf{m}_v-1)}$. When $p\equiv 3 \pmod 4$,*

$$(L_{\mathbf{m}}(\mathbf{F}_q)\otimes\mathbf{Z}_p)^{\chi} \cong {\mathbf{F}_q}^{a}$$

where

$$a = \#\{\textit{supersingular j-invariants in characteristic } p\}$$
$$-(1 \textit{ if } p\equiv 3 \pmod 8).$$

Proof. The first assertion is obvious. When $p\equiv 3 \pmod 4$ and v is a supersingular place not lying over 0 or 1728, then $\mathbf{m}_v = (p+1)/2$ and G acts on t_v by ω^{-2} so

$$\mathbf{F}_q \cong \left(U_v^{(1)}/U_v^{(\mathbf{m}_v)}\right)^{\chi}$$
$$a \mapsto E(at_v^{(p+1)/4}).$$

If v lying over 0 is a supersingular place, then $\mathbf{m}_v = (p+1)/6$ and G acts on t_v by ω^{-6} so

$$\mathbf{F}_q \cong \left(U_v^{(1)}/U_v^{(\mathbf{m}_v)}\right)^{\chi}$$
$$a \mapsto E(at_v^{(p+1)/12}).$$

(Note that when $p\equiv 3 \pmod 4$, 0 is supersingular if and only if $p\equiv 11 \pmod{12}$.) If v lies over 1728, then $\mathbf{m}_v = (p+1)/4$ and G acts on t_v by ω^{-4}. But $(p+1)/8$ is integral if and only if $p\equiv 7 \pmod 8$ in which case

$$\mathbf{F}_q \cong \left(U_v^{(1)}/U_v^{(\mathbf{m}_v)}\right)^{\chi}$$
$$a \mapsto E(at_v^{(p+1)/8}).$$

If $p\equiv 3 \pmod 8$, no power of t_v less than $\mathbf{m}_v - 1 = (p-3)/4$ is acted on by G by the character χ, so $\left(U_v^{(1)}/U_v^{(\mathbf{m}_v)}\right)^{\chi}$ is trivial. This completes the proof of the second assertion. □

The Jacobian J is a little less tractable; one knows (Mazur-Wiles, [12, Prop. 6 and Prop. 10]) that, if $h = h(-p)$ denotes the class number of positive definite quadratic forms of discriminant $-p$, then the χ eigencomponent of the p-torsion of $J(\mathbf{F}_p)$ contains a subgroup isomorphic to

$(\mathbf{Z}/p\mathbf{Z})^{(h-1)/2}$. More knowledge about J would clearly be useful, but we can at least calculate the order of $Hom(J_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z})$ without it (cf. Proposition 7.7).

Now we turn to the nature of the extension (7.1). The following proposition says that, at least on p-primary components, this extension is as non-trivial as possible.

Proposition 7.3. *The image of the p torsion of $J_{\mathbf{m}}$, $\{x \in J_{\mathbf{m}} | px = 0\}$, in J is trivial.*

Proof. Let $x \in J_{\mathbf{m}}$ such that $px = 0$ is represented by a divisor D on X_1. Then $pD = div(f)$ for some $f \in K^\times$ with $f \equiv 1 \pmod{\mathbf{m}}$. Since the divisor of f is everywhere divisible by p, $\frac{df}{f}$ is a regular differential. But a local calculation shows that

$$\begin{aligned} div(\frac{df}{f}) \geq & \frac{p-1}{2} \sum_{v \in S} [v] \\ & + \left(\frac{p-3}{4} [1728] \text{ if } p \equiv 3 \pmod 4 \right) \\ & + \left(\frac{p-5}{6} [0] \text{ if } p \equiv 2 \pmod 3 \right). \end{aligned}$$

Comparing with II.5.1, we see that the degree of the right hand side is strictly greater than $2g_{X_1} - 2$. Thus $\frac{df}{f} = 0$ which implies that $f = g^p$ for some g. Then $D = div(g)$ and so x is trivial in J. $\square$

As $Hom(J_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z}) \cong Hom(J_{\mathbf{m}}(\mathbf{F}_q)/pJ_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z})$, we consider the standard exact sequence

$$\begin{aligned} (7.4) \quad 0 \to L_{\mathbf{m}}(\mathbf{F}_q)_p \to J_{\mathbf{m}}(\mathbf{F}_q)_p \to J(\mathbf{F}_q)_p \to \\ L_{\mathbf{m}}(\mathbf{F}_q)/pL_{\mathbf{m}}(\mathbf{F}_q) \to J_{\mathbf{m}}(\mathbf{F}_q)/pJ_{\mathbf{m}}(\mathbf{F}_q) \to J(\mathbf{F}_q)/pJ(\mathbf{F}_q) \to 0. \end{aligned}$$

Note that this is an exact sequence of $\mathbf{F}_p$-vector spaces and that the map

$$J(\mathbf{F}_q)_p \to L_{\mathbf{m}}(\mathbf{F}_q)/pL_{\mathbf{m}}(\mathbf{F}_q)$$

sends D to the principal divisor pD. Using the proposition, we have

$$\begin{aligned} (7.5) \quad 0 \to Hom(J(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z}) \to Hom(J_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z}) \to \\ Hom(L_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z}) \to Hom(J(\mathbf{F}_q)_p, \mathbf{Z}/p\mathbf{Z}) \to 0. \end{aligned}$$

(this is exact because (7.3) is an exact sequence of vector spaces). Since the order of G is prime to p, we also have an exact sequence of eigencomponents

$$(7.6)\quad 0 \to Hom(J(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z})^{\chi^{-1}} \to Hom(J_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z})^{\chi^{-1}} \to$$
$$Hom(L_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z})^{\chi^{-1}} \to Hom(J(\mathbf{F}_q)_p, \mathbf{Z}/p\mathbf{Z})^{\chi^{-1}} \to 0.$$

In English, we have that $Hom(J_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z})$ contains $Hom(J(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z})$ as a subgroup and the quotient is isomorphic, via the restriction

$$Hom(J_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z}) \to Hom(L_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z})$$

to those homomorphisms which vanish on principal divisors of the form pD. A similar statement holds for the χ^{-1}-eigencomponents.

Proposition 7.7. *The order of* $Hom(J_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z})$ *is* $q^{\sum(\mathbf{m}_v - 1)}$.

The order of $Hom(J_{\mathbf{m}}(\mathbf{F}_q), \mathbf{Z}/p\mathbf{Z})^{\chi^{-1}}$ *is* q^a *where*

$$a = \#\{\textit{supersingular j-invariants in characteristic } p\}$$
$$-\,(1 \textit{ if } p \equiv 3 \pmod 8)\,.$$

Proof. Using Proposition 7.2, the claims follow from the exact sequences 7.5 and 7.6 and the assertions that the order of $(J(\mathbf{F}_q)/pJ(\mathbf{F}_q))$ is equal to the order of $(J(\mathbf{F}_q)_p)$ and that the order of $(J(\mathbf{F}_q)/pJ(\mathbf{F}_q))^{\chi}$ is equal to the order of $(J(\mathbf{F}_q)_p)^{\chi}$. The first assertion is trivial and the second is nearly so; we give an elementary proof for the situation at hand.

Lemma 7.8. *Let a cyclic group* G *of order dividing* $p-1$ *act on a* p*-group* J*. Then* $(J/pJ)^{\chi}$ *and* $(J_p)^{\chi}$ *have the same order for all characters* χ *of* G*.*

Proof. Choose a basis of eigenvectors $\overline{x}_1, \ldots, \overline{x}_m$ of the vector space J/pJ and let a_i be the associated eigenvalues for σ a generator of G. Let $x_i \in J$ be representatives for the $\overline{x}_i$ and let p^{n_i} be their orders in J. We can assume that $n_1 \leq \cdots \leq n_m$. Then $y_i = p^{n_i - 1}x_i$ is of order p and $\{y_i\}$ forms a basis of J_p. But

$$\sigma(x_i) = a_i x_i + p(\sum_{j \neq i} b_j x_j)$$

so

$$\begin{aligned}\sigma(y_i) &= a_i y_i + p^{n_i}(\sum_{j\neq i} b_j x_j) \\ &= a_i y_i + p^{n_i}(\sum_{j>i} b_j x_j).\end{aligned}$$

Thus the matrix of σ with respect to the basis $\{y_i\}$ is lower triangular with the a_i on the diagonal and J_p and J/pJ are (non-canonically) isomorphic as G-modules. This completes the proof of the lemma and of the proposition. $\square$

Finally, to deal with the cusp condition we need to examine the image of $\langle cusps \rangle$ in the group $J_{\mathbf{m}}(\mathbf{F}_q)/pJ_{\mathbf{m}}(\mathbf{F}_q)$. Let C be the set of divisors of degree zero supported on the cusps of X_1. This is a free Abelian group on $(p-3)/2$ generators. Clearly the image of $\langle cusps \rangle$ in $J_{\mathbf{m}}(\mathbf{F}_q)/pJ_{\mathbf{m}}(\mathbf{F}_q)$ is equal to the image of C/pC in this group. Now the $\mathbf{F}_p$-vector space C/pC can be written as the direct sum of 1-dimensional eigenspaces for the action of G: choosing a cusp c_1 of X_1 all cusps can be labeled by the elements of G so that $c_\sigma = c_1^\sigma$. Fix a generator g of G and let χ be a non-trivial (${\mathbf{F}_p}^\times$-valued) character of G. Then

$$D_\chi = \sum_{\sigma \in G} \chi^{-1}(\sigma)(c_1 - c_g)^\sigma$$

is an eigenvector in C/pC for G: $D_\chi^\sigma = \chi(\sigma) D_\chi$ and the set of D_χ for non-trivial χ form a basis for C/pC.

Proposition 7.9. *The divisor D_χ is trivial in $J_{\mathbf{m}}(\mathbf{F}_q)/pJ_{\mathbf{m}}(\mathbf{F}_q)$ if and only if $\chi = \omega^{-2}$.*

Proof. The divisor D_χ is trivial in $J_{\mathbf{m}}(\mathbf{F}_q)/pJ_{\mathbf{m}}(\mathbf{F}_q)$ if and only if there exists a divisor E on X_1 such that

$$D_\chi - pE = (f)$$

where $f \equiv 1 \pmod{\mathbf{m}}$. If this holds then the differential $\frac{df}{f}$ satisfies the inequality (5.1), i.e. has poles only at the cusps and vanishes to high order at the supersingular points. We conclude as in No. 5 that either $\frac{df}{f} = 0$ and f is a p-power or that f lies in $Sel(K, F)$ and thus lies in the ω^{-2} eigenspace for G. But f cannot be a p-th power as D_χ is non-zero in C/pC. Thus if D_χ is trivial,

then it lies in the ω^{-2} eigenspace, i.e. $\chi = \omega^{-2}$ and conversely, $D_{\omega^{-2}}$ clearly satisfies a relation as above with f coming from $Sel(K,F)$. $\square$

Thus the cusp condition eliminates one homomorphism from each χ-eigenspace except when $\chi = 1$ or ω^{-2}. Combining this with Proposition 7.7, we have determined the order of $Sel(\mathbf{F}_q(j), V)$.

Theorem 7.10.

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

8. The p Descent. The problem now is to combine the preceding multiplicative and étale descents into a full p descent thus obtaining a bound on the rank of E. We do this by using the exact sequence of group schemes over K

$$0 \to Ker\ F \to Ker\ p \to Ker\ V \to 0. \tag{8.1}$$

Because $Ker\ F \cong \mu_p$ and $Ker\ V \cong \mathbf{Z}/p\mathbf{Z}$ over K, this extension is of the type considered in Chapter III.

For every completion K_v, we get

$$H^0(K_v, \mathbf{Z}/p\mathbf{Z}) \xrightarrow{\delta_0} H^1(K_v, \mu_p) \to H^1(K_v, Ker\ p) \xrightarrow{\phi} H^1(K_v, \mathbf{Z}/p\mathbf{Z}) \xrightarrow{\delta_1} H^2(K_v, \mu_p). \tag{8.2}$$

The image $a = \delta_0(1)$ is the class of the extension (8.1) in $Ext_{K_v}(\mathbf{Z}/p\mathbf{Z}, \mu_p) \cong K^\times/K^{\times p}$ (cf. III.10), which we determined in 5.3: it is a generator of $Sel(K,F)$. The map δ_1 is the cup product pairing $\delta_1(b) = [b,a)$ and the fibers of ϕ were determined in Lemma III.10.1: if $b \in H^1(K_v, \mathbf{Z}/p\mathbf{Z})$ is represented by the Galois extension L/K_v with generator $\sigma \in Gal(L/K_v)$, then

$$\phi^{-1}(b) = \{x \in L^\times/L^{\times p} | \frac{\sigma(x)}{x} \equiv a\}.$$

The sequence (8.2) induces an exact sequence of local Selmer groups

$$0 \to \mathbf{Z}/p\mathbf{Z} \to Sel_v(K,F) \to Sel_v(K,p) \xrightarrow{\tilde{\phi}} Sel_v(K,V) \to 0 \tag{8.3}$$

(the map on the right is surjective by the definition of the local Selmer groups). Fix $b = (L, \sigma)$ in $Sel_v(K, V)$. Then clearly $\tilde{\phi}^{-1}(b) \subseteq \phi^{-1}(b) \cap Sel_v(L, F)$. In fact, this is often an equality.

Lemma 8.4. *If $b = (L, \sigma)$ in $Sel_v(K, V)$ is such that L/K_v is unramified then*

$$\tilde{\phi}^{-1} = \phi^{-1}(b) \cap Sel_v(L, F).$$

We remark that this equality never holds when L/K_v is (necessarily wildly) ramified.

Proof. The inclusion $\subseteq$ is clear. On the other hand, the set on the right hand side is a principal homogeneous space for $Sel_v(K, F)/a^{\mathbf{Z}}$ when L/K_v is unramified. This follows from the local computations in No. 5 and a similar computation for L. Because (8.3) is exact, the equality follows. □

We can use the lemma to control the fibers of ϕ over elements of the global Selmer group $Sel(K, V)$ which correspond to unramified extensions.

Proposition 8.5. *Let $b = (L, \sigma) \in Sel(K, V)$ be such that L/K is everywhere unramified. Then b is not in the image of $\phi : Sel(K, p) \to Sel(K, V)$.*

Proof. This is essentially the argument of No. 5: suppose $f \in L^\times/L^{\times p}$ is in $Sel_v(L, F)$ for all v and is such that $\sigma(f)/f \equiv a$; then by Lemma 8.4 and a local calculation similar to No. 5, $\frac{df}{f}$ vanishes to order $\frac{p-1}{2}$ at the supersingular places, to order $\frac{p-3}{4}$ at 1728 if it is supersingular, and to order $\frac{p-5}{6}$ at 0 if it is supersingular. Furthermore, because $p \nmid ord_v(a)$, at a cusp v of K, the condition $\sigma(f)/f \equiv a$ implies that $\frac{df}{f}$ has a pole at $p-1$ of the places of L over v and is regular at one of them. Then either $\frac{df}{f} = 0$ or $deg(\frac{df}{f}) > 2g_L - 2$ and the latter is impossible. This implies that $f \in L^{\times p}$ which cannot be the case if $\sigma(f)/f \equiv a$ because a is not a p-power in L. This contradiction shows that no such f exists, and proves the proposition. □

Applying this yields the following bound on the rank of E.

Proposition 8.6. *Write $q = p^f$ and let $h = h(-p)$ be the class number of the quadratic field*

$\mathbf{Q}(\sqrt{-p})$. *Then,*

$$\mathrm{Rank}(E(\mathbf{F}_q(j)) \leq \begin{cases} \dfrac{p+5}{12}f - \dfrac{h-1}{2} - 1 & \text{when } p \equiv 7 \pmod{24} \\ \dfrac{p+1}{12}f - \dfrac{h-1}{2} - 1 & \text{when } p \equiv 11 \pmod{24} \\ \dfrac{p-7}{12}f - \dfrac{h-1}{2} - 1 & \text{when } p \equiv 19 \pmod{24} \\ \dfrac{p+13}{12}f - \dfrac{h-1}{2} - 1 & \text{when } p \equiv 23 \pmod{24} \end{cases}.$$

Proof. The multiplicative descent (Theorem 5.3) shows that $\phi : Sel(\mathbf{F}_q(j), p) \to Sel(\mathbf{F}_q(j), V)$ is an isomorphism and Proposition 8.5 shows that the cokernel of ϕ contains the unramified $\mathbf{Z}/p\mathbf{Z}$-torsors over $\mathbf{F}_q(j)$. As we noted before, Mazur and Wiles ([12, Prop. 10]) show that there exists at least $\frac{h-1}{2}$ such torsors over $\mathbf{F}_q(j)$. The result now follows from the étale descent (Theorem 7.10) and arithmetic. □

Unfortunately, this result is definitely not the best possible. In fact, the equality of the numbers $\tau(E^{(p)}, dx/2y, \mathbf{F}_q(j))/\tau(E, dx/2y, \mathbf{F}_q(j))$ and $|Sel(\mathbf{F}_q(j), V)|$ strongly suggests that, when q is an odd power of p, $Sel(K, p)$ is trivial and $Ш(\mathbf{F}_q(j), E^{(p)})_p \cong Sel(\mathbf{F}_q(j), V)$. (Note that $|Sel(K, V)|$ is a square exactly when q is an odd power of p). Similar considerations on K lead me to make the following stronger conjecture.

Conjecture 8.7. *Assume that q is an odd power of p and let K be the function field $\mathbf{F}_q(X_1)$. Then $Sel(K, p)$ is trivial and $Ш(K, E^{(p)})_p \cong Sel(K, V)$.*

If this is the case then $E(K)$ has rank zero and we have formulas for $|Ш(K, E)|$ and $|Ш(K, E^{(p)})|$ as in 14.1 when $H_q(q^{-1}) \neq 0$.

Chapter V
Examples

All of the examples presented here were calculated using the Lisp language on a Symbolics 3600 computer.

1. Igusa Curves. Here is a table giving the genus and an affine equation of the Igusa curve of level p for the first few primes p. These are calculated recursively using formulas in Swinnerton-Dyer [29].

p	$g(X_1)$	Equation of X_1
5	0	$Q = 1$
7	0	$R = 1$
11	0	$QR = 1$
13	1	$6Q^3 + 8R^2 = 1$
17	2	$8Q^4 + 10QR^2 = 1$
19	3	$8Q^3R + 12R^3 = 1$
23	5	$10Q^4R + 14QR^3 = 1$
29	10	$4Q^7 + 18Q^4R^2 + 8QR^6 = 1$
31	12	$29Q^6R + 30Q^3R^3 + 4R^5 = 1$
37	19	$2Q^9 + 32Q^6R^2 + 15Q^3R^4 + 26R^6 = 1$
41	24	$33Q^{10} + 4Q^7R^2 + 29Q^4R^4 + 17QR^6 = 1$

2. Hecke polynomials. Here is a table 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 of T_p acting on S_3 for primes $p \equiv 3 \pmod 4$ with $7 \leq p \leq 71$ except $p = 67$ which was beyond the patience of the computer. The polynomial was determined by calculating the action of T_p on the Fourier coefficients of a basis of S_3, gotten by using Ross' simplification of the Hijikata trace formula [21] and the multiplicity one theorem. The factors are irreducible over $\mathbf{Z}$. Note that in every case the factor not equal to $(1+pT)$ has no root equal to p times a root of unity. (Because, for example, p does not divide the coefficient of T.) Thus, $\mathrm{Rank}(E/\mathbf{F}_q(j)) = 0$ for all $\mathbf{F}_q \not\supseteq \mathbf{F}_{p^2}$, $p \leq 71$, $p \neq 67$.

p	d	h	H_p
7	1	1	$(1+7T)$
11	1	1	$(1+11T)$
19	3	1	$(1+19T)(1+12T+361T)$
23	3	3	$(1+23T)^3$
31	5	3	$(1+31T)^3(1+10T+961T^2)$
43	7	1	$(1+43T)(1-10T+147T^2+135020T^3$ $+271803T^4-34188010T^5+6321363049T^6)$
47	7	5	$(1+47T)^5(1-62T+2209T^2)$
59	9	3	$(1+59T)^3(1-156T+13007T^2-812312T^3$ $+45277367T^4-1890308316T^5+42180533641T^6)$
67	11	1	???
71	11	7	$(1+71T)^7(1-152T+12658T^2-766232T^3+25411681T^4)$

3. Global Points. 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

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

The global height of this point is $-\frac{1}{6}log\ q$ (the local contributions are $\frac{1}{2}log\ q$ at 0, $-\frac{2}{3}log\ q$ at 1728, and 0 at ∞). Since $\tau(E, dx/2y, \mathbf{F}_q(j)) = 6$, the Birch and Swinnerton-Dyer equality implies $|Ш(\mathbf{F}_q(j), E)| = 1$ (which also follows from IV.8).

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

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

The global height of this point is $\frac{1}{2}log\ q$ (the local contributions are 0 at 0, $-\frac{3}{2}log\ q$ at 1728, and $2log\ q$ at ∞). Since $\tau(E, dx/2y, \mathbf{F}_q(j)) = 2$, the Birch and Swinnerton-Dyer equality implies $|Ш(\mathbf{F}_q(j), E)| = 1$ (which again also follows from IV.8).

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, and 3 independent points are

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

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

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

The author does not know if these points generate $E(\mathbf{F}_q(j))$ because he has not computed the global height pairing on them.

References

1. A. Altman and S. Kleiman, *Introduction to Grothendieck Duality Theory (Lecture Notes in Math. 146)*, Springer, Berlin, 1968.
2. M. Artin, *Grothendieck Topologies*, Lecture notes, Harvard Univ. Math. Dept. (1962), Cambridge, Mass.
3. P. Deligne, *Formes modulaire et représentations ℓ-adiques*, Seminaire Bourbaki 1968/69, Exposé 355 (Lecture Notes in Math. 179), Springer, Heidelberg, 1969.
4. M. Demazure, *Lectures on p-Divisible Groups (Lecture Notes in Math. 302)*, Springer, Berlin, 1972.
5. M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abhandlung aus dem Mathematischen Seminar der Hansischen Universität **14** (1941), 197-272.
6. M. Eichler, *The basis problem for modular forms and the traces of the Hecke operators*, Modular Forms of One Variable (Lecture Notes in Math. 320), Springer, Berlin, 1973, pp. 75-151.
7. B. Gross, *Heegner points and the modular curve of prime level*, Jour. Math. Soc. Japan **39** (1987).
8. E. Hecke, *Über Modulfunktionen und die Dirichletscher Reihen mit Eulerscher Produktentwicklung II.*, Math. Ann. **114** (1937), 316-351 (= Mathematische Werke, 36).
9. Y. Ihara, *Hecke polynomials as congruence ζ-functions in elliptic modular case*, Annals of Math. **85** (1967), 267-295.
10. N. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Princeton University Press, Princeton, 1985.
11. W. Li, *Newforms and functional equations*, Math. Ann. **212** (1975), 285-315.
12. B. Mazur and A. Wiles, *Analogies between function fields and number fields*, American Journal of Math. **105** (1983), 507-521.
13. J.S. Milne, *The Brauer group of a rational surface*, Inventiones Math. **11** (1970), 304-307.
14. J.S. Milne, *On a conjecture of Artin and Tate*, Annals of Math. **102** (1975), 517-533.
15. J.S. Milne, *Etale Cohomology*, Princeton University Press, Princeton, 1980.
16. J.S. Milne, *Arithmetic Duality Theorems*, Academic Press, Orlando, Florida, 1986.
17. D. Mumford, *Abelian Varieties*, Oxford University Press, Oxford, 1970.
18. F. Oort and J. Tate, *Group schemes of prime order*, Ann. Scient. de l'Ecole Normal Superieur **3 (4ième Série)** (1970), 1-21.
19. A. Robert, *Elliptic Curves (Lecture Notes in Math. 326)*, Springer, New York, 1973.
20. L. Roberts, *The flat cohomology of group schemes of rank p*, American Journal of Math. **45** (1973), 688-702.
21. S. Ross, *Hecke operators for $\Gamma_0(N)$, their traces, and applications*, Ph.D. Thesis, University of Rochester (1985).
22. S. Schatz, *Profinite Groups, Arithmetic, and Geometry*, Princeton University Press, Princeton, 1972.
23. J.-P. Serre, *Sur la topologie des variétés algébriques en charactéristic p*, Symposium internacional de topologia algebraica, Universidad Autónoma de México and UNESCO, Mexico, 1958, pp. 24-53.
24. J.-P. Serre, *Groupes Algebriques et Corps de Classes*, Hermann, Paris, 1959.
25. J.-P. Serre, *Corps Locaux*, Hermann, Paris, 1962.
26. J.-P. Serre, *Letter to Fontaine (1979)*.
27. T. Shioda, *On elliptic modular surfaces*, Jour. Math. Soc. Japan **24** (1972), 20-58.
28. J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.
29. H.P.F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms*, Modular Forms of One Variable III (Lecture Notes in Math. 350), Springer, Heidelberg, 1973.
30. J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Int. Cong. Math. Stockholm (1962), 288-295.
31. J. Tate, *Algebraic cycles and poles of zeta functions*, Arithmetical Algebraic Geometry, Harper and Row, New York, 1965.

32. J. Tate, *On the conjecture of Birch and Swinnerton-Dyer and a geometric analog*, Seminaire Bourbaki 1965/66, Exposé 306.
33. J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular Forms of One Variable IV (Lecture Notes in Math. 476), Springer, Heidelberg, 1975.
34. A. Weil, *Basic Number Theory*, Springer, New York, 1974.
35. A. Weil, *Adeles and Algebraic Groups*, Birkhäuser, Boston, 1982.