

# $p$ -descent in characteristic $p$

Douglas L. Ulmer

Department of Mathematics

California Institute of Technology

Pasadena, CA 91125

September 23, 1990

This paper is concerned with the problem of calculating the Selmer group for the multiplication by  $p$  isogeny on an elliptic curve over a global field of characteristic  $p$ . The motivation for studying this problem comes from our earlier work on universal elliptic curves over Igusa curves, which are expected to have points of infinite order. After developing the machinery of  $p$ -descents in general in the first half of the paper, we turn to the universal curves, where we are able to express the Selmer group in terms of modular forms (mod  $p$ ) of low weights. In particular, we produce a subspace of the Selmer group predicted by earlier  $L$ -function computations and the Birch and Swinnerton-Dyer conjecture.

The plan of the paper is as follows: In the first section we establish some notation and prove a few easy lemmas on Selmer groups which reduce the problem to certain cohomology calculations. Next, two modular forms  $A$  and  $B$  on elliptic curves in characteristic  $p$  are defined. The Hasse invariant  $A$  is interpreted in terms of finite flat group schemes; a similar interpretation of  $B$  occurs later in the paper. The third section applies these results to calculate the Selmer group for the Frobenius and Verschiebung isogenies for an elliptic curve over a global field of characteristic  $p$  in terms of invariants of the base field such as

its differentials and generalized Jacobians. In order to make the Selmer group calculation for the multiplication by  $p$  isogeny, we require rather detailed information on the kernel of  $p$  on a supersingular elliptic curve over a finite field and section four contains this analysis, as well as an application to the Selmer group for  $p$  on a constant supersingular elliptic curve over a global field. Section five, which is the main technical computation, contains a calculation of the local Selmer group for  $p$  on an elliptic curve over a local field of characteristic  $p$  with good, supersingular reduction. In section six, we tie up some loose ends for the cases  $p = 2, 3$  by using Voloch's explicit descent formulae. The seventh section is devoted to explicitly describing the Selmer groups for Frobenius, Verschiebung and  $p$  on the universal elliptic curves over Igusa curves studied in [16] in terms of modular forms (mod  $p$ ). These groups have surprising extra structure, such as a filtration similar to the Hodge filtration on 1-dimensional deRham cohomology, and a symmetric bilinear form on the Selmer group for  $p$ . Finally, section eight presents some examples of the universal case and treats explicitly the cases excluded from the general theory of section seven.

Explicit formulae for doing  $p$  descents in characteristic  $p$  have been given by K. Kramer [5] for  $p = 2$ , and by J.F. Voloch [18] for general  $p$ . It is a pleasure to thank Voloch for numerous comments on and corrections to an earlier version of this paper and to thank B. Gross for suggesting this problem and for his continued interest in it.

**1. The Selmer group** In what follows, a global field will be either a number field or the function field of a curve over a finite field; a local field will be the completion of a global field at some place. Unless stated otherwise, all cohomology groups will be calculated on the flat ( $fppf$ ) site. Let  $f : A \rightarrow A'$  be an isogeny of abelian varieties over a global field  $K$ . Then there is an exact sequence of sheaves for the flat topology on  $K$

$$0 \rightarrow \text{Ker } f \rightarrow A \rightarrow A' \rightarrow 0$$

and for every place  $v$  of  $K$  we define the local Selmer group  $\text{Sel}(K_v, f)$  to be the image of the coboundary map

$$A'(K_v) \rightarrow H^1(K_v, \text{Ker } f).$$

The global Selmer group  $\text{Sel}(K, f)$  is defined to be the set of elements in  $H^1(K, \text{Ker } f)$  whose restrictions to  $H^1(K_v, \text{Ker } f)$  lie in  $\text{Sel}(K_v, f)$  for all  $v$ . The interest of this group is that there is an exact sequence

$$0 \rightarrow A'(K)/f(A(K)) \rightarrow \text{Sel}(K, f) \rightarrow \mathbb{H}(K, A)_f \rightarrow 0 \quad (1.1)$$

where the Tate-Shafarevitch group  $\mathbb{H}(K, A)$  is  $\text{Ker}(H^1(K, A) \rightarrow \prod_v H^1(K_v, A))$  and  $\mathbb{H}(K, A)_f$  is the subgroup of elements in the kernel of the induced map  $f : \mathbb{H}(K, A) \rightarrow \mathbb{H}(K, A')$ . Moreover,  $\text{Sel}(K, f)$  is finite and usually computable in practice. In particular, if  $A = A'$  and  $f$  is multiplication by an integer, the map 1.1 (together with the Mordell-Weil theorem) gives a bound on the rank of the Mordell-Weil group  $A(K)$ .

We collect here a few lemmas on the Selmer group. The first result often allows one to calculate the local Selmer groups in terms of the cohomology of finite flat group schemes.

**Lemma 1.2.** *Let  $K_v$  be a local field with ring of integers  $R_v$  and let  $f : A \rightarrow A'$  be an isogeny of abelian varieties with good reduction over  $R_v$ . Then the restriction map  $H^1(R_v, \text{Ker } f) \rightarrow H^1(K_v, \text{Ker } f)$  induces an isomorphism  $\text{Sel}(K_v, f) \cong H^1(R_v, \text{Ker } f)$ .*

**Proof:** Since  $A'$  has good reduction,  $A'(K_v) = A'(R_v)$  and by Lang's theorem and Hensel's lemma (see [11] VI.4 cor. 1 and [6] I.4.3),  $H^1(R_v, A) = 0$ , so  $A'(R_v) \rightarrow H^1(R_v, \text{Ker } f)$  is surjective. Finally,  $\text{Ker } f$  is a flat group scheme so the restriction  $H^1(R_v, \text{Ker } f) \rightarrow H^1(K_v, \text{Ker } f)$  is injective and the lemma follows.  $\square$

The following result will be useful in applying lemma 1.2.

**Lemma 1.3.** *Let  $L/K_v$  be a Galois extension of local fields with Galois group  $G$  of order prime to the degree of  $f$ . Then the inclusion  $H^1(K_v, \text{Ker } f) \rightarrow H^1(L, \text{Ker } f)$  induces an isomorphism  $\text{Sel}(K_v, f) \cong \text{Sel}(L, f)^G$ .*

**Proof:** Since the order of  $G$  is prime to the degree of  $f$ , we have an isomorphism  $H^1(K_v, \text{Ker } f) \cong H^1(L, \text{Ker } f)^G$  and clearly the image of  $\text{Sel}(K_v, f)$  lies in  $\text{Sel}(L, f)^G$ . Now  $\text{Ker}(H^1(K_v, A) \rightarrow H^1(L, A))$  has no elements of order dividing the degree of  $f$ , so  $\text{Sel}(K_v, f) = \text{Ker}(H^1(K_v, \text{Ker } f) \rightarrow H^1(K_v, A))$  maps onto  $\text{Ker}(H^1(L, \text{Ker } f) \rightarrow H^1(L, A))^G = \text{Sel}(L, f)^G$  which completes the proof.  $\square$

**Lemma 1.4.** *If  $L/K$  is a Galois extension of global fields with Galois group  $G$  of order prime to the degree of  $f$ , then the restriction map  $H^1(K, \text{Ker } f) \rightarrow H^1(L, \text{Ker } f)$  induces an isomorphism  $\text{Sel}(K, f) \cong \text{Sel}(L, f)^G$ .*

**Proof:** As before,  $H^1(K, \text{Ker } f) \cong H^1(L, \text{Ker } f)^G$  and  $\text{Sel}(K, f) \hookrightarrow \text{Sel}(L, f)^G$ . But if  $x \in \text{Sel}(L, f)^G$ , then the restriction  $x_w$  lies in  $\text{Sel}(L_w, f)^{G_w}$  for all places  $w$  of  $L$ , where

$G_w$  is the decomposition group at  $w$ . By the previous lemma,  $x_w$  is the image of some  $y_v$  in  $\text{Sel}(K_v, f)$  and so the  $y \in H^1(K, \text{Ker } f)$  mapping to  $x$  lies in  $\text{Sel}(K, f)$ .  $\square$

**2. The modular forms  $A$  and  $B$**  Let  $S$  be a scheme of characteristic  $p$  and  $\pi : E \rightarrow S$  an elliptic curve over  $S$ . Recall that the deRham cohomology sheaf  $\mathcal{H}_{dR}^1(E/S)$  is defined to be the hyper direct image  $\mathcal{R}^1\pi_*(\mathcal{O}_E \rightarrow \Omega_{E/S}^1)$ . One knows that  $\mathcal{H}_{dR}^1(E/S)$  is a locally free sheaf of rank 2 on  $S$  equipped with a non-degenerate alternating bilinear form  $\langle, \rangle_{dR} : \mathcal{H}_{dR}^1(E/S) \times \mathcal{H}_{dR}^1(E/S) \rightarrow \mathcal{O}_S$  and there is an exact sequence of locally free sheaves

$$0 \rightarrow \pi_*\Omega_{E/S}^1 \rightarrow \mathcal{H}_{dR}^1(E/S) \rightarrow R^1\pi_*\mathcal{O}_E \rightarrow 0.$$

If  $e : S \rightarrow E$  is the zero section, then  $\pi_*\Omega_{E/S}^1 = e^*\Omega_{E/S}^1$  and it is traditional to denote both of these invertible sheaves by  $\underline{\omega}$ . One has  $R^1\pi_*\mathcal{O}_E \cong \underline{\omega}^{-1}$  by Serre duality.

If  $F : E \rightarrow E^{(p)}$  denotes the  $S$ -linear Frobenius, we have an induced map  $F^* : \mathcal{H}_{dR}^1(E^{(p)}/S) \rightarrow \mathcal{H}_{dR}^1(E/S)$ . To get a local coordinate expression for  $F^*$ , choose a local generator  $\omega$  of  $\underline{\omega}$ . Further choose a section  $\eta$  of  $\mathcal{H}_{dR}^1(E/S)$  with  $\langle \omega, \eta \rangle_{dR} = 1$ ;  $\eta$  is determined up to addition of multiples of  $\omega$  and projects to a section of  $R^1\pi_*\mathcal{O}_E$  dual to  $\omega$ . Base changing by the absolute Frobenius of  $S$ , we get elements  $\omega^{(p)}, \eta^{(p)}$  of  $\mathcal{H}_{dR}^1(E^{(p)}/S)$  and  $F^*(\omega^{(p)}) = 0$ ,  $F^*(\eta^{(p)}) = A\eta + B\omega$  for certain sections  $A$  and  $B$  of  $\mathcal{O}_S$ . Moreover,  $A$  depends only on  $E$  and  $\omega$  (not on the choice of  $\eta$ ) and  $A(E, a^{-1}\omega) = a^{p-1}A(E, \omega)$ —in other words,  $A$  is a modular form of weight  $p-1$  on elliptic curves in characteristic  $p$ ; it is called the *Hasse invariant*. The local sections  $A(E, \omega)$  of  $\mathcal{O}_S$  define sections  $A(E, \omega)\omega^{(p-1)}$  which patch together to give a global section  $A(E)$  of  $\underline{\omega}^{\otimes(p-1)}$  on  $S$ . As is well-known, when  $S$  is the spectrum of a field  $k$ ,  $E$  is supersingular (e.g., has no point of order  $p$  over  $\bar{k}$ ) exactly when  $A = 0$ . See [4, 12.4.1] for several other calculations of  $A$ .

The invariant  $B$  does depend on the choice of  $\eta$ , but only up to addition of multiples of  $A$ . In particular, where  $A = 0$ , i.e.,  $E$  is supersingular,  $B$  is a well-defined function of  $E$  and  $\omega$ , and  $B(a^{-1}\omega) = a^{p+1}B(E, \omega)$ —in other words,  $B$  is a modular form of weight  $p+1$  on supersingular elliptic curves in characteristic  $p$ . When  $p > 3$ , there are congruences  $A \equiv E_{p-1}$ ,  $B \equiv -\frac{1}{12}E_{p+1}$  where  $E_k$  is the Eisenstein series of weight  $k$ . We will interpret  $A$  and  $B$  in terms of certain finite group schemes in 2.1 and 4.1.

Recall that by the Oort-Tate classification [15], a group scheme of order  $p$  over a scheme  $S$  of characteristic  $p$  is determined by giving an invertible sheaf  $\mathcal{L}$  and sections  $a$  of  $\mathcal{L}^{\otimes(p-1)}$ ,  $b$  of  $\mathcal{L}^{\otimes(1-p)}$  such that  $ab = 0$ . Write  $G_{\mathcal{L},a,b}$  for this group scheme. For example,  $G_{\mathcal{O},1,0} \cong \mathbf{Z}/p\mathbf{Z}$ ,  $G_{\mathcal{O},0,1} \cong \mu_p$ , and  $G_{\mathcal{O},0,0} \cong \alpha_p$ .

**Proposition 2.1.** *Let  $E$  be an elliptic curve over a scheme  $S$  of characteristic  $p$ ,  $F : E \rightarrow E^{(p)}$  the Frobenius isogeny, and  $V : E^{(p)} \rightarrow E$  its dual, the Verschiebung. Then as finite flat group schemes over  $S$ ,  $\text{Ker } F \cong G_{\underline{\omega}^{-1},0,A(E)}$  and  $\text{Ker } V \cong G_{\underline{\omega},A(E),0}$ .*

**Proof:** We will prove this for  $\text{Ker } F$ ; the statement for  $\text{Ker } V$  follows by Cartier duality. First note that  $\text{Ker } F$  is a  $S$ -group of height 1, i.e., for every  $x$  in the defining ideal of the zero section,  $x^p = 0$ . But such group schemes are determined by their  $p$ -Lie algebras ([8], p. 139), and  $p\text{-Lie}(\text{Ker } F) = p\text{-Lie}(E)$ . Now  $p\text{-Lie}(E)$  is abelian of rank one, and the  $p$ -power map is given locally by  $D^p = A(E, \omega)D$  where  $D$  is a section of  $\underline{\omega}^{-1}$  dual to a generating section  $\omega$  of  $\underline{\omega}$  (use a relative version of [8], p. 148 and the definition of  $A$ ). But it follows easily from the definition that the height 1 group scheme on  $S$  with this  $p$ -Lie algebra is exactly  $G_{\underline{\omega}^{-1},0,A(E)}$ .  $\square$

We will apply this where  $S$  is the spectrum of a field or a discrete valuation ring, so

$\mathcal{L}$  will be trivial. In this case, we write  $G_{a,b}$  for  $G_{\mathcal{L},a,b}$ .

**3. Frobenius and Verschiebung descents** We now specialize the Selmer group considerations of section 1 to the case where  $K$  is the function field of a curve over a finite field of characteristic  $p$  and  $A = E$  is an elliptic curve. We also exclude until the end of this section the case where the  $j$ -invariant of  $E$  is an element of the constant field of  $K$ . As a first step toward determining  $\text{Sel}(K, p)$  we factor  $p$  as  $V \circ F$ , where  $F : E \rightarrow E^{(p)}$  is the  $K$ -linear Frobenius and  $V : E^{(p)} \rightarrow E$ , is the Verschiebung, the dual isogeny, and calculate the groups  $\text{Sel}(K, F)$  and  $\text{Sel}(K, V)$ .

Now  $E^{(p)}(K)$  has a non-trivial point of order  $p$  if and only if  $\text{Ker } V \cong \mathbf{Z}/p\mathbf{Z}$  over  $K$ , if and only if for some choice of differential  $\omega$  one has  $A(E, \omega) = 1$ . Since  $j(E)$  is not a constant,  $A(E, \omega) \neq 0$  (as “ $A$  has simple zeros” [4] 12.4.3) so there is an extension of  $K$  of degree dividing  $p - 1$  over which  $E^{(p)}$  has such a point; from now on, we replace  $K$  with this extension, i.e., assume that  $E^{(p)}(K)$  has a non-trivial point of order  $p$ . This is no loss, since lemma 1.4 allows one to recover the Selmer groups for  $F$ ,  $V$ , and  $p$  over the original field from those over  $K$ .

Now *fix once and for all a choice of non-trivial point  $P$  of order  $p$  in  $E^{(p)}(K)$* . This choice allows us to define canonically a differential  $\omega_{can}$  on  $E$  such that  $A(E, \omega_{can}) = 1$ :  $P$  defines an isomorphism  $\mathbf{Z}/p\mathbf{Z} \xrightarrow{\sim} \text{Ker } V$  over  $K$  ( $1 \mapsto P$ ) so by Cartier duality  $\text{Ker } F \xrightarrow{\sim} \mu_p$  and  $\omega_{can}$  is the unique differential on  $E$  restricting to the pull back of  $dt/t$  on  $\text{Ker } F$  (where  $t$  is the usual coordinate on  $\mu_p$ ). Replacing  $P$  by  $a^{-1}P$  replaces  $\omega_{can}$  by  $a^{-1}\omega_{can}$  for  $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ .

For every place  $v$  of  $K$ , let  $K_v$  be the completion of  $K$  at  $v$ . By Kummer theory

$H^1(K_v, \text{Ker } F) \cong H^1(K_v, \mu_p) \cong K_v^\times / K_v^{\times p}$  and by Artin-Schreier theory,  $H^1(K_v, \text{Ker } V) \cong H^1(K_v, \mathbf{Z}/p\mathbf{Z}) \cong K_v / \wp(K_v)$  (where  $\wp(x) = x^p - x$ ). We define certain subgroups as follows:  $U^{[i]} = \{\bar{f} \in K_v^\times / K_v^{\times p} \mid v(1 - f) \geq i\}$  ( $i \geq 0$ ) and  $P^{[j]} = \{\bar{f} \in K_v / \wp(K_v) \mid v(f) \geq -j\}$  ( $j \geq 0$ ). The  $U^{[i]}$  form a decreasing exhaustive filtration of the compact group  $K_v^\times / K_v^{\times p}$  by subgroups of finite index with  $(K_v^\times / K_v^{\times p}) / U^{[0]} \cong \mathbf{Z}/p\mathbf{Z}$  (canonically),  $U^{[i]} / U^{[i+1]} \cong \mathbf{F}_q$  (non-canonically) if  $p \nmid i$ , and  $U^{[pi]} / U^{[pi+1]} \cong 1$ . The  $P^{[j]}$  form an increasing exhaustive filtration of the discrete group  $K_v / \wp(K_v)$  by finite groups with  $P^{[0]} \cong \mathbf{Z}/p\mathbf{Z}$  (canonically),  $P^{[i]} / P^{[i-1]} \cong \mathbf{F}_q$  (non-canonically) if  $p \nmid i$ , and  $P^{[pi]} / P^{[pi-1]} = 0$ .

Recall the discriminant modular form  $\Delta$ :  $\Delta(E, \omega) \in K$ ,  $\Delta(E, a^{-1}\omega) = a^{12}\Delta(E, \omega)$ , and  $v(\Delta(E, \omega_{Néron})) = 0$  for a Néron differential  $\omega_{Néron}$  if and only if  $E$  has good reduction at  $v$ .

**Proposition 3.1.** *Let  $E$  be an elliptic curve with non-constant  $j$ -invariant over a global field  $K$  of characteristic  $p$  and assume that  $p > 3$  and that  $E^{(p)}$  has a fixed point  $P$  of order  $p$  rational over  $K$ .*

a) *If  $E$  has potentially good reduction at  $v$  (i.e.,  $v(j(E)) \geq 0$ ) then there are isomorphisms*

$$\text{Sel}(K_v, F) \cong U_{K_v}^{[i]} \text{ and } \text{Sel}(K_v, V) \cong P_{K_v}^{[j]} \text{ where } i = \lceil \frac{-p}{12} v(\Delta(E, \omega_{can})) \rceil \text{ and } j = \lfloor \frac{-p}{12} v(\Delta(E, \omega_{can})) \rfloor. \text{ (Here } \lceil x \rceil \text{ denotes the smallest integer } \geq x \text{ and } \lfloor x \rfloor \text{ denotes the largest integer } \leq x.)$$

b) *If  $E$  has potentially multiplicative reduction at  $v$  (i.e.,  $v(j(E)) < 0$ ) then  $\text{Sel}(K_v, F) =$*

$$K_v^\times / K_v^{\times p} \text{ and } \text{Sel}(K_v, V) = 0.$$

We call the places where  $v(\Delta(E, \omega_{can})) = 0$  *ordinary* places, the places where  $v(\Delta(E, \omega_{can})) < 0$

0 *supersingular* places, and the places where  $v(\Delta(E, \omega_{can})) > 0$  *cuspidal* places, or *cusps*.

Since  $A(E, \omega_{can}) = 1$ , case a) of proposition 3.1 corresponds to ordinary and supersingular places while case b) corresponds to cuspidal places. In particular, at ordinary places,  $\text{Sel}(K, F) \cong U^{[0]}$  and  $\text{Sel}(K, V) \cong P^{[0]}$ .

**Proof:** a) Since  $p > 3$ , we can find a local Galois extension  $L/K_v$  of degree prime to  $p$  with Galois group  $G$  such that  $E$  and  $E^{(p)}$  obtain good reduction over  $L$ . Let  $\mathcal{O}_L$  be the ring of integers of  $L$ ,  $w$  the normalized valuation of  $L$  and  $t$  a uniformiser of  $L$ . Then  $n = -w(\Delta(E, \omega_{can}))/12$  is a (non-negative) integer and  $t^{-n}\omega_{can}$  is a Néron differential for  $E$  over  $L$ . As  $E$  and  $E^{(p)}$  have good reduction over  $\mathcal{O}_L$ ,  $\text{Ker } F$  and  $\text{Ker } V$  are finite flat group schemes over  $\mathcal{O}_L$  isomorphic to  $G_{0,A}$  and  $G_{A,0}$  respectively, where  $A = A(E, t^{-n}\omega_{can}) = t^{(p-1)n}$ . Applying lemma 1.2 and a cohomology calculation of Milne (see [6], III.7.5), we find  $\text{Sel}(L, F) \cong H^1(\mathcal{O}_L, G_{0,A}) \cong U_L^{[pm]}$  and  $\text{Sel}(L, V) \cong H^1(\mathcal{O}_L, G_{A,0}) \cong P_L^{[pm]}$ . Finally, lemma 1.3 and an easy invariant calculation show that  $\text{Sel}(K_v, F) \cong \text{Sel}(L, F)^G \cong U_{K_v}^{[i]}$  and  $\text{Sel}(K_v, V) \cong \text{Sel}(L, V)^G \cong P_{K_v}^{[j]}$  as was to be shown.

b) In this case, there exists a local Galois extension  $L/K_v$  of degree prime to  $p$  such that  $E$  and  $E^{(p)}$  obtain split multiplicative reduction over  $L$ . Thus we have parametrizations

$$L^\times / q^{\mathbf{Z}} \xrightarrow{\sim} E(L)$$

$$L^\times / q^{p\mathbf{Z}} \xrightarrow{\sim} E^{(p)}(L)$$

for some element  $q \in L$ . Composing the second with the coboundary map  $E^{(p)}(L) \rightarrow H^1(L, \text{Ker } F) \cong L^\times / L^{\times p}$  yields the natural surjection  $L^\times / q^{p\mathbf{Z}} \rightarrow L^\times / L^{\times p}$  and so  $\text{Sel}(L, F) \cong L^\times / L^{\times p}$ . Applying lemma 1.3,  $\text{Sel}(K_v, F) \cong K_v^\times / K_v^{\times p}$ . On the other hand,  $L^\times / q^{p\mathbf{Z}} \xrightarrow{\sim}$

$E^{(p)}(L) \rightarrow E(L) \xrightarrow{\sim} L^\times/q^{\mathbf{Z}}$  is clearly surjective, so  $\text{Sel}(L, V) = 0$  and by lemma 1.3,  $\text{Sel}(K_v, V) = 0$ .  $\square$

Note that in all cases Tate duality (see [7] III.7.2) holds:  $\text{Sel}(K_v, F)$  and  $\text{Sel}(K_v, V)$  are orthogonal complements under the Artin-Schreier pairing. We postpone a discussion of the cases  $p = 2, 3$  until section 6.

Introduce a divisor  $D = \sum_v \text{cuspidal}[v] - \sum_v \text{non-cuspidal} i_v[v]$  where  $i_v = \lceil \frac{-p}{12}v(\Delta(E, \omega_{can})) \rceil - 1$  if  $p \nmid \lceil \frac{-p}{12}v(\Delta(E, \omega_{can})) \rceil$  and  $i_v = \lceil \frac{-p}{12}v(\Delta(E, \omega_{can})) \rceil$  otherwise. Define a modulus (effective divisor)  $\mathbf{m} = \sum_v \text{non-cuspidal} j_v[v]$  where  $j_v = \lfloor \frac{-p}{12}v(\Delta(E, \omega_{can})) \rfloor + 1$  if  $p \nmid \lfloor \frac{-p}{12}v(\Delta(E, \omega_{can})) \rfloor$  and  $j_v = \lfloor \frac{-p}{12}v(\Delta(E, \omega_{can})) \rfloor$  otherwise. Note that  $i_v = j_v = 0$  at ordinary  $v$ .

If  $X$  is the complete non-singular curve over  $\mathbf{F}_q$  associated to  $K$ , then  $H^0(X, \Omega_X^1(D))$  is a finite dimensional  $\mathbf{F}_q$  vector space and the subset of elements fixed by the  $p^{-1}$ -linear Cartier operator  $\mathcal{C}$  (see [14]) is an  $\mathbf{F}_p$  vector space. Associated to  $X$  we also have the generalized Jacobian  $J_{\mathbf{m}}$  for the modulus  $\mathbf{m}$ ;  $J_{\mathbf{m}}$  is an algebraic group whose points parameterize divisors of degree 0 on  $X$  supported away from  $\mathbf{m}$  modulo divisors of functions  $f$  such that  $f \equiv 1 \pmod{\mathbf{m}}$  ([11], ch. 5). Let  $\langle \text{cusps} \rangle$  be the subgroup of  $J_{\mathbf{m}}(\mathbf{F}_q)$  generated by the classes of  $\mathbf{F}_q$ -rational divisors of degree 0 supported on the cusps.

**Theorem 3.2.** *Let  $E$  be an elliptic curve with non-constant  $j$ -invariant over a global field  $K$  of characteristic  $p$  and assume that  $p > 3$  and that  $E^{(p)}$  has a fixed point  $P$  of order  $p$  rational over  $K$ . Then we have isomorphisms  $\text{Sel}(K, F) \cong H^0(X, \Omega_X^1(D))^{\mathcal{C}}$  and  $\text{Sel}(K, V) \cong \text{Hom}(J_{\mathbf{m}}(\mathbf{F}_q)/\langle \text{cusps} \rangle, \mathbf{Z}/p\mathbf{Z})$ .*

**Proof:** There is an injective map  $K^\times/K^{\times p} \rightarrow \Omega_K^1$  where  $\Omega_K^1$  is space of meromorphic

differentials on  $X$  (i.e., the stalk at the generic point of  $\Omega_X^1$ ), given by  $\bar{f} \rightarrow df/f$  and the image consists of exactly those differentials fixed by the Cartier operator. Now  $\bar{f} \in \text{Sel}(K_v, F)$  if and only if  $v(df/f) \geq i_v$  for non-cuspidal  $v$ , so the local conditions given in proposition 3.1 say exactly that  $\bar{f} \in \text{Sel}(K, F)$  if and only if  $df/f \in H^0(X, \Omega_X^1(D))^c$ .

For the  $V$  descent, note that by Artin-Schreier theory, elements of  $K/\wp(K)$  parameterize Galois extensions  $L/K$  with isomorphisms  $\text{Gal}(L/K) \cong \mathbf{Z}/p\mathbf{Z}$ . Moreover,  $\bar{f} \in \text{Sel}(K_v, V)$  if and only if the associated extension  $L/K$  has conductor  $\leq j_v$  at  $v$  ([11], VI.12, ex. 2) for non-cuspidal  $v$ . The condition at a cusp  $v$  that  $\bar{f} = 0 \in K_v/\wp(K_v)$  is exactly that  $L/K$  be completely split at  $v$ . By geometric class field theory ([11], ch. 6), the Galois group of the maximal extension whose conductor is bounded by  $\mathbf{m}$  and which is split at the cusps is isomorphic to  $J_{\mathbf{m}}(\mathbf{F}_q)/\langle \text{cusps} \rangle$  and so  $\text{Sel}(K, V) \cong \text{Hom}(J_{\mathbf{m}}(\mathbf{F}_q)/\langle \text{cusps} \rangle, \mathbf{Z}/p\mathbf{Z})$ .

□

For completeness, we record the following proposition on the Selmer groups of a constant elliptic curve over a global field of characteristic  $p$ . The proofs are an easy exercise using 1.2, 1.4, and 2.1.

**Proposition 3.3.** *Let  $E$  be an elliptic curve over a finite field  $k$ ,  $\omega$  a non-zero invariant differential on  $E$ , and put  $A = A(E, \omega) \in k$ . Let  $K$  be the function field of a smooth, irreducible, complete curve  $X$  over  $k$  and consider  $E$  as an elliptic curve over  $K$  by base extension.*

a) *If  $A \neq 0$ , so  $E$  is ordinary, then  $\text{Sel}(K, F) \cong H^1(X, G_{0,A}) \cong \{\omega \in H^0(X, \Omega_X^1) | \mathcal{C}(\omega) = A\omega\}$  and  $\text{Sel}(K, V) \cong H^1(X, G_{A,0}) \cong \{\eta \in H^1(X, \mathcal{O}_X) | \text{Fr}(\eta) = A\eta\}$ .*

b) *If  $A = 0$ , so  $E$  is supersingular, then  $\text{Sel}(K, F) \cong \text{Sel}(K, V) \cong H^1(X, G_{0,0}) \cong \{\omega \in$*

$$H^0(X, \Omega_X^1) | \mathcal{C}(\omega) = 0 \cong \{ \eta \in H^1(X, \mathcal{O}_X) | Fr(\eta) = 0 \}$$

We remark that if  $E$  is ordinary, then the kernel of  $p$  on  $E$  splits as a direct sum  $\text{Ker } p = G_{0,A} \oplus G_{A^{1/p},0} \cong G_{0,A} \oplus G_{A,0}$  of finite flat group schemes, and the Selmer group for  $p$  is a direct sum of Selmer groups for the simpler isogenies  $F$  and  $V$ . On the other hand, if  $E$  is supersingular, the kernel of  $p$  is a non-trivial extension of  $G_{0,0}$  by  $G_{0,0}$  and the  $p$ -descent is more difficult. We will treat this case at the end of the next section.

**4. The kernel of  $p$  on a supersingular curve** In order to make local descent calculations for multiplication by  $p$ , we will need rather detailed information on the kernel of multiplication by  $p$  on a supersingular elliptic curve over a finite field  $k$ . Since  $\text{Ker } F$  and  $\text{Ker } V$  are isomorphic to  $G_{0,0} \cong \alpha_p$  over  $k$  (by proposition 2.1) and  $p = V \circ F$  is a self-dual isogeny, we recover the well known fact that  $\text{Ker } p$  is a self-dual extension of  $\alpha_p$  by  $\alpha_p$ ; we will require somewhat more precise information.

Let  $W_n$  denote the ring scheme of Witt vectors of length  $n$ ; there are homomorphisms  $F : W_n \rightarrow W_n$ ,  $V : W_n \rightarrow W_{n+1}$ , and  $R : W_n \rightarrow W_{n-1}$  (see [19]). We will frequently write  $V$  for  $RV$ . Recall that the group scheme  $\alpha_p$  over  $k$  has ring of functions  $k[z]/z^p$  and comultiplication  $m^* : z \mapsto z \otimes 1 + 1 \otimes z$  and is naturally isomorphic to the kernel of  $F$  on  $W_1$ .

**Proposition 4.1.** *Let  $E$  be a supersingular elliptic curve over a finite field  $k$ ,  $F : E \rightarrow E^{(p)}$  and  $V : E^{(p)} \rightarrow E$  the Frobenius and Verschiebung isogenies respectively. Fix an invariant differential  $\omega$  on  $E$  and let  $B = B(E, \omega) \in k$ . Let  $i : \text{Ker } F \rightarrow \alpha_p$  be the unique isomorphism such that  $i^*(dz) = \omega$  and let  $j = i^{\vee-1} : \text{Ker } V \rightarrow \alpha_p$  be*

the inverse of the Cartier dual of  $i$ . If  $G = \text{Ker}(B^{-1}F + VB^{-1} : W_2 \rightarrow W_2)$ , then  $0 \rightarrow \alpha_p \xrightarrow{VB} G \xrightarrow{R} \alpha_p \rightarrow 0$  is an exact sequence of finite flat group schemes over  $k$ , and there is a unique isomorphism  $\text{Ker } p \xrightarrow{\sim} G$  such that the following diagram commutes:

$$\begin{array}{ccccccc} 0 & \rightarrow & \text{Ker } F & \rightarrow & \text{Ker } p & \rightarrow & \text{Ker } V \rightarrow 0 \\ & & i \downarrow & & \downarrow & & \downarrow j \\ 0 & \rightarrow & \alpha_p & \xrightarrow{VB} & G & \xrightarrow{R} & \alpha_p \rightarrow 0 \end{array}$$

**Remark:** If  ${}_m W_n$  denotes the kernel of  $F^m$  on  $W_n$ , then  ${}_2 W_1$  and  ${}_1 W_2$  define canonically elements of  $\text{Ext}_k^1(\alpha_p, \alpha_p)$  and  $k \cong \text{Hom}_k(\alpha_p, \alpha_p)$  acts on  $\text{Ext}_k^1(\alpha_p, \alpha_p)$  by push-out and pull-back. Using the maps  $i$  and  $j$  above,  $\text{Ker } p$  also defines an element of  $\text{Ext}_k^1(\alpha_p, \alpha_p)$  and the proposition is equivalent to the statement that  $\text{Ker } p \cong B_*^{-1} {}_1 W_2 - B^{-1*} {}_2 W_1$  in  $\text{Ext}_k^1(\alpha_p, \alpha_p)$ .

**Proof:** The uniqueness of the isomorphism  $\text{Ker } p \rightarrow G$  and the exactness of the bottom row of the diagram are clear. We will use Dieudonné modules and Oda's thesis [9] to show the existence. Let  $W(k)$  be the infinite Witt vectors with coordinates in  $k$ ,  $\sigma : W(k) \rightarrow W(k)$  the map induced by the absolute Frobenius of  $k$ , and  $A$  the non-commutative ring  $W(k)\{F, V\}$  with relations  $FV = VF = p$ ,  $Fa = a^\sigma F$ , and  $aV = Va^\sigma$ . Let  $CW$  be the scheme of Witt covectors over  $k$ :  $CW = \varinjlim_n W_n$  where  $W_n$  is made into a  $W$  module via  $\sigma^n$  and the limit is taken with respect to the maps  $V : W_n \rightarrow W_{n+1}$ ;  $CW$  is naturally an  $A$ -module. The contravariant functor  $G \mapsto M(G) = \text{Hom}_{k\text{-group}}(G, CW)$  is an equivalence of categories from finite, flat, unipotent group schemes over  $k$  to  $A$ -modules of finite length on which  $V$  is nilpotent. The functor which sends an  $A$ -module to the (representable) group functor  $R \mapsto G(R) = \text{Hom}_A(M, CW(R))$  for  $k$ -algebras  $R$  is a quasi-inverse. We can canonically identify  $M(\alpha_p)$  with the cyclic  $A$ -module  $A/(F, V)$  by requiring that  $1 \in A$

correspond to the natural  $\phi \in \text{Hom}(\alpha_p, CW)$  induced from  $\alpha_p \hookrightarrow W_1$ .

Now Oda's theorem ([9], 5.11) gives a canonical identification of  $M(\text{Ker } p)$  with  $H_{dR}^1(E)$  and an isomorphism of exact sequences

$$\begin{array}{ccccccc} 0 & \leftarrow & M(\text{Ker } F) & \leftarrow & M(\text{Ker } p) & \leftarrow & M(\text{Ker } V) & \leftarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \leftarrow & H^1(E, \mathcal{O}) & \leftarrow & H_{dR}^1(E) & \leftarrow & H^0(E, \Omega^1) & \leftarrow & 0. \end{array}$$

(Here we are using that  $\text{Ker}(F : E \rightarrow E^{(p)}) = \text{Ker}(V : E \rightarrow E^{(p^{-1})})$  and  $E \cong E^{(p^2)}$  for a supersingular curve  $E$ .) The actions of  $F$  and  $V \in A$  on the cohomology groups are via Frobenius and the Cartier operator respectively (see [9], 5.8).

We identify the given  $\omega \in H^0(E, \Omega^1)$  with its image in  $H_{dR}^1(E)$  and choose  $\eta \in H_{dR}^1(E)$  such that  $\langle \omega, \eta \rangle_{dR} = 1$ . (Here the deRham pairing  $\langle, \rangle_{dR}$  is normalized so that for  $\omega \in H^0(E, \Omega^1)$ ,  $\langle \omega, \eta \rangle_{dR} = (\omega, \bar{\eta})_{\text{Serre}}$ , where  $\bar{\eta}$  is the image of  $\eta$  in  $H^1(E, \mathcal{O})$  and  $(, )_{\text{Serre}}$  is the Serre duality pairing.) We can then identify  $H^0(E, \Omega^1)$  (resp.  $H^1(E, \mathcal{O})$ ) with the cyclic module  $A/(F, V)$  by sending  $\omega$  (resp.  $\bar{\eta}$ ) to 1. Moreover,  $H_{dR}^1(E)$  is identified with  $A/(p, B^{-1}F + VB^{-1})$  by sending  $\eta$  to 1. Indeed,  $F(\eta) = B\omega$  (by definition of  $B$ ) and  $V(\eta) = -B^{1/p}\omega$ : since  $F$  and  $V$  are transposes for  $\langle, \rangle_{dR}$ , in the sense that  $\langle Vx, y \rangle_{dR} = \langle x, Fy \rangle_{dR}^{1/p}$  for all  $x, y$ , we have  $\langle V\eta, \omega \rangle_{dR} = 0$  and  $\langle V\eta, \eta \rangle_{dR} = -B^{1/p}$  and so  $V\eta = -B^{1/p}\omega$ . Thus we have a commutative diagram with exact rows and vertical isomorphisms

$$\begin{array}{ccccccc} 0 & \leftarrow & M(\text{Ker } F) & \leftarrow & M(\text{Ker } p) & \leftarrow & M(\text{Ker } V) & \leftarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \leftarrow & A/(F, V) & \leftarrow & A/(p, B^{-1}F + VB^{-1}) & \leftarrow & A/(F, V) & \leftarrow & 0. \\ & & 1 & \leftarrow & 1 & \leftarrow & B^{-1}F & \leftarrow & 1 \end{array}$$

Now if  $G' = \text{Ker}(B^{-1/p^2}F + VB^{-1/p^2} : W_2 \rightarrow W_2)$ , then  $M(G') \cong A/(p, B^{-1}F + VB^{-1})$  and taking into account the canonical identification  $M(\alpha_p) = A/(F, V)$ , the above sequence of  $A$ -modules induces a commutative diagram of finite, flat, unipotent group schemes

$$\begin{array}{ccccccc} 0 & \rightarrow & \text{Ker } F & \rightarrow & \text{Ker } p & \rightarrow & \text{Ker } V \rightarrow 0 \\ & & i' \downarrow & & \downarrow & & \downarrow j' \\ 0 & \rightarrow & \alpha_p & \xrightarrow{V} & G' & \xrightarrow{B^{-1/p^2}R} & \alpha_p \rightarrow 0 \end{array}$$

where the vertical maps are isomorphisms. Now the equation  $B^{\frac{p-1}{p^2}}(B^{-1}F + VB^{-1})B^{\frac{p-1}{p^2}} = B^{-1/p^2}F + VB^{-1/p^2}$  shows that  $G' \cong G$  via the map  $x \mapsto B^{\frac{p-1}{p^2}}x$  and it follows from the definition of the isomorphism  $H^1(E, \mathcal{O}) \cong M(\text{Ker } F)$  ([9], 4.3) that  $i'^*(dz) = B^{1/p}\omega$ ; since  $\omega$  and  $\eta$  are Serre dual,  $j' = i'^{\vee-1}$ , so putting  $i = B^{-1/p}i'$ ,  $j = B^{1/p}j'$ , we get a diagram

$$\begin{array}{ccccccc} 0 & \rightarrow & \text{Ker } F & \rightarrow & \text{Ker } p & \rightarrow & \text{Ker } V \rightarrow 0 \\ & & i \downarrow & & \downarrow & & \downarrow j \\ 0 & \rightarrow & \alpha_p & \xrightarrow{VB} & G & \xrightarrow{R} & \alpha_p \rightarrow 0 \end{array}$$

with  $i^*(dz) = \omega$  and  $j = i^{\vee-1}$ , as required.  $\square$

**Proposition 4.2.** *Let  $G$  be the group scheme  $\text{Ker}(B^{-1}F + VB^{-1} : W_2 \rightarrow W_2)$ , let  $R$  be a  $k$ -algebra and assume that  $H^1(R, \mathbf{G}_a) = 0$ . Then the long exact cohomology sequence associated to the short exact sequence  $0 \rightarrow \alpha_p \xrightarrow{VB} G \xrightarrow{R} \alpha_p \rightarrow 0$  of  $R$ -groups (obtained by base extension from  $k$ ) is canonically isomorphic to*

$$\begin{array}{ccccccc} 0 & \longrightarrow & \alpha_p(R) & \longrightarrow & G(R) & \longrightarrow & \alpha_p(R) \xrightarrow{\delta} \\ & & & & & & \\ & & & & R/R^p & \xrightarrow{V} & W_2(R)/(B^{-1}F + VB^{-1})W_2(R) \xrightarrow{BR} R/R^p \rightarrow 0 \end{array}$$

where  $\delta(x) = -B^{-1}x$ ,  $V(x) = (0, x)$ , and  $BR(x, y) = Bx$ .

**Proof:** The calculation of the cohomology groups is completely standard starting from the exact sequences  $0 \rightarrow \alpha_p \rightarrow \mathbf{G}_a \xrightarrow{F} \mathbf{G}_a \rightarrow 0$ ,  $0 \rightarrow \mathbf{G}_a \xrightarrow{V} W_2 \xrightarrow{R} \mathbf{G}_a \rightarrow 0$  and  $0 \rightarrow G \rightarrow W_2 \xrightarrow{B^{-1}F+VB^{-1}} W_2 \rightarrow 0$  of  $R$  group schemes. To check the maps, we use Čech cohomology.

If  $x \in \alpha_p(R)$ , then  $S = R[y]/(y^p - x)$  is a flat cover of  $R$ , and  $(y^p, -B^{\frac{p-1}{p}}y) \in G(S)$  maps to  $x$ . Its coboundary (a 1-cocycle in  $G(S \otimes S)$ ) comes from the  $S \otimes S$ -valued point  $-B^{-1/p} \otimes 1 + 1 \otimes B^{-1/p}$  of  $\alpha_p$  which corresponds to  $-B^{-1}x$  in  $R/R^p$ . This proves that the map  $\alpha_p(R) \rightarrow R/R^p$  is induced by  $x \mapsto -B^{-1}x$ . If  $\bar{x} \in R/R^p$  is represented by  $x \in R$ , then  $S = R[y]/(y^p - x)$  is a flat cover of  $R$  and the  $S \otimes S$ -valued point  $y \otimes 1 - 1 \otimes y$  of  $\alpha_p$  is a Čech cocycle representing the class of  $\bar{x}$  in  $H^1(R, \alpha_p)$ . It maps to the  $S \otimes S$ -valued point  $(0, By \otimes 1 - 1 \otimes By)$  of  $G$ . On the other hand,  $(B^{-1}F + VB^{-1})(0, By) = (0, x)$ , so the class of  $(0, x)$  in  $W_2(R)/(B^{-1}F + VB^{-1})W_2(R) \cong H^1(R, G)$  is represented by the  $S \otimes S$ -valued point  $(0, By \otimes 1) - (0, 1 \otimes By) = (0, By \otimes 1 - 1 \otimes By)$  of  $G$ . This proves that the map  $R/R^p \rightarrow W_2(R)/(B^{-1}F + VB^{-1})W_2(R)$  is induced by  $V$ . Similarly, if  $(x, y) \in W_2(R)$ , then associated class in  $H^1(R, G)$  is represented by a  $T \otimes T$ -valued point  $(z_1, z_2)$  of  $G$  where  $T = R[s, t]/(s^p - x, t^p + B^{p-1}s - B^p y)$  and  $z_1 = B^{1/p}s \otimes 1 - 1 \otimes B^{1/p}s$ . The image in  $H^1(R, \alpha_p)$  is thus represented by the  $T \otimes T$ -valued point  $z_1$  of  $\alpha_p$ , which corresponds to  $Bx$  in  $R/R^p$ . Thus the map  $W_2(R)/(B^{-1}F + VB^{-1})W_2(R) \rightarrow R/R^p$  is induced by  $BR$ . □

As a first application of these results, we consider the Selmer group for multiplication by  $p$  on a constant supersingular elliptic curve over a global field of characteristic  $p$ . The following proposition, analogous to 3.3, is again an easy exercise left to the reader.

**Proposition 4.3.** *Let  $E$  be a supersingular elliptic curve over a finite field  $k$ ,  $\omega$  a non-zero invariant differential on  $E$ , and put  $B = B(E, \omega) \in k$ . Let  $K$  be the function field of a smooth, irreducible, complete curve  $X$  over  $k$  and consider  $E$  as an elliptic curve over  $K$  by base extension. Then  $\text{Sel}(K, p) \cong \text{Ker}(B^{-1}F + VB^{-1} : H^1(X, W_2) \rightarrow H^1(X, W_2))$ . Moreover, there is an exact sequence  $0 \rightarrow H^1(X, \alpha_p) \rightarrow \text{Sel}(K, p) \rightarrow H^1(X, \alpha_p)$ .*

It is perhaps worth making this more explicit. We consider  $H^1(X, W_2)$  as a group of “repartitions”:  $H^1(X, W_2) \cong W_2(\mathbf{A})/(W_2(K) + W_2(\mathbf{A}(0)))$ , where  $\mathbf{A}$  denotes the adèles of  $K$  and  $\mathbf{A}(0)$  denotes the adèles all of whose coordinates  $(f_v, g_v)$  lie in the local ring at  $v$ . The condition that  $(f_v, g_v) \in H^1(X, W_2)$  lie in the kernel of  $B^{-1}F + VB^{-1}$  is that there exist global functions  $F, G \in K$  such that  $(F, G) - (B^{-1}F + VB^{-1})(f_v, g_v) \in W_2(R_v)$  for all  $v$ . Now

$$\begin{aligned} (F, G) - (B^{-1}F + VB^{-1})(f_v, g_v) \\ = \left( F - B^{-1}f_v^p, G - B^{-p}g_v^p - B^{-1}f_v - \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} F^i (-B^{-1}f_v^p)^{p-i} \right) \end{aligned} \quad (4.4)$$

The condition that 4.4 lie in  $W_2(R_v)$  for all  $v$  implies that  $(B^{-1}f_v^p) \in H^1(X, \mathcal{O})$  is trivial and that  $-B^{-1}f_v - \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} F^i (-B^{-1}f_v^p)^{p-i}$  (which is well-defined only up to the addition of  $p$ -powers) is an element of  $F(H^1(X, \mathcal{O}))$ , or equivalently, is orthogonal to  $H^0(X, \Omega^1)^{C=0}$  under Serre duality. Conversely, these two conditions clearly guarantee that an element  $(f_v) \in H^1(X, \mathcal{O})$  is in the image of  $\text{Sel}(K, p) \rightarrow H^1(X, \alpha_p) = H^1(X, \mathcal{O})^{F=0}$ . Note that the two conditions define an  $\mathbf{F}_{p^2}$ -vector space in  $H^1(X, \mathcal{O})$ , as expected.

In the case where  $X$  itself is a supersingular elliptic curve, there is only one exact

differential to check against, and we can take it be  $dF$ . To compute the pairing

$$\left( dF, -B^{-1}f_v - \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} F^i (-B^{-1}f_v^p)^{p-i} \right)_{Serre} \quad (4.5)$$

note that  $\frac{1}{p} \binom{p}{i} F^i (-B^{-1}f_v^p)^{p-i} dF$  is exact, and therefore has no residue, if  $i \not\equiv -1 \pmod{p}$ . Thus the pairing 4.5 is equal to  $B^{-1} \sum_v \text{Res}_v (f_v dF - f_v^p F^{p-1} dF)$ . From the definition of the modular form  $B$ , we have  $\sum_v \text{Res}_v f_v dF = B(X, \omega')/B(E, \omega)$  where  $\omega'$  is the differential on  $X$  Serre dual to  $(f_v)$ . Since  $\mathcal{C}(f_v^p F^{p-1} dF) = f_v dF$  and  $\text{Res}(\mathcal{C}\omega)^p = \text{Res}(\omega)$  for any  $\omega$ , the condition that the pairing 4.5 vanish is that  $B(X, \omega')/B(E, \omega)$  lie in the prime field  $\mathbf{F}_p$ . The existence of differentials  $\omega, \omega'$  for which this holds is implied by, but weaker than, the condition that  $X$  and  $E$  be isogenous over  $k$ . If they exist, the order of  $\text{Sel}(K, p)$  is  $qr$  where  $q$  is the order of  $k$  and  $r$  is the order of  $\mathbf{F}_{p^2} \cap k$ ; if not, the order of  $\text{Sel}(K, p)$  is  $q$ .

**5.  $p$ -descent** Let  $K$  be a field of characteristic  $p$  and  $E$  an ordinary elliptic curve over  $K$ . We assume that  $E^{(p)}$  has a fixed  $K$ -rational point of order  $p$ , so  $\text{Ker } V \cong \mathbf{Z}/p\mathbf{Z}$  and by Cartier duality  $\text{Ker } F \cong \mu_p$ . Then we have an exact sequence

$$0 \rightarrow \mu_p \rightarrow \text{Ker } p \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow 0 \quad (5.1)$$

over  $K$  which defines an element of  $\text{Ext}_K^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ .

**Lemma 5.2.**  $\text{Ext}_K^1(\mathbf{Z}/p\mathbf{Z}, \mu_p) \cong H^1(K, \mu_p)$ .

**Proof:** The exact sequence  $0 \rightarrow \mathbf{Z} \xrightarrow{p} \mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow 0$  induces

$$0 = \text{Hom}_K(\mathbf{Z}, \mu_p) \rightarrow \text{Ext}_K^1(\mathbf{Z}/p\mathbf{Z}, \mu_p) \rightarrow \text{Ext}_K^1(\mathbf{Z}, \mu_p)_p \rightarrow 0$$

and  $\text{Ext}_K^1(\mathbf{Z}, \mu_p)_p = H^1(K, \mu_p)_p = H^1(K, \mu_p)$ .  $\square$

Let  $q$  be the class in  $K^\times/K^{\times p} \cong H^1(K, \mu_p)$  defined by 5.1. There is an injection  $K^\times/K^{\times p} \hookrightarrow \Omega_K^1 (f \mapsto df/f)$  and it will be more convenient to work with  $dq/q$ . By general non-sense (e.g., the theory of the Yoneda pairing),  $q$  is the image of  $1 \in H^0(K, \mathbf{Z}/p\mathbf{Z}) \cong \text{Hom}_K(\mathbf{Z}/p\mathbf{Z}, \mathbf{Z}/p\mathbf{Z}) \rightarrow \text{Ext}_K^1(\mathbf{Z}/p\mathbf{Z}, \mu_p) \cong H^1(K, \mu_p)$ , i.e.,  $q$  is the image under the  $F$ -descent of the chosen point  $P \in E^{(p)}(K)$ . The suggestive notation for this differential will be justified in section 7.

From now on, we take  $K$  to be the function field of a curve over a finite field  $\mathbf{F}_q$  or one of its completions. In this case, the Kähler differentials  $\Omega_K^1$  are a 1-dimensional vector space over  $K$  (in the local case, we take the separated module of differentials) and we can define a map  $\theta : K \rightarrow K$  by  $df = \theta(f) \frac{dq}{q}$ , i.e.,  $\theta(f) = \frac{df}{dq/q} = q \frac{df}{dq}$ . The map  $\theta$  depends only on the class of  $q$  in  $K^\times/K^{\times p}$ , and we have  $\theta^p = \theta$ . Using  $\theta$ , we can define a subgroup of  $K$ : put  $K^0 = \text{Im } \theta = \{f | \mathcal{C}(f \frac{dq}{q}) = 0\}$  where  $\mathcal{C}$  is the Cartier operator; there is a direct sum decomposition  $K = K^0 \oplus K^p$ , where the projection to  $K^0$  is  $\theta^{p-1}$ .

**Proposition 5.3.** *Let  $K$  be the function field of a curve over a finite field or one of its completions and let  $E$  be an ordinary elliptic curve over  $K$  with a fixed non-trivial  $K$ -rational point of order  $p$  on  $E^{(p)}$ . If  $dq/q$ , the extension class of  $\text{Ker } p$ , is non-zero and  $K = K^0 \oplus K^p$  is the associated splitting of  $K$ , then  $H^1(K, \text{Ker } p) \cong K^0$ . If  $dq/q$  is zero, then  $\text{Ker } p \cong \mu_p \oplus \mathbf{Z}/p\mathbf{Z}$  and  $H^1(K, \text{Ker } p) \cong K^\times/K^{\times p} \oplus K/\wp(K)$ .*

**Proof:** The case where  $dq/q$  is zero is immediate, so assume  $dq/q \neq 0$ . Consider an element  $x \in H^1(K, \text{Ker } p)$  whose image in  $H^1(K, \mathbf{Z}/p\mathbf{Z})$  corresponds to  $(L, \sigma)$  where  $L/K$  is a Galois extension of degree  $p$  and  $\sigma$  is the image of 1 in  $\mathbf{Z}/p\mathbf{Z} \xrightarrow{\sim} G = \text{Gal}(L/K)$ . By the Hochschild-Serre spectral sequence, we have an isomorphism  $H^1(K, \text{Ker } p) \cong$

$H^1(L, \text{Ker } p)^G$ ; let  $y$  be the image of  $x$ . Since the image of  $y$  in  $H^1(L, \mathbf{Z}/p\mathbf{Z})$  is trivial, we can lift it to  $\omega \in H^1(L, \mu_p) \hookrightarrow \Omega_L^1$  with  $\mathcal{C}(\omega) = \omega$  and  $\omega$  is defined up to addition of multiples of  $dq/q$ . By the definition of the extension class, we have  $\omega^\sigma - \omega = dq/q$ . Conversely, given  $L, \sigma$ , and  $\omega \in \Omega_L^1$  with  $\omega^\sigma - \omega = dq/q$ , we can recover  $x \in H^1(K, \text{Ker } p)$ ;  $(L, \sigma, \omega)$  and  $(L, \sigma, \omega + dq/q)$  give the same  $x$ .

Now data  $(L, \sigma, \omega)$  as above are in 1-1 correspondence with elements of  $K^0$  as follows: consider the element  $z = \omega/(dq/q)$  of  $L$ . We have  $z^\sigma - z = 1$ , so  $z$  is an Artin-Schreier generator of  $L/K$  and so  $\wp(z) = z^p - z = x \in K$ . But since  $\omega$  came from  $H^1(K, \mu_p)$ , it is logarithmic, i.e.,  $\mathcal{C}(\omega) = \mathcal{C}(z \frac{dq}{q}) = z \frac{dq}{q}$ . Thus  $\mathcal{C}(x \frac{dq}{q}) = \mathcal{C}(z^p \frac{dq}{q} - z \frac{dq}{q}) = z \mathcal{C}(\frac{dq}{q}) - z \frac{dq}{q} = 0$ , and  $x$  is an element of  $K^0$ . Conversely, given an element  $x$  of  $K^0$ , we get an Artin-Schreier extension  $L$  by solving  $\wp(X) = x$ , and a differential  $\omega = X \frac{dq}{q}$ . Since  $\mathcal{C}(x \frac{dq}{q}) = 0$ , reversing the calculation above shows that  $X \frac{dq}{q}$  is logarithmic, so determines an element of  $H^1(L, \mu_p)$ . One easily checks that the map  $H^1(K, \text{Ker } p) \rightarrow K^0$  is a homomorphism, so we have the desired isomorphism.  $\square$

The above isomorphism is compatible with the extension structure in the sense that the diagram

$$\begin{array}{ccccccccc}
\mathbf{Z}/p\mathbf{Z} & \xrightarrow{\delta_0} & (\Omega_K^1)^{\mathcal{C}=1} & \xrightarrow{i} & K^0 & \xrightarrow{j} & K/\wp(K) & \xrightarrow{\delta_1} & \mathbf{Z}/p\mathbf{Z} \\
\uparrow & & \uparrow & & \uparrow & & \uparrow & & \uparrow \\
H^0(K, \mathbf{Z}/p\mathbf{Z}) & \rightarrow & H^1(K, \mu_p) & \rightarrow & H^1(K, \text{Ker } p) & \rightarrow & H^1(K, \mathbf{Z}/p\mathbf{Z}) & \rightarrow & H^2(K, \mu_p)
\end{array}$$

commutes, where the vertical maps are isomorphisms, and  $\delta_0(1) = \frac{dq}{q}$ ,  $i(\omega) = \wp(\omega/(dq/q))$ ,  $j(f) = \bar{f}$  and  $\delta_1(f) = [f, q] = \text{Tr}_{\mathbf{F}_q/\mathbf{F}_p} \text{Res}(f \frac{dq}{q})$ .

In order to complete the local  $p$ -descent, we have to determine the image  $E(K_v) \rightarrow H^1(K_v, \text{Ker } p)$ . We begin with an easy case.

**Proposition 5.4.** *Assume  $p > 3$  and  $E$  has potentially multiplicative reduction at  $v$ .*

*Then  $\text{Sel}(K_v, p) = K_v^0 \cap \wp(K_v)$ .*

**Proof:** This follows trivially from the exact sequence  $\text{Sel}(K_v, F) \rightarrow \text{Sel}(K_v, p) \rightarrow \text{Sel}(K_v, V)$  and the facts (3.1b) that  $\text{Sel}(K_v, V) = 0$  and  $\text{Sel}(K_v, F) = K_v^\times / K_v^{\times p}$  when  $E$  has potentially multiplicative reduction.  $\square$

To state the result for potentially good reduction we need some notation. Let  $R_v$  be the ring of integers of  $K_v$ , assume that  $E$  has good reduction at  $v$ , and choose a Néron differential  $\omega_{\text{Néron}}$  for  $E$  over  $R_v$ . Set  $\alpha = \omega_{\text{can}} / \omega_{\text{Néron}}$  so  $A(E, \omega_{\text{Néron}}) = \alpha^{p-1}$ . Recall the modular form  $B$ , which was determined only up to multiples of  $A$ , i.e.,  $B(E, \omega_{\text{Néron}})$  is determined up to addition of an element of  $A(E, \omega_{\text{Néron}})R_v$ . We define  $B = B(E, \omega_{\text{can}})$  as  $\alpha^{-(p+1)}B(E, \omega_{\text{Néron}}) \in K_v$ , which is well defined up to addition of an element of  $\alpha^{-(p+1)}A(E, \omega_{\text{Néron}})R_v = \alpha^{-2}R_v$ . If  $p > 3$  and  $E$  only has potentially good reduction, we can define  $B(E, \omega_{\text{can}})$  over an extension of degree dividing 6 where  $E$  has good reduction, and then note that  $B(E, \omega_{\text{Néron}})$  actually lies in  $K_v$ . (For example, because  $B \equiv -\frac{1}{12}E_{p+1} \pmod{p}$ .)

**Theorem 5.5.** *Assume  $p > 3$  and  $E$  has potentially good reduction at  $v$ . Then*

*$\text{Sel}(K_v, p) \subseteq K_v^0$  is equal to the group*

$$\left\{ f - \wp \left( \frac{\theta f}{B(E, \omega_{\text{can}})} \right) + \wp(g) \mid f, g \in K_v, v(f) > -v(\alpha^p), v(g) \geq -v(\alpha^{-p}dq/q) \right\} \cap K_v^0.$$

In the typical case  $v$  ordinary and  $v(dq/q) = 0$ , this group is just  $R_v^0 = R_v \cap K_v^0$ .

**Proof:** Since  $p > 3$ , after a separable extension of degree prime to  $p$   $E$  obtains good reduction. We will prove the theorem in the case where  $E$  has good reduction over  $R_v$ ; the general case follows easily from this by taking invariants (use 1.3).

Write  $\mathcal{S}$  for the group in the statement and first note that  $\mathcal{S}$  is independent of the choice of  $B = B(E, \omega_{can})$ . Indeed,  $B$  is determined up to an element of  $\alpha^{-2}R_v$  so changing  $B$  changes the second term by  $\wp(\theta f \alpha^{2p}x)$  with  $x \in R_v$ . But  $v(\theta f \alpha^{2p}x) \geq v(\frac{\alpha^p df}{\alpha^{-p} dq/q})$  and  $v(df) \geq -v(\alpha^p)$  so  $\wp(\theta f \alpha^{2p}x) = \wp(g)$  with  $v(g) \geq -v(\alpha^{-p} dq/q)$ , as needed.

Secondly,  $\text{Sel}(K_v, F)$  maps to  $\mathcal{S}$  ( $\omega \mapsto \wp(\omega/(dq/q))$ ) and the image is the set of elements of  $\mathcal{S}$  with  $f = 0$ ; moreover,  $\mathcal{S}$  maps surjectively to  $\text{Sel}(K_v, V)$  and the kernel is the image of  $\text{Sel}(K_v, F)$ . Indeed, the kernel consists of elements  $f - \wp(\theta f/B) + \wp(g) \in K^0$  such that  $v(f) > -v(\alpha^p)$ ,  $v(g) \geq -v(\alpha^{-p} dq/q)$ , and  $f = \wp(x)$ . Then  $v(x) > -v(\alpha)$  and the claim is that  $v(x + \frac{\theta x}{B}) \geq -v(\alpha^{-p} dq/q)$ . Now  $v(\frac{\theta x}{B} \alpha^{-p} dq/q) = v(u \alpha dx) \geq 0$  (where  $u$  is a unit) and  $v(x \alpha^{-p} dq/q) > v(\alpha^{-p-1} dq/q)$ . It follows from a consideration of the universal case that  $\alpha^{-p-1} dq/q$  has at worst a simple pole (use 2.4 of [16] and 7.7 of this paper), so the claim follows. Thus every element of the kernel of  $\mathcal{S} \rightarrow \text{Sel}(K_v, V)$  can be written as  $\wp(g)$  with  $v(g) \geq -v(\alpha^{-p} dq/q)$ , i.e., is in the image of  $\text{Sel}(K_v, F) \rightarrow \mathcal{S}$ .

With these reductions, we need only prove that any element of  $\text{Sel}(K_v, p)$  lies in  $\mathcal{S}$ . We will do this by applying the analysis 4.2 of the cohomology of the kernel of  $p$  on a supersingular curve. First we reformulate slightly the cohomology calculation of Milne alluded to in the proof of 3.1. Noting that  $G_{A,0} \cong \text{Ker}(\wp_A : \mathbf{G}_a \rightarrow \mathbf{G}_a)$  (where  $\wp_A(x) = x^p - Ax$ ), we have that for any  $R$  such that  $H^1(R, \mathbf{G}_a) = 0$ ,  $H^1(R, G_{A,0}) = R/\wp_A(R)$ . Moreover, if  $A = \alpha^{p-1}$  with  $\alpha$  a unit in  $R$ , then  $G_{A,0} \cong G_{1,0} = \mathbf{Z}/p\mathbf{Z}$  and the map  $R/\wp_A(R) \cong H^1(R, G_{A,0}) \rightarrow H^1(R, \mathbf{Z}/p\mathbf{Z}) \cong R/\wp(R)$  is  $f \mapsto \alpha^{-p} f$ . For any quotient  $R'$  of  $R$ , the restriction map  $H^1(R, G_{A,0}) \rightarrow H^1(R', G_{A,0})$  is the natural map  $R/\wp_A(R) \rightarrow R'/\wp_A(R')$ . If  $R$  is the ring of integers in a local field  $K$  of characteristic  $p$  (so  $H^1(R, \mathbf{G}_m) =$

0), then  $H^1(R, G_{0,A}) = (\Omega_R^1)^{C=A} = \{\omega \in \Omega_R^1 \mid \mathcal{C}(\omega) = A\omega\}$ . If  $A = \alpha^{p-1}$  with  $\alpha$  a unit in  $R$ , then  $G_{0,A} \cong G_{0,1} \cong \mu_p$  and the map  $(\Omega_R^1)^{C=A} \rightarrow R^\times/R^{\times p} \xrightarrow{\sim} (\Omega_R^1)^{C=1}$  is  $\omega \mapsto \alpha^p \omega$ . In particular, the image of the restriction  $H^1(R, G_{0,A}) \rightarrow (\Omega_K^1)^{C=1}$  is the set of differentials  $\omega$  with  $v(\omega) \geq v(\alpha^p)$ . (This last statement is actually what was proved by Milne; the preceding claims follow easily from an invariants argument.) If  $R'$  is a quotient of  $R$  in which  $A$  is zero, then  $H^1(R', G_{0,A}) = H^1(R', G_{0,0}) \cong R'/R'^p \cong (\Omega_{R'}^1)^{exact} = \{\omega \in \Omega_{R'}^1 \mid \omega = df \text{ for some } f \in R'\}$ , and the restriction map  $H^1(R, G_{0,A}) \rightarrow H^1(R', G_{0,A})$  is the natural map  $(\Omega_R^1)^{C=A} \rightarrow (\Omega_{R'}^1)^{exact}$ .

Now consider an element of  $K_v^0$  which is in  $\text{Sel}(K_v, p)$ ; we can write it in the form  $f + \wp(h)$  where  $v(f) > -v(\alpha^p)$ . Let  $(L, \sigma)$  be the image of  $f$  in  $\text{Sel}(K_v, V)$ , i.e.,  $L = K_v(X)$  where  $\wp(X) = f$  and  $X^\sigma = X + 1$ , and let  $S$  be the ring of integers of  $L$ . Then  $L/K_v$  is separable, so the restriction map  $H^1(K_v, \text{Ker } p) \rightarrow H^1(L, \text{Ker } p)$  is injective; the image of  $f + \wp(h)$  lies in the image of  $\text{Sel}(L, \text{Ker } f)$  and so corresponds to the differential  $(X + h) \frac{dq}{q}$ .

Choose a Néron differential  $\omega_{\text{Néron}}$  for  $E$  over  $R_v$  and set  $\alpha = \omega_{\text{can}}/\omega_{\text{Néron}}$ . Given this differential we can identify  $\text{Ker } F$  with  $G_{0,A}$  and  $\text{Ker } V$  with  $G_{A,0}$  over  $R_v$  where  $A = \alpha^{p-1}$ . Then the image of  $f + \wp(h) \in H^1(K_v, \mathbf{Z}/p\mathbf{Z})$  in  $H^1(R_v, G_{A,0}) \cong R_v/\wp_A(R_v)$  is the class of  $\alpha^p f$  and the image of the differential  $(X + h) \frac{dq}{q} \in (\Omega_L^1)^{C=1} \cong H^1(L, \mu_p)$  in  $H^1(S, G_{0,A}) \cong (\Omega_S^1)^{C=A}$  is  $\alpha^{-p}(X + h) \frac{dq}{q}$ .

We now subject the choice of Néron differential  $\omega_{\text{Néron}}$  to the following condition: over  $R_A = R_v/A(E, \omega_{\text{Néron}})$   $E$  is supersingular, so by simple vanishing of the Hasse invariant ([4] 12.4.3),  $E$  over  $R_A$  is constant, i.e.,  $E_{/R_A} \cong E_{/\mathbf{F}_q} \otimes_{\mathbf{F}_q} R_A$ . We require that under this isomorphism the differential  $\omega_{\text{Néron}}$  also be constant, i.e., come from a differential on

$E/\mathbb{F}_q$ . Clearly this does not affect the statement of the theorem.

With this choice of  $\omega_{Néron}$ , the entire situation  $(E, \text{Ker } F, \text{Ker } V, \text{Ker } p, \dots)$  is constant over  $R_A$ . Thus we can apply 4.2. In particular, if an element of  $H^1(R_A, \text{Ker } p)$  maps to  $x$  in  $H^1(R_A, \text{Ker } V)$ , then its restriction to  $H^1(S_A, \text{Ker } p)$  (where  $S_A = S/A(E, \omega_{Néron})$ ) comes from the element  $-B(E, \omega_{Néron})^{-1}dy \in H^1(S_A, \text{Ker } F) \cong (\Omega_{S_A}^1)^{exact}$  (up to elements of the image of  $H^0(S_A, G_{A,0})$ ) where  $y^p = \wp_A(y) = x$ . (Indeed,  $(B^{-1}x_1, x_2) \in W_2(R_A)/(B^{-1}F + VB^{-1})W_2(R_A)$  maps to  $x_1$  in  $H^1(R_A, \text{Ker } V) \cong R_A/R_A^p$  and is equivalent to  $(B^{-1}x_1, x_2) - (B^{-1}F + VB^{-1})(y_1, y_2) = (0, -B^{-1}y_1)$  in  $W_2(S_A)/(B^{-1}F + VB^{-1})W_2(S_A)$ , where  $y_1$  and  $y_2$  in  $S_A$  satisfy  $y_1^p = x_1$ ,  $(B^{-1}y_2)^p = x_2$ .) Now  $\Omega_{S_A}^1 \cong \Omega_S^1/(A\Omega_S^1 + SdA)$  (by the second exact sequence of Kähler differentials—or trivial calculation) so applying the above to  $f + \wp(h)$  we find

$$\alpha^{-p}(X + h)\frac{dq}{q} + B(E, \omega_{Néron})^{-1}d(\alpha X) = A\omega + x dA + dy$$

where  $\omega \in \Omega_S^1$ ,  $x \in S$ , and  $y \in R_v$  such that  $y^p \equiv 0 \pmod{A}$ . After a short calculation, one finds that

$$h - \frac{\theta f}{B} + X + B^{-1}X \frac{\theta \alpha}{\alpha} = (A\omega + x dA + dy)/(\alpha^{-p} dq/q).$$

Now the right hand side has valuation greater than or equal to that of  $(\alpha^{-p} dq/q)^{-1}$ , so if we show the claim that  $X + B^{-1}X \frac{\theta \alpha}{\alpha}$  has the same property then  $f + \wp(h)$  can be written  $f - \wp(\theta f/B) + \wp(g)$  where  $v(g) \geq -v(\alpha^{-p} dq/q)$ .

If  $f$  represents a class in  $P_{K_v}^{[0]}$ , then the claim is clear, so we can assume not, which means that  $L/K$  is totally ramified. Let  $w$  be the normalized valuation of  $L$ . Under the coboundary map  $H^0(R_v, G_{A,0}) \rightarrow H^1(R_v, G_{0,A})$ ,  $\alpha$  maps to  $\alpha^{-p} dq/q$ . On the other

hand, by 4.2, in  $H^0(R_A, G_{A,0}) \rightarrow H^1(R_A, G_{0,A})$ ,  $\alpha$  maps to  $-B(E, \omega_{Néron})^{-1} d\alpha$ . Thus,  $-\alpha^{-p} dq/q + B(E, \omega_{Néron})^{-1} d\alpha = A\omega + x dA$  with  $\omega \in \Omega_{R_v}^1$ ,  $x \in R_v$  (since  $\Omega_{R_A}^1 = \Omega_{R_v}^1 / (A\Omega_{R_v}^1 + R_v dA)$ ) so  $B^{-1} \frac{d\alpha/\alpha}{dq/q} + 1 = (A\omega + x dA) / (\alpha^{-p} dq/q)$ . The claim now follows from the facts that  $w(XA\omega) \geq w(XA) \geq 0$  and  $w(Xx dA) \geq w(X dA) \geq 0$  where  $w$  is the valuation on  $L$ . Indeed,  $w(X) = v(f) > -pv(\alpha) = -w(\alpha) \geq -w(A)$ , and  $w(dA) \geq w(A)$  as  $p|w(A)$ .

This completes the proof of theorem 5.5.  $\square$

**6. Remarks on the cases  $p = 2$  and  $3$**  First note that the descent results 3.1 and 5.5 hold as stated (with the same proofs) in the case that  $E/K_v$  obtains good or split multiplicative reduction over an extension of degree prime to  $p$ . In general, if  $E$  has good reduction over  $L_v$  with  $G = \text{Gal}(L_v/K_v)$ , then the Hochschild-Serre spectral sequence gives  $0 \rightarrow \text{Sel}(K_v, F) \rightarrow \text{Sel}(L_v, F)^G$  and  $\text{Sel}(K_v, V) \subseteq \phi^{-1}(\text{Sel}(L_v, V)^G)$  where  $\phi : \text{Sel}(K_v, V) \rightarrow \text{Sel}(L_v, V)$  and  $\text{Ker } \phi \subseteq H^1(L_v/K_v, \text{Ker } V)$  is a finite group. Now these two upper bounds also yield lower bounds, as by Tate duality  $\text{Sel}(K_v, F)$  and  $\text{Sel}(K_v, V)$  are orthogonal complements under the Artin-Schreier pairing  $K_v/K_v^{\times p} \times K_v/\wp(K_v) \rightarrow \mathbf{Z}/p\mathbf{Z}$ . To determine the local Selmer groups exactly then just requires a finite amount of computation using Voloch's explicit formulas for 2 and 3 descents [18].

If  $p = 2$  and  $E$  is represented as a plane cubic

$$y^2 + a_1xy = x^3 + a_2x^2 + a_6$$

then the Hasse invariant  $A = a_1$  and the canonical point  $P$  of order 2 on  $E^{(2)}$  has coordinates  $(0, a_6)$ . Using  $P$  to identify  $\text{Ker } V \cong \mathbf{Z}/p\mathbf{Z}$ , we have  $\omega_{can} = dx/a_1y$  and

$dq/q = da_6/a_6$ . The descent maps are

$$\begin{aligned}
 E^{(2)}(K_v) \rightarrow K_v^\times / K_v^{\times 2} & \quad (x, y) \mapsto \begin{cases} 1 & \text{if } (x, y) = 0 \\ a_6 & \text{if } (x, y) = P \\ x & \text{otherwise} \end{cases} \\
 E(K_v) \rightarrow K_v / \wp(K_v) & \quad (x, y) \mapsto (x + a_2) / a_1^2 \\
 E(K_v) \rightarrow K_v^0 & \quad (x, y) \mapsto a_6 / (a_1 x)^2 + \wp(\theta x / x).
 \end{aligned} \tag{6.1}$$

If  $p = 3$  and  $E$  is represented as a plane cubic

$$y^2 = x^3 + a_2 x^2 + a_6$$

then the Hasse invariant  $A = a_2 = \alpha^2$  and the canonical point  $P$  of order 3 on  $E^{(3)}$  has coordinates  $(-a_6, a_6 \alpha^3)$ . Using  $P$  to identify  $\text{Ker } V \cong \mathbf{Z}/p\mathbf{Z}$ , we have  $\omega_{can} = \alpha^{-1} dx / 2y$  and  $dq/q = da_6/a_6$ . The descent maps are

$$\begin{aligned}
 E^{(3)}(K_v) \rightarrow K_v^\times / K_v^{\times 3} & \quad (x, y) \mapsto \begin{cases} 1 & \text{if } (x, y) = 0 \\ a_6 & \text{if } (x, y) = P \\ (\alpha^3 y + a_2^3 x)^{-1} & \text{otherwise} \end{cases} \\
 E(K_v) \rightarrow K_v / \wp(K_v) & \quad (x, y) \mapsto y / \alpha^3 \\
 E(K_v) \rightarrow K_v^0 & \quad (x, y) \mapsto (a_6 y) / (\alpha^3 x^3) - \wp(\theta y / \alpha x).
 \end{aligned} \tag{6.2}$$

Since the local Selmer groups sit in an exact sequence

$$\text{Sel}(K_v, F) \rightarrow \text{Sel}(K_v, p) \rightarrow \text{Sel}(K_v, V) \rightarrow 0,$$

to determine  $\text{Sel}(K_v, p)$  it suffices to apply the  $p$ -descent map to each element of a set of points of  $E(K_v)$  mapping onto the finite group  $\text{Sel}(K_v, V)$ . We will apply these formulae to some example curves in section 8.

**7. Applications to Igusa curves** In this section we will consider the universal case for  $p$ -descents, namely the case where  $K$  is the function field of an Igusa curve and  $E$  is the universal curve over  $K$  studied in [16]. The first five sections of [1] provide a useful summary of much of the background on modular forms and Igusa curves we will need.

Fix a prime  $p$  and a positive integer  $N$  relatively prime to  $p$ ; for simplicity we assume  $N > 4$ . (The case  $N$  arbitrary,  $p > 3$  can be easily handled by taking invariants; the cases  $p = 2$ ,  $N = 3$  and  $p = 3$ ,  $N = 1, 2, 4$  will be treated directly in section 8.) Let  $X_1(N)$  be the moduli space for “generalized elliptic curves over  $\mathbf{F}_p$ -algebras together with an injection  $\mathbf{Z}/N\mathbf{Z} \hookrightarrow E$  whose image meets every irreducible component of each geometric fiber” (i.e. generalized elliptic curves with  $\Gamma_1(N)$ -structure) and let  $Ig_1(N)$  be the moduli space for “generalized elliptic curves over  $\mathbf{F}_p$ -algebras together with a  $\Gamma_1(N)$ -structure and a point  $P \in E^{(p)}$  which generates the kernel of the Verschiebung  $V : E^{(p)} \rightarrow E$ ” (i.e., elliptic curves with  $\Gamma_1(N)$ -structure and Igusa structure of level  $p$ ). The curves  $X_1(N)$  and  $Ig_1(N)$  are smooth, proper, and geometrically irreducible over  $\mathbf{F}_p$ ; ignoring the Igusa structure induces a finite map

$$pr : Ig_1(N) \rightarrow X_1(N)$$

of degree  $p - 1$ . The map  $pr$  is totally ramified at the points parametrizing supersingular elliptic curves; naming the points parametrizing singular elliptic curves the *cusps*, and the remaining points *ordinary*,  $pr$  is completely split at the cusps and unramified at the ordinary points. Over  $X_1(N)$  we have a universal (generalized) elliptic curve

$$\pi : \mathcal{E} \rightarrow X_1(N)$$

which is equipped with a canonical point of order  $N$ . When pulled back to  $Ig_1(N)$ ,  $\mathcal{E}$  has a canonical Igusa structure, i.e., a non-trivial point of order  $p$  on  $\mathcal{E}^{(p)}$ .

Let  $K = \mathbf{F}_q(Ig_1(N))$  be the function field of  $Ig_1(N)$  over  $\mathbf{F}_q$  and let  $E/K$  be the generic fiber of the universal curve over  $Ig_1(N)$ . Then  $E$  is an ordinary elliptic curve over  $K$ , and it has split multiplicative reduction at the cuspidal places, has good, supersingular reduction at the supersingular places, and has good ordinary reduction elsewhere. If  $P \in E^{(p)}(K)$  is the canonical point of order  $p$  on  $E^{(p)}$ , we fix an isomorphism  $(\mathbf{Z}/p\mathbf{Z})^\times \cong \text{Gal}(K/\mathbf{F}_q(X_1(N)))$  by requiring  $\langle a \rangle P = a^{-1}P$ .

If  $\Omega_{\mathcal{E}/X_1(N)}^{1 \text{ reg}}$  denotes the sheaf of regular differentials on  $\mathcal{E}$  over  $X_1(N)$  (i.e., the relative dualizing sheaf), then  $\underline{\omega} = \pi_* \Omega_{\mathcal{E}/X_1(N)}^{1 \text{ reg}}$  is an invertible sheaf on  $X_1(N)$ . We define the space  $M_k(\Gamma_1(N), \mathbf{F}_q)$  of modular forms of weight  $k$  for  $\Gamma_1(N)$  over  $\mathbf{F}_q$  as  $H^0(X_1(N) \otimes \mathbf{F}_q, \underline{\omega}^{\otimes k})$ . Equivalently,  $M_k(\Gamma_1(N), \mathbf{F}_q)$  is the set of functorial assignments of  $k$ -fold differentials to elliptic curves with  $\Gamma_1(N)$ -structures over  $\mathbf{F}_q$ -algebras. The subspace of cusp forms  $S_k(\Gamma_1(N), \mathbf{F}_q) = H^0(X_1(N) \otimes \mathbf{F}_q, \underline{\omega}^{\otimes k}(\text{cusps}))$  consists of those forms vanishing at the cusps. For example, the Hasse invariant  $A$  is an element of  $M_{p-1}(\Gamma_1(N), \mathbf{F}_p)$  which vanishes simply at the supersingular points and is a generating section elsewhere.

We recall that the field  $K$  is intimately related to modular forms in characteristic  $p$ . Namely, let  $R$  be the affine ring of  $Ig_1(N) - \{\text{supersingular points}\}$  over  $\mathbf{F}_q$ ; there is a surjective map

$$\bigoplus_{k=0}^{\infty} M_k(\Gamma_1(N), \mathbf{F}_q) \rightarrow R \quad (7.1)$$

whose kernel is the ideal generated by  $A - 1$  where  $A$  is the Hasse invariant. The map is defined as follows: on  $E/K$  there is a canonical invariant differential form  $\omega_{can}$  intro-

duced in section 3;  $\omega_{can}$  can be viewed as a section of  $\underline{\omega}$  (the pull back of  $\underline{\omega}$  on  $X_1(N)$  to  $Ig_1(N)$ ). Given a modular form  $f$  of weight  $k$ ,  $f(E)$  defines a section of  $\underline{\omega}^{\otimes k}$  on  $Ig_1(N)$  and  $f(E, \omega_{can}) = f(E)/\omega_{can}^k$  is an element of  $K$ . We have  $\langle a \rangle^* \omega_{can} = a^{-1} \omega_{can}$ , so  $\langle a \rangle f(E, \omega_{can}) = a^k f(E, \omega_{can})$ . Since  $\omega_{can}$  vanishes simply as a section of  $\underline{\omega}$  at the supersingular points and is a generating section elsewhere,  $f(E, \omega_{can})$  has poles of order no worse than  $k$  at the supersingular points and is regular elsewhere. We define the *filtration* of an element of  $R$  to be the smallest integer  $k$  such that it comes from modular forms of weights less than or equal to  $k$ . Equivalently,  $\text{fil}(f) = \max_v \text{supersingular} \{-v(f)\}$ . The ring  $R$  also inherits a grading by weights  $(\text{mod } p-1)$  which corresponds to its decomposition into eigenspaces for  $\text{Gal}(K/\mathbf{F}_q(X_1(N))) \cong (\mathbf{Z}/p\mathbf{Z})^\times$ . If an element  $f$  has a weight, then we have  $\text{fil}(f) \equiv \text{wt}(f) \pmod{p-1}$ .

Using 7.1, we define elements  $Q = E_4(E, \omega_{can})$ ,  $R = E_6(E, \omega_{can})$ , and  $\Delta = \Delta(E, \omega_{can})$  of  $K$ . These are related by  $1728\Delta = Q^3 - R^2$  and the  $j$  invariant of  $E$  is  $j = Q^3/\Delta$ . We also define a differential  $dq/q$  as  $(3RdQ - 2QdR)/(Q^3 - R^2)$  when  $p > 3$  and as  $d\Delta/\Delta = -dj/j$  when  $p = 2$  or  $3$ . (We will prove momentarily that this  $dq/q$  is the  $dq/q$  of section 5.) The divisors of  $\Delta$  and  $dq/q$  are given by  $(\Delta) = C - 12 \sum_v \text{supersingular} [v]$  and  $(dq/q) = p \sum_v \text{supersingular} [v] - \sum_v \text{cuspidal} [v]$  where  $C$  is an effective divisor supported on the cusps.

As for differentials, Serre proved (see [1] or [4] 12.8.8) that the map  $f \rightarrow f(E, \omega_{can})dq/q$  gives isomorphisms

$$\bigoplus_{k=2}^p S_k(\Gamma_1(N), \mathbf{F}_q) \cong H^0(Ig_1(N) \otimes \mathbf{F}_q, \Omega^1)$$

and

$$\bigoplus_{k=2}^p M_k(\Gamma_1(N), \mathbf{F}_q) \cong H^0(Ig_1(N) \otimes \mathbf{F}_q, \Omega^1(\text{cusps})). \quad (7.2)$$

The image of  $M_k(\Gamma_1(N), \mathbf{F}_q)$  lies in the subspace of differentials with  $\langle a \rangle^* \omega = a^{k-2} \omega$  for all  $\langle a \rangle \in (\mathbf{Z}/p\mathbf{Z})^\times \cong \text{Gal}(K/\mathbf{F}_p(X_1(N)))$  and the differential  $dq/q$  is the image of  $A \in M_{p-1}(\Gamma_1(N), \mathbf{F}_p)$ .

There are a number of operators on the ring of modular forms and on the curve  $Ig_1(N)$ . In particular, we have correspondences  $T_\ell$  for  $\ell \nmid pN$ ,  $U_\ell$  for  $\ell|N$ ,  $U = U_p$ ,  $V = V_p$ , a derivation  $\theta$ , and automorphisms  $\langle a \rangle = \langle a \rangle_p$  for  $a \in (\mathbf{Z}/p\mathbf{Z})^\times \cong \text{Gal}(Ig_1(N)/X_1(N))$  (which have already been alluded to) and  $\langle a \rangle_N$  for  $a \in (\mathbf{Z}/N\mathbf{Z})^\times$ . On  $q$ -expansions,

$$\begin{aligned} U &: \sum a_n q^n \mapsto \sum a_{pn} q^n \\ V &: \sum a_n q^n \mapsto \sum a_n q^{pn} \\ \theta &: \sum a_n q^n \mapsto q \frac{d}{dq} \sum a_n q^n = \sum n a_n q^n \end{aligned}$$

and  $\theta^{p-1} = 1 - VU$ . We again refer to [1] for definitions of  $T_\ell$  and  $U_\ell$  and proofs that the maps 7.1 and 7.2 are compatible with all of these operators. Among these compatibilities, we note the following: let  $\sigma$  be the absolute Frobenius on modular forms in characteristic  $p$  (whose effect on  $q$ -expansions is  $\sum a_n q^n \mapsto \sum a_n^p q^n$ ). Then the Cartier operator on  $H^0(Ig_1(N), \Omega^1(\text{cusps}))$  goes over to  $\sigma^{-1}U$  on modular forms, and the absolute Frobenius of  $R$  goes over to  $\sigma V$  on modular forms. In particular,  $\mathcal{C}(dq/q) = dq/q$ .

For the rest of this paper, we refer to the algebra generated over  $\mathbf{F}_p$  by the  $T_\ell$  for  $\ell \nmid pN$ ,  $U_\ell$  for  $\ell|N$ , and  $\langle a \rangle_N$  for  $a \in (\mathbf{Z}/N\mathbf{Z})^\times$  (but *not*  $U_p$  or  $V_p$ ) as the Hecke algebra. If  $M$  is a module for the Hecke algebra, we denote by  $M[n]$  the twisted module, where  $T_\ell(f[n]) = \ell^n T_\ell f$ ,  $U_\ell(f[n]) = \ell^n U_\ell f$ , and  $\langle a \rangle_N f[n] = \langle a \rangle_N f$ ; for completeness, we define

$Uf[n] = Uf$ ,  $Vf[n] = Vf$  and  $\sigma f[n] = \sigma f$ . The relations  $T_\ell\theta = \ell\theta T_\ell$ ,  $U_\ell\theta = \ell\theta U_\ell$ , and  $\theta\langle a \rangle_N = \langle a \rangle_N\theta$  show that  $\theta$  maps  $S_k(\Gamma_1(N), \mathbf{F}_q)[1]$  to  $S_{k+p+1}(\Gamma_1(N), \mathbf{F}_q)$ . Serre has shown ([13]) that under the isomorphism

$$H^1(Ig_1(N) \otimes \mathbf{F}_q, \mathcal{O}) \cong H^0(Ig_1(N) \otimes \mathbf{F}_q, \Omega^1)^* \cong \bigoplus_{k=2}^p S_k(\Gamma_1(N), \mathbf{F}_q)^*$$

the correspondences  $T_\ell$  and  $U_\ell$  of  $Ig_1(N)$  go over to  $(\ell^{p-k}T_\ell)^t$  and  $(\ell^{p-k}U_\ell)^t$  on  $S_k(\Gamma_1(N), \mathbf{F}_q)^*$  (where  $*$  denotes the  $\mathbf{F}_q$ -linear dual (or  $\mathbf{F}_p$ -linear dual—see below) and  $^t$  denotes the transpose). In other words, we have isomorphisms of Hecke modules

$$H^1(Ig_1(N) \otimes \mathbf{F}_q, \mathcal{O}) \cong \bigoplus_{k=2}^p S_k(\Gamma_1(N), \mathbf{F}_q)[p-k]^*. \quad (7.3)$$

As for the action of Frobenius on  $H^1(Ig_1(N) \otimes \mathbf{F}_q, \mathcal{O})$ , the following two lemmas (whose proofs are immediate) show that it goes over to  $(\sigma^{-1}U)^t$  on modular forms.

**Lemma 7.4.** *If  $E/F$  is a finite separable extension of fields and  $\langle, \rangle : V \times W \rightarrow E$  is a non-degenerate pairing of  $E$  vector spaces, then  $\text{Tr}_{E/F} \circ \langle, \rangle$  is a non-degenerate pairing of  $F$  vector spaces.*

**Lemma 7.5.** *Let  $X$  be a curve over a finite field  $\mathbf{F}_q$  and let  $\langle, \rangle : H^0(X, \Omega_X^1) \times H^1(X, \mathcal{O}_X) \rightarrow \mathbf{F}_q$  be the Serre duality pairing. Then the transpose of the Frobenius on  $H^1(X, \mathcal{O}_X)$  with respect to  $\text{Tr}_{\mathbf{F}_q/\mathbf{F}_p} \langle, \rangle$  is  $\mathcal{C}$ , the Cartier operator.*

We now turn to the Selmer groups. Recall the isogenies  $F : E \rightarrow E^{(p)}$ ,  $V : E^{(p)} \rightarrow E$ , and  $p = V \circ F : E \rightarrow E$  of the universal  $E$  over  $K$ .

**Theorem 7.6.**  $\text{Sel}(K, F) \cong \mathbf{F}_p \frac{dq}{q} \subseteq (\Omega_K^1)^{\mathcal{C}}$ .

**Proof:** The divisor of  $\Delta$  is  $C - 12 \sum_v \text{supersingular}[v]$  where  $C$  is an effective divisor supported on the cusps. Thus the divisor  $D$  in 3.2 is  $\sum_v \text{cuspidal}[v] - p \sum_v \text{supersingular}[v]$ ; in

particular,  $\deg D = 2-2g$  where  $g$  is the genus of  $Ig_1(N)$  ([4], 12.9.4). In fact,  $(dq/q) = -D$ , so  $H^0(Ig_1(N), \Omega^1(D))$  is one dimensional over  $\mathbf{F}_q$  spanned by  $dq/q$ . Since  $\mathcal{C}(dq/q) = dq/q$ , we have  $H^0(Ig_1(N), \Omega^1(D))^{\mathcal{C}} = \mathbf{F}_p \frac{dq}{q}$  which according to 3.2 is what was to be shown.  $\square$

**Corollary 7.7.** *The extension class of the kernel of  $p$  on  $E$  is equal to  $dq/q$ .*

Thus  $\theta$  on  $R$  corresponds to  $\theta$  on modular forms.

It is possible to analyze the Selmer group for  $V$  using the class field theoretic description of 3.2, however we will proceed differently. First note that the isomorphism  $H^1(K, \text{Ker } V) \cong K/\wp(K)$  (and thus the natural imbedding  $\text{Sel}(K, V) \subseteq K/\wp(K)$ ) is *not* equivariant for the action of  $\text{Gal}(K/\mathbf{F}_q(X_1(N)))$ :  $\text{Ker } V$  is isomorphic to  $\mathbf{Z}/p\mathbf{Z}$  only over  $K$ . If for any  $\text{Gal}(K/\mathbf{F}_q(X_1(N)))$ -module  $M$ , we write  $M^{(k)}$  for the subgroup where  $\langle a \rangle$  acts by  $a^k$ , then using the fact that  $\langle a \rangle P = a^{-1}P$  for the canonical point  $P \in E^{(p)}(K)$  we find that  $\text{Sel}(K, V)^{(k-1)} \hookrightarrow (K/\wp(K))^{(k)}$ .

Introduce a filtration on  $\text{Sel}(K, V)$  as follows: for any positive integer  $j$  let  $\text{Sel}(K, V)_j$  be the subgroup of classes  $\bar{f}$  represented by elements  $f \in R$  of filtration  $\leq j$ . One has  $\text{Sel}(K, V)_j \cong \bigoplus_{k=1}^{p-1} \text{Sel}(K, V)_j^{(k-1)}$ . Write  $M_k(\Gamma_1(N), \mathbf{F}_q)^{\wp\text{-cusps}}$  for the subset of  $f \in M_k(\Gamma_1(N), \mathbf{F}_q)$  such that the value of  $f(E, \omega_{can})$  at each cusp lies in  $\wp(\mathbf{F}_q)$ ; define  $M_k(\Gamma_1(N), \mathbf{F}_q)^{\mathbf{F}_p\text{-cusp}}$  similarly.

**Theorem 7.8.**

- a)  $\text{Sel}(K, V)_0 = 0$  and  $\text{Sel}(K, V)_{p^2} = \text{Sel}(K, V)$ .
- b) For  $1 \leq k \leq p-1$  we have isomorphisms

$$\text{Sel}(K, V)_{p-1}^{(k-1)} \cong M_k(\Gamma_1(N), \mathbf{F}_q)^{\wp\text{-cusp}}.$$

c) Set  $k' = p + 1 - k$ . For  $1 \leq k \leq p - 1$ , we have inclusions

$$\mathrm{Sel}(K, V)^{(k-1)} / \mathrm{Sel}(K, V)_{p-1}^{(k-1)} \hookrightarrow S_{k'}(\Gamma_1(N), \mathbf{F}_q)[k-1]^*$$

where  $*$  denotes  $\mathbf{F}_p$ -linear dual. This map is an isomorphism when  $k \neq 1$ . When

$k = 1$ , the image is the orthogonal complement of

$$(\sigma^{-1}U - 1)(AM_1(\Gamma_1(N), \mathbf{F}_q)^{\mathbf{F}_p\text{-cusp}}) \subseteq S_p(\Gamma_1(N), \mathbf{F}_q).$$

d) For  $1 \leq k \leq p$  there are maps

$$S_{k'}(\Gamma_1(N), \mathbf{F}_q)[k-1] \rightarrow \mathrm{Sel}(K, V)^{(k-1)}.$$

The kernel of the induced map  $S_{k'}(\Gamma_1(N), \mathbf{F}_q)[k-1] \rightarrow \mathrm{Sel}(K, V)^{(k-1)} / \mathrm{Sel}(K, V)_{p-1}^{(k-1)}$

is the set of  $f \in S_{k'}(\Gamma_1(N), \mathbf{F}_q)[k-1]$  which have a companion (i.e., for which there

exists  $g \in S_k(\Gamma_1(N), \mathbf{F}_q)$  such that  $\theta^k f = \theta g$ ).

Note that in d), we do not require that  $f$  and  $g$  be eigenforms.

**Proof:** a)  $\mathrm{Sel}(K, V)_0$  is clearly zero, since the only elements of filtration 0 are constants, and the local conditions at the cusps imply that they must lie in  $\wp(\mathbf{F}_q)$ . Now take any element  $\bar{f} \in \mathrm{Sel}(K, V)$  represented by  $f \in K$  and for every place  $v$ , write  $f = f_v + \wp(g_v)$  where  $v(f_v) > -p$  at supersingular  $v$  and  $v(f_v) \geq 0$  elsewhere. Then  $\bar{f} \in \mathrm{Sel}(K, V)_{pj}$  for any  $j$  if and only if  $(g_v) \in H^1(Ig_1(N), \mathcal{O}(jD)) \cong \mathbf{A}_K / (K + \mathbf{A}_K(jD))$  is zero for  $D = \sum_{v \text{ supersingular}} [v]$ . (Here  $\mathbf{A}_K$  denotes the adèles of  $K$  and  $\mathbf{A}_K(jD) = \{(a_v) | v(a_v) \geq -jn_v\}$  when  $D = \sum n_v [v]$ .) But for  $D = \sum_{v \text{ supersingular}} [v]$ ,  $\deg pD > 2g - 2$  so  $H^1(Ig_1(N), \mathcal{O}(pD)) = 0$  and  $\mathrm{Sel}(K, V)_{p^2} = \mathrm{Sel}(K, V)$ .

b) This is clear from 7.1 and the fact that any element of filtration  $\leq p - 1$  whose values at the cusps lie in  $\wp(\mathbf{F}_q)$  defines a class in  $\mathrm{Sel}(K, V)$ .

c) We have  $H^1(Ig_1(N), \mathcal{O})^{(k)} \cong S_{k'}(\Gamma_1(N), \mathbf{F}_q)[k-1]^*$  so it will suffice to define a map  $\text{Sel}(K, V)^{(k-1)}/\text{Sel}(K, V)_{p-1}^{(k-1)} \hookrightarrow H^1(Ig_1(N), \mathcal{O})^{(k)}$ . Given  $\bar{f} \in \text{Sel}(K, V)^{(k-1)}$  represented by  $f \in K$ , for every place  $v$  of  $K$  write  $f = f_v + \wp(g_v)$  where  $f_v, g_v \in K_v$ ,  $v(f_v) > -p$  at supersingular  $v$ ,  $v(f_v) \geq 0$  elsewhere. We can choose  $f_v$  and  $g_v$  such that  $\langle a \rangle f_v = a^k f_v$  and  $\langle a \rangle g_v = a^k g_v$  for all  $a \in (\mathbf{Z}/p\mathbf{Z})^\times$ . The function  $g_v$  is determined up to elements of  $R_v$  and  $(g_v)$  defines a class in  $H^1(Ig_1(N), \mathcal{O})^{(k)}$  which is zero (as in a)) if and only if  $\bar{f} \in \text{Sel}(K, V)_{(p-1)}^{(k-1)}$ . Now the image of  $\text{Sel}(K, V)^{(k-1)} \rightarrow H^1(Ig_1(N), \mathcal{O})^{(k)}$  is exactly the kernel of the map

$$H^1(Ig_1(N), \mathcal{O})^{(k)} \rightarrow \frac{H^1(Ig_1(N), \mathcal{O}((p-1)D - \text{cusps}))}{\bigoplus_{\text{cuspidal } v} \wp(R_v)}$$

$$(g_v) \mapsto (\wp(g_v))$$

where  $D = \sum_{\text{supersingular } v} [v]$  and  $\text{cusps} = \sum_{\text{cuspidal } v} [v]$ . The latter group is isomorphic to  $(M_1(\Gamma_1(N), \mathbf{F}_q)^{\mathbf{F}_p - \text{cusp}})^*$  so if  $k \neq 1$  the map is zero and  $\text{Sel}(K, V)^{(k-1)} \rightarrow H^1(Ig_1(N), \mathcal{O})^{(k)}$  is surjective. If  $k = 1$ , the image is orthogonal (using 7.5) to  $(\sigma^{-1}U - 1)(AM_1(\Gamma_1(N), \mathbf{F}_q)^{\mathbf{F}_p - \text{cusp}})$  as claimed.

d) By the theory of  $\theta$ -cycles ([2]), for  $f \in S_{k'}(\Gamma_1(N), \mathbf{F}_q)$ ,  $h = \theta^{k-1}f(E, \omega_{\text{can}})$  has weight congruent to  $k$  and filtration  $pk$ ; moreover,  $\theta h$  has filtration at most  $k + p + 1$ . This implies that in terms of a suitable coordinate  $t_v$  at a supersingular place  $v$  (suitable means  $\langle a \rangle t_v = a^{-1}t_v$ )  $h = bt_v^{-pk} + ct_v^{-k} + \dots$ , so  $h$  defines a class in  $\text{Sel}(K, V)$ . Now  $h$  is zero in  $\text{Sel}(K, V)/\text{Sel}(K, V)_{p-1}$  if and only if  $h = g_1(E, \omega_{\text{can}}) + \wp(g_2(E, \omega_{\text{can}}))$  with  $g_1, g_2 \in S_k(\Gamma_1(N), \mathbf{F}_q)$ . In this case,  $\theta^k f(E, \omega_{\text{can}}) = \theta h = \theta g_1(E, \omega_{\text{can}}) - \theta g_2(E, \omega_{\text{can}})$  which says exactly that  $g_1 - g_2$  is a companion to  $f$ . Conversely, if  $f \in S_{k'}(\Gamma_1(N), \mathbf{F}_q)$  and  $g \in S_k(\Gamma_1(N), \mathbf{F}_q)$  are companions and  $k \neq 1$ , then  $\theta^{k-1}f(E, \omega_{\text{can}}) = \theta^{p-1}g(E, \omega_{\text{can}}) = g(E, \omega_{\text{can}}) - VUg(E, \omega_{\text{can}}) = g(E, \omega_{\text{can}}) - (\sigma^{-1}Ug(E, \omega_{\text{can}}))^p$ . Since  $\sigma^{-1}Ug(E, \omega_{\text{can}})$

has filtration at most  $k$ ,  $\theta^{k-1}f(E, \omega_{can}) \in \text{Sel}(K, V)_{p-1}$ . If  $k = 1$  then  $f(E, \omega_{can}) + \wp(g(E, \omega_{can}))$  lies in the kernel of  $\theta$  and has filtration  $p$ , so equals  $h(E, \omega_{can})$  for some  $h$  of weight 1. Thus the class of  $f(E, \omega_{can})$  lies in  $\text{Sel}(K, V)_{p-1}$ .  $\square$

**Remarks:** 1) Consider the complex  $\mathcal{O} \xrightarrow{\wp(\cdot) \frac{dq}{q}} \Omega^1(\text{cusps})$  of sheaves on  $Ig_1(N)$  where the arrow sends a local section  $f$  to the local differential  $\wp(f) \frac{dq}{q}$ . Then  $\text{Sel}(K, V)$  maps injectively to the first hypercohomology  $\mathbf{H}^1(\mathcal{O} \xrightarrow{\wp(\cdot) \frac{dq}{q}} \Omega^1(\text{cusps}))$  and the induced filtration on  $\text{Sel}(K, V)$  is  $0 \subseteq \text{Sel}(K, V)_{p-1} \subseteq \text{Sel}(K, V)$ .

2) Combining c) and d) and untwisting, we have a map  $S_k(\Gamma_1(N), \mathbf{F}_q) \rightarrow S_k(\Gamma_1(N), \mathbf{F}_q)^*$ , i.e., a bilinear form on  $S_k(\Gamma_1(N), \mathbf{F}_q)$  for  $1 \leq k \leq p$ . By d), the left kernel of this pairing consists of the forms with companions, which is a Hecke submodule of  $S_k(\Gamma_1(N), \mathbf{F}_q)$ . One can check that the right kernel is also exactly the set of forms with a companion.

Recall the sheaf  $\underline{\omega}$  on  $X_1(N)$ . The modular form  $A \in H^0(X_1(N), \underline{\omega}^{\otimes p-1})$  defines an exact sequence

$$0 \rightarrow \underline{\omega}^{\otimes k-(p-1)} \xrightarrow{A} \underline{\omega}^{\otimes k} \rightarrow \underline{SS}_k \rightarrow 0 \quad (7.9)$$

of sheaves on  $X_1(N)$  where  $\underline{SS}_k$  is a skyscraper sheaf consisting of a one-dimensional vector space at each supersingular point. Its global sections  $SS_k(\Gamma_1(N), \mathbf{F}_q) = H^0(X_1(N) \otimes \mathbf{F}_q, \underline{SS}_k)$  are naturally the modular forms of weight  $k$  for  $\Gamma_1(N)$  on supersingular elliptic curves.

The long exact cohomology sequence of 7.9 yields a short exact sequence

$$0 \rightarrow W_k(\Gamma_1(N), \mathbf{F}_q) \rightarrow SS_k(\Gamma_1(N), \mathbf{F}_q) \rightarrow H^1(X_1(N) \otimes \mathbf{F}_q, \underline{\omega}^{\otimes k-(p-1)}) \rightarrow 0$$

where  $W_k(\Gamma_1(N), \mathbf{F}_q) = M_k(\Gamma_1(N), \mathbf{F}_q) / AM_{k-(p-1)}(\Gamma_1(N), \mathbf{F}_q)$ . Now as vector spaces,  $H^1(X_1(N) \otimes \mathbf{F}_q, \underline{\omega}^{\otimes k-(p-1)}) \cong H^0(X_1(N) \otimes \mathbf{F}_q, \Omega^1 \otimes \underline{\omega}^{\otimes (p-1)-k})^* \cong S_{k'}(\Gamma_1(N), \mathbf{F}_q)^*$  and

Serre has shown that as Hecke modules,  $H^1(X_1(N) \otimes \mathbf{F}_q, \underline{\omega}^{\otimes k-(p-1)}) \cong S_{k'}(\Gamma_1(N), \mathbf{F}_q)[k-1]^*$ . To see this, note that there is a pairing

$$SS_k(\Gamma_1(N), \mathbf{F}_q) \times SS_{k'}(\Gamma_1(N), \mathbf{F}_q) \rightarrow \mathbf{F}_q$$

$$f, g \mapsto \langle f, g \rangle = \sum_{(E, \alpha)} \frac{fg}{B}(E, \alpha) \quad (7.10)$$

where the sum is over all supersingular  $E$  with  $\Gamma_1(N)$ -structures  $\alpha$ . This pairing is non-degenerate, and using the fact that  $\phi^*(B(E)) = \ell B(E')$  where  $\phi : E \rightarrow E'$  is an isogeny of degree  $\ell$  ([10], thm. B), one easily computes the transposition formula  $\langle T_\ell f, g \rangle = \langle f, \ell^{k-1} T_\ell g \rangle$ . Moreover, the orthogonal complement of  $W_k(\Gamma_1(N), \mathbf{F}_q) \subseteq SS_k(\Gamma_1(N), \mathbf{F}_q)$  is the image of  $S_{k'}(\Gamma_1(N), \mathbf{F}_q) \rightarrow SS_{k'}(\Gamma_1(N), \mathbf{F}_q)$ . (An alternative definition which makes this clear is  $\langle f, g \rangle = \sum_{v=(E, \alpha)} \text{Res}_v f g \frac{dq}{q}$ , again summing over supersingular  $E$  with  $\Gamma_1(N)$ -structures.) Thus we have an isomorphism of Hecke modules  $SS_k(\Gamma_1(N), \mathbf{F}_q)/W_k(\Gamma_1(N), \mathbf{F}_q) \cong$

$S_{k'}(\Gamma_1(N), \mathbf{F}_q)[k-1]^*$  and an exact sequence

$$0 \rightarrow W_k(\Gamma_1(N), \mathbf{F}_q) \rightarrow SS_k(\Gamma_1(N), \mathbf{F}_q) \rightarrow S_{k'}(\Gamma_1(N), \mathbf{F}_q)[k-1]^* \rightarrow 0 \quad (7.11)$$

for  $1 \leq k \leq p-1$ . The modules  $W_k$  and  $SS_k$  were studied by Serre and Tate and Serre [13] has given a quaternionic interpretation of  $SS_k$ .

We can now describe the Selmer group for  $p$  in terms of the  $SS_k(\Gamma_1(N), \mathbf{F}_q)$ . Note that as in the remark before 7.8,  $H^1(K, \text{Ker } p) \cong K^0$  is not equivariant for  $\text{Gal}(K/\mathbf{F}_q(X_1(N)))$ : we have  $\text{Sel}(K, p)^{(k-1)} \hookrightarrow (K^0)^{(k)}$ .

**Theorem 7.12.**

a) *There is a canonical injection  $\text{Sel}(K, p)^{(k-1)} \hookrightarrow SS_k(\Gamma_1(N), \mathbf{F}_q)$  and identifying  $\text{Sel}(K, p)^{(k-1)}$*

with its image, we have an exact sequence

$$0 \rightarrow W_k(\Gamma_1(N), \mathbf{F}_q)^{k\sigma+k'U=0} \rightarrow \text{Sel}(K, p)^{(k-1)} \rightarrow S_{k'}(\Gamma_1(N), \mathbf{F}_q)[k-1]^{*(k'\sigma+kU)^t=0} \rightarrow 0$$

for  $1 \leq k \leq p-1$ .

b) We have an isomorphism  $S_p(\Gamma_1(N), \mathbf{F}_q)^{U=0} \cong \text{Sel}(K, p)^{(0)}$ .

**Proof:** a) We begin by reformulating the local condition 5.5 at the supersingular places. According to Swinnerton-Dyer and Katz ([3]), we have the formula  $\theta f = \partial f - kBf$  for  $f$  of weight  $k$ , where  $\partial$  is a derivation of the ring of modular forms which increases weights by 2. (Of course,  $\partial$  depends on the choices made to define  $B$ .) Thus if  $f \in K$  has filtration  $< p$ ,  $\theta f/B(E, \omega_{can}) = -kf + g$  with  $v(g) \geq 0$  at supersingular places  $v$ . Putting this in 5.5, we have

$$\text{Sel}(K_v, p)^{(k-1)} = \{kf_v^p + k'f_v + g_v \mid f_v, g_v \in K_v^{(k)}, v(f_v) > -p, v(g_v) \geq 0\} \cap K_v^0$$

for supersingular  $v$ . Recall that for ordinary  $v$ ,  $\text{Sel}(K_v, p) = R_v \cap K_v^0$  and for cuspidal  $v$ ,  $\text{Sel}(K_v, p) = \wp(K_v) \cap K_v^0 = (t_v R_v) \cap K_v^0$  where  $t_v$  is a uniformiser at  $v$ .

Given  $f \in \text{Sel}(K, p)^{(k-1)} \subseteq K^0$ , write  $f = kf_v^p + k'f_v + g_v$  with  $f_v \in K_v^{(k)}$ ,  $v(f_v) > -p$  and  $v(g_v) \geq 0$  at each supersingular place  $v$ . Then  $(f_v \omega_{can}^{\otimes k})$  is a well-defined element of  $SS_k(\Gamma_1(N), \mathbf{F}_q)$  and this defines an injection  $\text{Sel}(K, p)^{(k-1)} \hookrightarrow SS_k(\Gamma_1(N), \mathbf{F}_q)$ .

If  $(f_v \omega_{can}^{\otimes k})$  is in the image of  $W_k(\Gamma_1(N), \mathbf{F}_q) \rightarrow SS_k(\Gamma_1(N), \mathbf{F}_q)$ , then there exists  $g \in M_k(\Gamma_1(N), \mathbf{F}_q)$  such that  $kg(E, \omega_{can})^p + k'g(E, \omega_{can}) = f$ , and  $f \in K^0$  implies  $kg + k'\sigma^{-1}Ug = 0$ . Conversely, for such a  $g$ ,  $f = kg(E, \omega_{can})^p + k'g(E, \omega_{can})$  is in  $\text{Sel}(K, p)$ . (The local conditions are clear at the supersingular and ordinary places. At the cuspidal  $v$ ,  $f \in K^0$  implies  $v(f) > 0$ .)

Since  $pr : Ig_1(N) \rightarrow X_1(N)$  is finite and  $pr_* \mathcal{O}_{Ig_1(N)} \cong \bigoplus_{k=0}^{p-2} \underline{\omega}^{\otimes -k}$  ([4], 12.8.5) we have  $H^1(X_1(N), \underline{\omega}^{\otimes k-(p-1)}) \cong H^1(Ig_1(N), \mathcal{O})^{(k)}$ . Now the composed map  $SS_k(\Gamma_1(N), \mathbf{F}_q) \rightarrow H^1(Ig_1(N), \mathcal{O})^{(k)}$  sends  $(f_v \omega_{can}^{\otimes k})$  to  $(f_v)$ . The image of an element of  $\text{Sel}(K, p)$  clearly satisfies the relation  $(k\text{Fr} + k')(f_v) = 0$  in  $H^1(Ig_1(N), \mathcal{O})^{(k)}$ , which goes over to the relation  $(k\sigma^{-1}U + k')^t = 0$  in  $S_{k'}(\Gamma_1(N), \mathbf{F}_q)[k-1]^*$ . It remains to show surjectivity. First assume  $k \neq 1$  and represent an element of  $H^1(Ig_1(N), \mathcal{O})^{(k)}$  killed by  $k\text{Fr} + k'$  as  $(f_v)$  where  $f_v \in K_v^{(k)}$ ,  $v(f_v) \geq -k$  for supersingular  $v$ ,  $v(f_v) \geq 0$  for ordinary  $v$  and  $v(f_v) > 0$  for cuspidal  $v$  (which we can do since  $H^1(Ig_1(N), \mathcal{O}((p-1) \sum_{\text{supersingular } v} [v] - \sum_{\text{cuspidal } v} [v]))^{(k)} = 0$  for  $k \neq 1$ ). Clearly there is a function  $f \in K$  with  $v(f - kf_v^p - k'f_v) \geq 0$  for all  $v$ , but we must choose  $(f_v)$  so that  $f \in K^0$  and  $f$  satisfies the local conditions. Note that changing  $(f_v)$  by a global function  $g$  changes  $f$  to  $f - kg^p - k'g$ , so to have  $\mathcal{C}(f dq/q) = 0$  we must solve

$$(1 - (-k'/k)\mathcal{C})(g \frac{dq}{q}) = (1/k)\mathcal{C}(f \frac{dq}{q}) \quad (7.13)$$

for  $g$ . Choose  $c \in \overline{\mathbf{F}_p}$  such that  $c^{p-1} = -k/k'$ . Then solving 7.13 over  $\mathbf{F}_q$  is equivalent to solving  $(1 - \mathcal{C})(\tilde{g} \frac{dq}{q}) = (c/k)\mathcal{C}(f \frac{dq}{q})$  over  $\mathbf{F}_q(c)$ . (Given  $\tilde{g}$ , project it into the appropriate eigenspace for  $\text{Gal}(\mathbf{F}_q(c)/\mathbf{F}_q)$  and put  $g = \tilde{g}/c$ .)

Now there is an exact sequence (take the étale cohomology on  $K$  of [7], III.5.6; cf. also ex. 5.9)

$$\Omega_K^1 \xrightarrow{1-\mathcal{C}} \Omega_K^1 \rightarrow H^2(K, \mu_p) \cong \text{Br}(K)_p$$

where  $\text{Br}(K)_p$  is the  $p$ -torsion in the Brauer group of  $K$ . Viewing  $\text{Br}(K)_p$  as a subgroup of  $\bigoplus_v \mathbf{Z}/p\mathbf{Z}$ , the map  $\Omega_K^1 \rightarrow \text{Br}(K)_p$  is  $\omega \mapsto (\text{Tr}_{\mathbf{F}_q/\mathbf{F}_p} \text{Res}_v \omega)$ . Since  $(c/k)\mathcal{C}(f \frac{dq}{q})$  is everywhere regular, we can solve  $(1 - \mathcal{C})(\tilde{g} \frac{dq}{q})$ , and we can even insist that  $\tilde{g} \frac{dq}{q}$  be everywhere

regular, so  $g = \tilde{g}/c$  has filtration  $\leq k$  and vanishes at the cusps. Then  $f - kg^p - k'g$  lies in  $\text{Sel}(K, p)$  and maps to  $(f_v)$  as desired.

It remains to show surjectivity for  $k = 1$ . But in this case,  $M_k(\Gamma_1(N), \mathbf{F}_q)^{k\sigma+k'U=0} = 0$  as  $\sigma$  is an automorphism of  $M_k(\Gamma_1(N), \mathbf{F}_q)$ . Thus the map  $\text{Sel}(K, p)^{(0)} \rightarrow S_p(\Gamma_1(N), \mathbf{F}_q)^{*U^t=0}$  is an injection. It is also surjective, by comparing dimensions and using b).

b) To prove the last assertion, we note that according to the local conditions 5.5, an element of  $f \in \text{Sel}(K, p)^{(0)}$  is a function  $f \in K^0$  with exact filtration  $p$  such that  $\theta f$  has filtration 3. But for functions of filtration  $p$ ,  $f \in K^0$  implies automatically that  $\theta f$  has filtration 3. Indeed, otherwise,  $\theta^{p-1}f = f$  would have filtration  $p^2$  which is impossible. Finally, the set of elements of  $K^0$  of exact filtration  $p$  is isomorphic to  $S_p(\Gamma_1(N), \mathbf{F}_q)^{U=0}$ .

□

**Remarks:** 1) Consider the complex  $\mathcal{O} \xrightarrow{\cdot dq/q} \Omega^1(\text{cusps})$  of sheaves on  $Ig_1(N)$  where the arrow sends a local section  $f$  of  $\mathcal{O}$  to  $f dq/q$ . Then the hypercohomology  $\mathbf{H}^1(Ig_1(N), \mathcal{O} \xrightarrow{\cdot dq/q} \Omega^1(\text{cusps}))$  is isomorphic to  $\bigoplus_{k=1}^{p-1} SS_k(\Gamma_1(N), \mathbf{F}_q)$ . The map  $\text{Sel}(K, p) \rightarrow \bigoplus_{k=1}^{p-1} SS_k(\Gamma_1(N), \mathbf{F}_q)$  is the composite  $\text{Sel}(K, p) \hookrightarrow \text{Sel}(K, V) \rightarrow \mathbf{H}^1(Ig_1(N), \mathcal{O} \xrightarrow{\varphi(\cdot) dq/q} \Omega^1(\text{cusps})) \rightarrow \mathbf{H}^1(Ig_1(N), \mathcal{O} \xrightarrow{\cdot dq/q} \Omega^1(\text{cusps}))$  where the second map is that of the remark after 7.8 and the third is induced by the map of complexes

$$\begin{array}{ccc} \mathcal{O} & \xrightarrow{\varphi(\cdot) dq/q} & \Omega^1(\text{cusps}) \\ \varphi(\cdot) \downarrow & & \parallel \\ \mathcal{O} & \xrightarrow{\cdot dq/q} & \Omega^1(\text{cusps}). \end{array}$$

2) One can also define maps  $S_{k'}(\Gamma_1(N), \mathbf{F}_q)[k-1]^{(k'\sigma+kU)=0} \rightarrow \text{Sel}(K, p)^{(k-1)}$  for other values of  $k$  in the spirit of 7.8b, although some care is required when the ground field is not  $\mathbf{F}_p$ . We leave this as an exercise for the reader.

3) *A priori* the groups  $\text{Sel}(K, p)^{(k-1)}$  are just  $\mathbf{F}_p$ -vector spaces, but 7.12b shows that  $\text{Sel}(K, p)^{(0)} \cong \text{Sel}(\mathbf{F}_q(X_1(N)), p)$  actually has the structure of an  $\mathbf{F}_q$ -vector space. It would be interesting to know, for fixed  $N$  and varying  $p$ , how often this group is non-trivial.

4) In contrast to  $\text{Sel}(K, p)^{(0)}$ , when  $k-1 \not\equiv 0 \pmod{p-1}$   $\text{Sel}(K, p)^{(k-1)}$  has order bounded independent of the ground field  $\mathbf{F}_q$ . Indeed, if  $w$  is the  $\mathbf{F}_q$ -dimension of the subspace of  $W_k(\Gamma_1(N), \mathbf{F}_q)$  generated by forms lying in generalized eigenspaces for  $U$  with non-zero eigenvalue (the “ordinary part” in the sense of Hida) and if  $s$  denotes the  $\mathbf{F}_q$ -dimension of the similarly defined subspace of  $S_{k'}(\Gamma_1(N), \mathbf{F}_q)$ , then for sufficiently large  $\mathbf{F}_q$ , the  $\mathbf{F}_p$ -dimension of  $\text{Sel}(K, p)^{(k-1)}$  is  $w + s$ . Examples (using table 3.4 of [16]) and theoretical considerations which cannot be discussed here suggest that this dimension is usually larger than the rank of  $E(K)$ , so  $\mathbb{H}(E, K)_p$  will be non-trivial when  $\mathbf{F}_q$  is large.

Restricting the pairing 7.10 to the Selmer group and composing with the trace from  $\mathbf{F}_q$  to  $\mathbf{F}_p$ , we get pairings  $\text{Sel}(K, p)^{(k-1)} \times \text{Sel}(K, p)^{(k'-1)} \rightarrow \mathbf{F}_p$  for  $2 \leq k \leq p-1$ . Similarly, using a) and b) of 7.12 and composing with the trace, we get a pairing  $\text{Sel}(K, p)^{(0)} \times \text{Sel}(K, p)^{(0)} \rightarrow \mathbf{F}_p$ . Let  $\langle, \rangle_{\text{Sel}}$  denote the direct sum of these pairings. Note that  $\langle, \rangle_{\text{Sel}}$  for  $K \otimes \mathbf{F}_{q^f}$  is  $f$  times  $\langle, \rangle_{\text{Sel}}$  for  $K$ , and that  $\langle f, g \rangle_{\text{Sel}} = 0$  unless the projections of  $f$  and  $g$  to  $\text{Sel}(K, p)^{(k-1)}$  and  $\text{Sel}(K, p)^{(k'-1)}$  respectively are both non-zero for some  $k$ .

We also have a non-degenerate symmetric bilinear form on  $E(K)$ , namely the canonical height pairing  $\langle, \rangle_{ht}$ . By definition  $\langle, \rangle_{ht} = r \log q$  for some rational number  $r$ , and since the only types of bad reduction which occur for  $E$  over  $K$  are  $I_n$  for  $n|N$ , it's easy to see that  $r$  must be integral at  $p$ . Thus  $\langle, \rangle_{ht}/\log p$  makes sense mod  $p$ . Note that  $\langle, \rangle_{ht}/\log p$  for  $K \otimes \mathbf{F}_q$  is  $f$  times  $\langle, \rangle_{ht}/\log p$  for  $K$  and that  $\langle P, Q \rangle_{ht}/\log p \equiv 0 \pmod{p}$  unless the

projections of  $P$  and  $Q$  to  $(E(K)/pE(K))^{(k-1)}$  and  $(E(K)/pE(K))^{(1-k)}$  respectively are both non-zero for some  $k$ . Thus it is natural to ask “what is the relationship between  $\langle P, Q \rangle_{ht}/\log p$  and  $\langle \lambda(P), \lambda(Q) \rangle_{\text{Sel}}$ ?” where  $\lambda : E(K) \rightarrow \text{Sel}(K, p)$  is the descent map.

## 8. Examples

(8.1) Let  $p = 2$ ,  $N = 3$  and fix a ground field  $\mathbf{F}_q$  of characteristic 2. The ring of modular forms for  $\Gamma_1(3)$  over  $\mathbf{F}_q$  is the polynomial ring generated by the forms  $a_1$  in weight 1 and  $a_3$  in weight 3;  $a_1$  is the Hasse invariant and  $a_3$  reduces to  $B$  at the supersingular point. We have  $E_4 = a_1^4$ ,  $E_6 = a_1^6$  and  $\Delta = a_3^3(9a_1^3 - 27a_3)$ . Setting  $T = a_3/a_1^3 = a_3(E, \omega_{can})$ , the field  $K$  is the rational field  $\mathbf{F}_q(T)$  and the universal curve  $E$  has Weierstrass equation

$$y^2 + xy + Ty = x^3$$

with  $j$ -invariant  $T^{-3}(1-T)^{-1}$  and discriminant  $T^3(1-T)$ ; the coordinates of the canonical point  $P \in E^{(2)}(K)$  are  $(T^2, T^3)$ .

At the unique supersingular place  $T = \infty$ ,  $E$  has additive reduction of type  $IV^*$  with conductor  $f = 2$  and all 3 components of multiplicity 1 are rational. Since  $E$  obtains good reduction over an extension of degree prime to 2, 3.1 applies and  $\text{Sel}(K_v, F) = U_{K_v}^{[1]}$  and  $\text{Sel}(K_v, V) = P_{K_v}^{[0]}$ . From this it follows easily that  $\text{Sel}(K_v, p) = K_v^0 \cap R_v$ .

At the cusp  $T = 0$ ,  $E$  has split multiplicative reduction, so the Selmer groups are given by 3.1b and 5.4. At the cusp  $T = 1$ ,  $E$  has split multiplicative reduction if  $\mathbf{F}_4 \subseteq \mathbf{F}_q$  and non-split multiplicative reduction otherwise. Thus if  $\mathbf{F}_4 \not\subseteq \mathbf{F}_q$ , we get only  $\text{Sel}(K_v, V) \subseteq \text{Ker}(K_v/\wp(K_v) \rightarrow L/\wp(L)) \subseteq P_{K_v}^{[0]}$  (where  $L = K_v \otimes \mathbf{F}_4$ ). But this implies that  $U_{K_v}^{[0]} \subseteq \text{Sel}(K_v, F)$ , and a short computation using Voloch’s formula 6.1 shows that the point  $(T + T^2, T^{-1}[T(T+1)^3 + T^2(T+1)^6 + \dots])$  of  $E^{(2)}(K_v)$  maps to the non-trivial class in

$(K_v^\times/K_v^{\times 2})/U_{K_v}^{[0]}$ , so  $\text{Sel}(K_v, F) = K_v^\times/K_v^{\times 2}$  and  $\text{Sel}(K_v, V) = 0$ .

Applying the same reasoning as in 3.2, we have that  $\text{Sel}(K, F) = \mathbf{Z}/2\mathbf{Z}\frac{dq}{q}$  where  $dq/q = d\Delta/\Delta = dT/T + d(1-T)/(1-T)$ ,  $\text{Sel}(K, V) = 0$  and so  $\text{Sel}(K, p) = 0$ . By the main theorem of [17], the  $L$ -function of  $E/K$  is 1 (there are no cusp forms of weight 3 on  $\Gamma_1(6)$ ), and since the Tamagawa number  $\tau(E, K)$  of  $E$  is 9 (coming from components at the supersingular place and the cusp  $T = 0$ ), the Birch and Swinnerton-Dyer formula gives  $|\Sha(E, K)| = 1$ .

(8.2) Now assume  $p = 3$ ,  $N = 1$  and fix a ground field  $\mathbf{F}_q$  of characteristic 3. The ring of modular forms of level 1 over  $\mathbf{F}_q$  is a polynomial ring generated by the Hasse invariant  $A = a_2$  in weight 2 and  $\Delta$  in weight 12; we have  $E_4 = a_2^2$  and  $E_6 = a_2^3$ . Setting  $T = \Delta/a_2^6 = \Delta(E, \omega_{can})$ , the field  $K$  is the rational field  $\mathbf{F}_q(T)$  and the universal curve  $E$  has Weierstrass equation

$$y^2 = x^3 + x^2 - T$$

with  $j$ -invariant  $T^{-1}$  and discriminant  $T$ ; the canonical point  $P \in E^{(3)}(K)$  has coordinates  $(T, T)$ .

At the unique supersingular place  $T = \infty$ ,  $E$  has additive reduction of type  $II^*$  with conductor  $f = 3$  and  $E^{(3)}$  has additive reduction of type  $IV^*$  with all three components of multiplicity 1 rational over  $\mathbf{F}_3$ . The explicit computations in this case are fairly unpleasant, so we just note that by [17], the  $L$ -function of  $E/K$  is 1, and the Tamagawa number  $\tau(E, K) = 1$ . By the Birch and Swinnerton-Dyer formula,  $|\Sha(E, K)| = 1$ , so  $\text{Sel}(K, p) = 1$  and  $\text{Sel}(K, F) = \mathbf{Z}/3\mathbf{Z}\frac{dq}{q}$ . Since  $\tau(E^{(3)}, K) = 9$  (again from components at the supersingular place and the cusp) we also have  $\text{Sel}(K, V) = 1$ .

(8.3) Now assume  $p = 3$  and  $N = 2$ . The ring of modular forms for  $\Gamma_1(2)$  over  $\mathbf{F}_q$  is a polynomial ring generated by  $A = a_2$  in weight 2 and  $a_4$  in weight 4 with  $\Delta = 16a_2^2a_4^2 - 64a_4^3$ . The field  $K$  is the rational field  $\mathbf{F}_q(a_4(E, \omega_{can}))$ , the  $L$ -function of  $E/K$  is again 1 and nothing interesting happens.

(8.4) The case  $p = 3$ ,  $N = 4$  is more interesting. The ring of modular forms on  $\Gamma_1(4)$  over  $\mathbf{F}_q$  is a polynomial ring generated by  $\theta^2$  in weight 1 and the Hasse invariant  $A = a_2$  in weight 2. We have  $a_4 = (\theta^8 - 2a_2\theta^4 + a_2^2)/4$ . Putting  $T = \theta^2(E, \omega_{can})$ ,  $K$  is the rational field  $\mathbf{F}_q(T)$  and the universal curve  $E$  becomes

$$y^2 = x^3 + x^2 + T^{12} - T^8 - T^6 + T^2.$$

This curve has reduction type  $I_1$  at the cusps  $T = \pm 1$ ,  $I_2$  at the cusp  $T = 0$  and  $I_4$  at the cusps  $T = \pm\sqrt{-1}$ ; it has good reduction elsewhere. The canonical point of order 4 has coordinates  $(T^2(1 - T^2), T(1 - T^2))$ .

We have  $\text{Sel}(K, p)^{(0)} \cong S_3(\Gamma_1(4), \mathbf{F}_q)^{U=0} = 0$  and  $\text{Sel}(K, p)^{(1)} \cong W_2(\Gamma_1(4), \mathbf{F}_q)^{\sigma+U=0}$ .

Now  $W_2(\Gamma_1(4), \mathbf{F}_q)$  is one-dimensional, generated by the class  $\bar{\theta}^4$  of  $\theta^4$ , which satisfies  $U\bar{\theta}^4 = \bar{\theta}^4$ . Thus  $\text{Sel}(K, p)$  has order 3 when  $\mathbf{F}_9 \subseteq \mathbf{F}_q$  (generated by  $\sqrt{-1}\bar{\theta}^4$ ) and is trivial otherwise.

The  $L$ -function of  $E$  over  $K$  is  $(1 - (-3)^f q^{-s})$  where  $f = [\mathbf{F}_q : \mathbf{F}_3]$  (the unique cusp form of weight 3 on  $\Gamma_1(12)$  is the CM form associated to the Hecke character of conductor 2 on  $\mathbf{Q}(\sqrt{-3})$ ), so one expects a point of infinite order on  $E$  rational over  $K$  when  $\mathbf{F}_9 \subseteq \mathbf{F}_q$ . In fact, the point  $P$  with coordinates  $((T^2 - 1)^2, \sqrt{-1}(T^6 - 1))$  has infinite order. Its canonical height is  $\frac{1}{2} \log q$  and its image  $\lambda(P)$  in the Selmer group is  $\sqrt{-1}(T^6 - T^2) \subseteq K^0$  (using 6.2), which is the image of  $\sqrt{-1}\bar{\theta}^4$  under  $M_2(\Gamma_1(4), \mathbf{F}_q) \rightarrow \text{Sel}(K, p)^{(1)}$ . We remark

that  $\langle \lambda(P), \lambda(P) \rangle_{\text{Sel}} = f/2 \equiv \langle P, P \rangle_{ht} / \log 3$ .

(8.5) Assume  $p \equiv 3 \pmod{4}$ ,  $p > 3$  and  $N = 1$ . The universal curve in this case was studied in [16] and it was shown there that its  $L$ -function vanishes to order at least  $h$ , the class number of  $\mathbf{Q}(\sqrt{-p})$ , when  $\mathbf{F}_{p^2} \subseteq \mathbf{F}_q$ . Since the modular forms giving rise to the zeros of the  $L$ -function have character  $\omega^{(p-1)/2}$  for  $\text{Gal}(X_1(p)/X_1(1)) \cong (\mathbf{Z}/p\mathbf{Z})^\times / \pm 1$  (where  $\omega$  is the Teichmüller character) one expects to find a subgroup of  $\text{Sel}(K, p)^{((p-1)/2)}$  of order  $p^h$ . (*A priori*, the descent calculations of section 7 do not apply (as  $N = 1$ ) but as remarked at the beginning of that section, this case can be easily treated by taking invariants. Indeed, choose  $M$  so that  $p \nmid \#GL_2(\mathbf{Z}/M\mathbf{Z})$  (which is possible as  $p > 3$ ). Then the calculations of section 7 can be applied, *mutatis mutandis*, to the case where the base curve is  $X(M)$  and then  $\text{Sel}(K, p) = \text{Sel}(L, p)^{GL_2(\mathbf{Z}/M\mathbf{Z})}$  where  $L$  is the function field of the modular curve for full level  $M$  structures and Igusa structures of level  $p$ . One concludes that 7.12 holds as stated for arbitrary  $N$  when  $p > 3$ . We also note that section 10 of [1] catalogues the important differences for modular forms and Igusa curves between the cases  $N \leq 4$  and  $N > 4$ .)

Using the generalized 7.12, it is easy to produce the desired subgroup of  $\text{Sel}(K, p)$  when  $\mathbf{F}_{p^2} \subseteq \mathbf{F}_q$ . Indeed, the  $\theta$ -series  $\theta_C = \sum_{\mathfrak{a} \in C} q^{\text{Na}}$  (where  $C$  is an ideal class of  $\mathbf{Q}(\sqrt{-p})$  and the sum is over integral ideals in the given class) span an  $(h+1)/2$ -dimensional space of modular forms of weight 1 and quadratic character on  $\Gamma_1(p)$  stable under the Hecke algebra; the subspace of cusp forms is  $(h-1)/2$ -dimensional. These forms are CM (or dihedral) in the sense that the  $q$ -expansion coefficient  $a_\ell$  is zero when  $\ell$  is not a square mod  $p$ . By a general principle of Serre ([12] thm. 12), these forms reduce mod  $p$  to modular forms

of weight congruent to  $(p+1)/2$  on  $\Gamma(1)$ , and since  $U\theta_C = \theta_C$ , they must have filtration  $\leq p+1$ . One easily checks that the Hecke algebra acts semi-simply on the corresponding subspace of  $W_{(p+1)/2}(\Gamma_1(N), \mathbf{F}_p)$  (the point is that the eigenvalues for the Hecke algebra are sums of  $h$ -th roots of unity and  $h < p$ ). Thus we have an  $(h+1)/2$ -dimensional  $\mathbf{F}_p$  subspace  $T$  of  $W_{(p+1)/2}(\Gamma_1(N), \mathbf{F}_q)$  on which  $U$  acts as 1 and since the forms in  $T$  are CM, we get an  $(h-1)/2$ -dimensional  $\mathbf{F}_p$  subspace  $T'$  of  $S_{(p+1)/2}(\Gamma_1(N), \mathbf{F}_p)[(p-1)/2]^*$  where the Hecke algebra acts via the same semi-simple representation. When  $\mathbf{F}_{p^2} \subseteq \mathbf{F}_q$ ,  $\sigma + U$  and  $(\sigma + U)^t$  are zero on  $\sqrt{-1}T$  and  $\sqrt{-1}T'$  respectively so the Selmer group contains an  $h$ -dimensional  $\mathbf{F}_p$  subspace when  $\mathbf{F}_{p^2} \subseteq \mathbf{F}_q$ . *Assuming* that the Hecke algebra acts semi-simply on the entire isotypical component of  $W_{(p+1)/2}(\Gamma_1(N), \mathbf{F}_p)$  associated to the  $\theta$ -series (i.e., it consists of exactly these forms), we can recover a canonical subgroup of  $\text{Sel}(K, p)$  of order  $p^h$  as the isotypical component of  $SS_{(p+1)/2}(\Gamma_1(N), \mathbf{F}_{p^2})$  associated to the  $\theta$ -series where  $1 \neq \sigma \in \text{Gal}(\mathbf{F}_{p^2}/\mathbf{F}_p)$  acts by  $-1$ .

We note also that by comparing the formula at the bottom of p. 389 of [16] with 7.8, one finds that when  $\mathbf{F}_{p^2} \not\subseteq \mathbf{F}_q$  the  $p$ -primary component of  $\mathfrak{M}(K, E^{(p)})$  is killed by  $V$  (and thus also  $p$ ) if and only if  $\text{Sel}(K, p) = 0$ . This is the case when  $\mathbf{F}_q = \mathbf{F}_p$  and  $p \leq 223$  by computations of Atkin.

(8.6) The case  $p \equiv 1 \pmod{4}$ ,  $N = 4$  is very similar. The  $L$ -function of the universal curve vanishes to order at least  $h$ , the class number of  $\mathbf{Q}(\sqrt{-p})$ , when  $\mathbf{F}_{p^2} \subseteq \mathbf{F}_q$ . In this case, the modular forms contributing zeros of the  $L$ -function have character  $(\frac{\cdot}{p})$  (the Legendre character) so we expect to find a subgroup of  $\text{Sel}(K, p)^{((p-1)/2)}$  of order  $p^h$ ; note that  $(p+1)/2$  is odd in this case. Now we have an  $(h/2) + 1$ -dimensional space of  $\theta$  series of

weight 1 and character  $\left(\frac{-}{p}\right)$  on  $\Gamma_1(4p)$  and an  $(h/2) - 1$ -dimensional subspace of cusp forms.

Using these we again get a subgroup of  $\text{Sel}(K, p)^{((p-1)/2)}$  of order  $p^h$  when  $\mathbf{F}_{p^2} \subseteq \mathbf{F}_q$ .

## References

- 1 Gross, B.: The Galois representations associated to modular forms (mod  $p$ ). Preprint (1989)
- 2 Jochnowitz, N.: A study of the local components of the Hecke algebra mod  $\ell$ . Trans. Amer. Math. Soc. **270** (1982) 253-267
- 3 Katz, N.: A result on modular forms in characteristic  $p$ . In: Serre, J.-P. and Zagier, D.B. (Eds.) Modular Functions of One Variable V (Lect. Notes in Math. 601.) pp. 53-61 Berlin Heidelberg New York: Springer 1977
- 4 Katz, N. and Mazur, B.: Arithmetic Moduli of Elliptic Curves. Princeton: Princeton University Press 1985
- 5 Kramer, K.: Two-descent for elliptic curves in characteristic two. Trans. Amer. Math. Soc. **232** (1977) 279-295
- 6 Milne, J.S.: Etale Cohomology. Princeton: Princeton University Press 1980
- 7 Milne, J.S.: Arithmetic Duality Theorems. Orlando: Academic Press 1986
- 8 Mumford, D.: Abelian Varieties. Oxford: Oxford University Press 1970
- 9 Oda, T.: The first deRham cohomology group and Dieudonné modules. Ann. Sci. Ec. Norm. Super.(4) **2** (1969) 63-135
- 10 Robert, G.: Congruences entre séries d'Eisenstein, dans le cas supersingulier. Invent. Math. **61** (1980) 103-158
- 11 Serre, J.-P.: Groupes Algébriques et Corps de Classes. Paris: Hermann 1959
- 12 Serre, J.-P.: Formes modulaires et fonctions zêta  $p$ -adiques. In: Kuyk, W. and Serre, J.-P.(Eds.) Modular Functions of One Variable III (Lect. Notes in Math. 350.) pp. 191-268 Berlin Heidelberg New York: Springer 1973
- 13 Serre, J.-P.: Formes modulaires (mod  $p$ ). Cours au Collège de France (1987-88)
- 14 Seshadri, C.: L'opération de Cartier, applications. Séminaire Chevalley 1958/59 Secr. math., Paris (1960)
- 15 Tate, J. and Oort, F.: Group schemes of prime order. Ann. Sci. Ec. Norm. Super.(4) **3** (1970) 1-21
- 16 Ulmer, D.L.: On universal elliptic curves over Igusa curves. Invent. Math. **99** (1990) 377-391
- 17 Ulmer, D.L.:  $L$ -functions of universal elliptic curves over Igusa curves. (To appear in the American Journal of Mathematics) (1988)
- 18 Voloch, J.F.: Explicit  $p$ -descent for elliptic curves in characteristic  $p$ . (To appear in Comp. Math.) (1988)
- 19 Witt, E.: Zyklische Körper und Algebren der Charakteristik  $p$  vom Grade  $p^n$ . J. für reine u. ang. Math. **176** (1936) 126-140