Compositio Mathematica **119:** 111–132, 1999.

Complete p-Descent for Jacobians of Hermitian Curves

NEIL DUMMIGAN
Merton College, Oxford OX1 4JD, U.K.

(Received: 17 September 1997; accepted in final form: 10 July 1998)

Abstract. Let X be the Fermat curve of degree $q+1$ over the field k of q^2 elements, where q is some prime power. Considering the Jacobian J_X of X as a constant Abelian variety over the function field $k(X)$, we calculate the multiplicities, in subfactors of the Shafarevich–Tate group, of representations associated with the action on X of a finite unitary group. J_X is isogenous to a power of a supersingular elliptic curve E, the structure of whose Shafarevich–Tate group is also described.

Mathematics Subject Classification (1991): 11G20.

Key words: fermat curve, Abelian variety, descent, crystalline cohomology, finite unitary group.

The Shafarevich–Tate group is an important object associated with any Abelian variety over a global field. It classifies locally-trivial principal homogeneous spaces and is conjectured to be finite in all cases. For modular elliptic curves of analytic rank one or zero (and related higher dimensional examples) the finiteness is known, thanks to well-known work of Kolyvagin, as is information relating the structure of the group to the divisibility of certain Heegner points. Also, what is known about its order agrees with the Birch and Swinnerton–Dyer conjecture. See [16] and [17].

The constant Abelian varieties over global function fields, i.e. those already defined over the finite subfield of constant functions, form one of the other main classes for which finiteness of the Shafarevich–Tate group is known (see the last page of [15]). In this case the analog of the Birch and Swinnerton–Dyer conjecture is also known to be true (see [12]). In this paper we analyse the Shafarevich–Tate groups of some very special, symmetrical examples of constant Abelian varieties over global function fields. The special nature of the examples considered has two effects. First, there exists an intricate structure related to the action of the symmetry group, and second, it is possible to find it. To this end we avail ourselves of the great wealth of beautiful results in the literature concerning crystalline cohomology. The present work was originally motivated by the desire to calculate the determinants of certain Mordell–Weil lattices.

Let p be any prime number and $q = p^f$ for some $f > 0$. Let $k = \mathbb{F}_{q^2}$, the field with q^2 elements. Consider the Fermat curve of degree $q+1$ in the projective plane over k

$$X: x^{q+1} + y^{q+1} + z^{q+1} = 0.$$

The involutory qth power automorphism of k is analogous to complex conjugation, and the left-hand side of the above equation is analogous to a Hermitian form in three variables, so we say that X is a Hermitian curve. It has genus $g = q(q-1)/2$, by the degree-genus formula. Let

$$G = \mathrm{SU}_3(q) = \{A \in M_3(k) : A^{(q)t} = A^{-1}, \det A = 1\}$$

be the finite special unitary group in three variables. Here $A^{(q)t}$ is the transpose of the matrix obtained from A by raising each entry to the qth power. G acts naturally on X, by fractional linear transformations.

The curve X is also remarkable in that the q^2-power endomorphism of its Jacobian J_X is multiplication by $-q$. This follows from the following considerations. Recall that J_X is an Abelian variety representing the group of degree-zero divisors on X, modulo linear equivalence. The number of points on X defined over k is given by Weil's formula $\#X(k) = 1 + q^2 - \sum_{i=1}^{2g} a_i$ where the a_i are certain algebraic integers, the eigenvalues for the action of the q^2-power Frobenius endomorphism on an l-adic Tate module $T_l(J_X)$ (see [24]). With respect to any embedding of $\overline{\mathbb{Q}}$ in $\mathbb{C}$, the a_i all have absolute value $|k|^{1/2} = q$. This yields the Hasse–Weil upper bound $1 + q^2 + 2gq = 1 + q^3$ for $\#X(k)$. That this bound is actually attained is easily verified by changing the equation of X to $y^{q+1} = x^q z + x z^q$ then directly counting points. This compels all the a_i to be equal to $-q$. The opening statement of this paragraph follows from this.

Tate's theorem on endomorphisms of Abelian varieties over finite fields [24] now implies that J_X is isogenous over k to E^g, where E/k is any elliptic curve in the isogeny class such that the q^2-power endomorphism is multiplication by $-q$. Such elliptic curves may be constructed from elliptic curves with complex multiplication using reduction modulo $\mathfrak{p}$ (see [25]). (When $q \equiv 3 \bmod 4$, the elliptic curve $E: v^2 = u^3 - u$ is an example.) Note that E is supersingular and J_X also has maximal Newton polygon. For the number of points on a general diagonal hypersurface over a finite field see [28]. For more on Fermat varieties over finite fields, see [26] and [23].

In this paper we tackle 'descent' problems associated to the constant Abelian varieties J_X and E over the global function field $k(X)$.

Since J_X is isogenous to E^g and since $\mathrm{End}_k(E)$ (a maximal order in a quaternion algebra) has rank 4, the rank of $\mathrm{End}_k(J_X)$ is $4g^2$ and the rank of $\mathrm{Hom}_k(J_X, E)$ is $4g = 2q(q-1)$. The group $H := G \times G$ acts naturally on the endomorphism ring $\mathrm{End}_k(J_X)$ by $(g_1, g_2)\phi(x) = g_2(\phi(g_1^{-1}(x)))$. Similarly it acts on several objects we shall encounter. If we choose a k-rational point on X to embed it in its Jacobian then $\mathrm{End}_k(J_X)$ becomes identified with $\mathrm{Mor}_k(X, J_X)/\mathrm{tors.} \simeq J_X(k(X))/\mathrm{tors.}$, the group of $k(X)$-rational points on J_X, modulo torsion. This follows from the fact that every morphism from X to an Abelian variety (in particular to J_X) factors through J_X.

$\mathrm{End}_k(J_X)$ is in fact naturally an even integral lattice which we shall call L. This lattice may be identified with the interesting subgroup of the group of divisors

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

modulo numerical equivalence on the surface $X \times X$. The symmetric bilinear form is simply the intersection pairing, and is a scalar multiple of the canonical height pairing for $J_X/k(X)$.

Let Ш be the Shafarevich–Tate group for the constant Abelian variety J_X over the global function field $k(X)$. By definition,

$$Ш = \ker(H^1(k(X), J_X) \to \prod_v H^1(k(X)_v, J_X)),$$

where the cohomology is for the flat topology (see [14]) and the product is over all local completions of the function field. According to Milne's formula [12] (a special case of the analog of the Birch and Swinnerton–Dyer conjecture),

$$|Ш| \det L = (q^2)^{g^2} = q^{2g^2}.$$

The main goal of this paper is to analyse the structure of Ш and the action of the group H upon it. Let $Ш_n$ denote the set of n-torsion elements in Ш. Milne's formula shows that Ш is a finite p-group so we have a finite filtration

$$Ш_p \subset Ш_{p^2} \subset Ш_{p^3} \subset \cdots \subset Ш.$$

Each subquotient $Ш_{p^i}/Ш_{p^{i-1}}$ is an $\mathbb{F}_p[H]$-module, which in general is not completely reducible. However, we shall determine its composition factors with multiplicities, for each i. Of course, this determines the separate factors $|Ш|$ and $\det L$, and the group structure of Ш.

There is a similar problem for the Shafarevich–Tate group of the elliptic curve E over $k(X)$, where only the group G acts. In this case Milne's formula reads

$$|Ш| \det L = (q^2)^g = q^{q(q-1)},$$

where L is the Mordell–Weil lattice $E(k(X))/\text{tors.} \simeq \text{Hom}_k(J_X, E)$, of rank $4g = 2q(q-1)$. In [2] we calculated $\det L$, thus determining the order of the Shafarevich–Tate group but not its structure. In this paper we examine the filtration of Ш by the kernels of powers of the pth-power isogeny π. For each occurring irreducible $\mathbb{F}_p[G]$-module we have calculated the sequence of multiplicities, confirming that it is as predicted in [2]. In the calculation of the complete p-descent for the full Jacobian J_X, not just its factor E, we find strange patterns for the multiplicities of the $\mathbb{F}_p[H]$-modules, intimately related to those for the $\mathbb{F}_p[G]$-modules in the elliptic curve case.

We mention a simple corollary of our results.

(1) For both $J_X/k(X)$ and $E/k(X)$, Ш is trivial iff $f \leqslant 2$ (where $q = p^f$).
(2) For $J_X/k(X)$, the smallest power of p annihilating Ш is $p^{[f/3]}$. For $E/k(X)$, the smallest power of π annihilating Ш is $\pi^{[f/3]}$.

We provide full details for the Jacobian J_X, but in the elliptic curve case we confine ourselves to some remarks in Section 9 on the analogous calculation. The

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

Shafarevich–Tate group of E over the function field of a suitable hyperelliptic quotient of X may be dealt with similarly. Indeed, our prediction for the multiplicities was motivated partly by the requirement that it be consistent with bounds obtained by Elkies [4] in the hyperelliptic, characteristic 2 case.

Section 1 describes the mechanism of descent and gives the Selmer group for the multiplication-by-p^i map as the first cohomology group over X (for the flat topology) of the sheaf associated to the group-scheme kernel of p^i. Section 2 recovers this group-scheme from the Dieudonné module of J_X, which is naturally isomorphic to the first crystalline cohomology of X. All this is inspired by a letter from D. Ulmer to B. Gross explaining the elliptic curve case (see Section 4 of [27] for something closely related).

In Section 3 we derive the simple expression $\mathrm{Sel}p^i \simeq \mathrm{End}_A(H^1_{\mathrm{crys}}(X)/p^i)$, where A is the Dieudonné ring (defined in Section 2). To establish this we use several things:

(1) The identification of the first crystalline cohomology of X with the first deRham cohomology of its natural lifting X^*/W, where W is the ring of infinite Witt vectors over k.
(2) The decomposition of this W-module into rank-one eigenspaces for the action of the diagonal subgroup of G, and (following Shioda, Section 4 of [22]) the arrangement of these eigenspaces into cyclic orbits for the action of the pth-power operator F.
(3) Further information on the action of F deduced from Mazur's results on Frobenius and the Hodge filtration, as in [18] and [22].
(4) The identification (in our case) of the first crystalline cohomology of X with Serre's first Witt vector cohomology (introduced in [21]). This is what allows us to describe the Selmer groups in terms of crystalline cohomology rather than flat cohomology.

$H^1_{\mathrm{crys}}(X)/p^i$ is isomorphic to the Dieudonné module of the group-scheme $\ker p^i$. It follows that an equivalent expression for $\mathrm{Sel}p^i$ is $\mathrm{End}_k(\ker p^i)$. Therefore endomorphisms of $\ker p^i$ which do not lift to endomorphisms of J_X contribute to the p^i-torsion in the Shafarevich–Tate group. One might expect that $\mathrm{Sel}m \simeq \mathrm{End}_k(\ker m)$ for multiplication by any integer m on the Jacobian of any curve over a finite field k (considered as an Abelian variety over the function field of that curve). In the case that m is coprime to p this may be proved easily using geometric class field theory (the subject of [20]).

In Section 4 we explain how double-rowed 'circle-diagrams' may be used to label pairs of the irreducible $\mathbb{F}_p[H]$-modules which occur as composition factors of Ш. In Section 5 we state the main theorem on how the multiplicities of these irreducible modules in $Ш_{p^i}/Ш_{p^{i-1}}$ may be read off from the double-rowed circle diagrams. In Sections 6, 7 and 8 we use the expression for $\mathrm{Sel}p^i$ established in Section 3 to carry out the calculation necessary to prove the theorem.

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

1. The Descent Mechanism

Recall that the $2g$ eigenvalues of (q^2-power) Frobenius for X/k are all equal to $-q$. It follows that the number of points on the Jacobian J_X defined over the extension of degree r of k is $(1-(-q)^r)^{2g}$. This is never divisible by p, so J_X has no nontrivial p-torsion points defined over the algebraic closure of k. However, for each $i \geqslant 1$, the kernel of multiplication by p^i is well-defined as a group-scheme over k.

Associated to any commutative group-scheme G over k is a sheaf, also denoted G, on the flat site over Spec$k$ (see [14] for the flat site and its sheaf cohomology). For any scheme S locally of finite type over Spec$k$, the group of sections of G over S is simply $\mathrm{Mor}_k(S, G)$. Consider the following exact sequence of sheaves on the flat site over k

$$0 \to \ker p^i \to J_X \xrightarrow{p^i} J_X \to 0.$$

Our reason for using the flat site is to ensure that the multiplication-by-p^i map is surjective (c.f. [14] Ch. 2, 2.18). We actually have a commutative diagram with exact rows, for any $i \geqslant 1$:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \ker p^i & \longrightarrow & J_X & \xrightarrow{p^i} & J_X & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle p^{i-1}} & & \downarrow{\scriptstyle p^{i-1}} & & \downarrow{\scriptstyle \mathrm{id}} & & \downarrow \\
0 & \longrightarrow & \ker p & \longrightarrow & J_X & \xrightarrow{p} & J_X & \longrightarrow & 0.
\end{array}$$

From the long exact sequences in flat cohomology over X we may extract the following commutative diagram with exact rows (notice that $L \simeq H^0(X, J_X)/\mathrm{tors}$.):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & L/p^iL & \longrightarrow & H^1(X, \ker p^i) & \dashrightarrow & H^1(X, J_X)_{p^i} & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \mathrm{proj}} & & \downarrow{\scriptstyle p^{i-1}} & & \downarrow{\scriptstyle p^{i-1}} & & \downarrow \\
0 & \longrightarrow & L/pL & \longrightarrow & p^{i-1}H^1(X, \ker p^i) & \longrightarrow & p^{i-1}H^1(X, J_X)_{p^i} & \longrightarrow & 0.
\end{array}$$

Now it follows from the fact that the Abelian variety J_X over the function field $k(X)$ is already defined over k, that $H^1(X, \ker p^i)$ is isomorphic to the Selmer group for p^i (see [27]) and that $H^1(X, J_X)$ is isomorphic to the Shafarevich–Tate group Ш of $J_X/k(X)$ (see [12]). Therefore we take the opportunity to rewrite the bottom row as

$$0 \to L/pL \to p^{i-1}\mathrm{Sel}p^i \to p^{i-1}Ш_{p^i} \to 0.$$

The right-hand term of this sequence is isomorphic to a subfactor of Ш:

$$p^{i-1}Ш_{p^i} \simeq Ш_{p^i}/Ш_{p^{i-1}}.$$

This follows readily from the exact sequence

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

$$0 \to Ш_{p^{i-1}} \to Ш_{p^i} \xrightarrow{p^{i-1}} p^{i-1} Ш_{p^i} \to 0.$$

Therefore to determine the $\mathbb{F}_p[H]$-module composition factors (with multiplicities) of each $Ш_{p^i}/Ш_{p^{i-1}}$ it suffices to determine those of each term in the descent filtration $\mathrm{Sel}\, p \supset p\mathrm{Sel}\, p^2 \supset \cdots \supset L/pL$.

2. Dieudonné Modules and Group Schemes

We will find it necessary to use the crystalline cohomology, for which a convenient reference is [7]. Let W be the ring of infinite Witt vectors over k, so that W is the ring of integers in the unramified extension of degree $2f$ of $\mathbb{Q}_p$. W is a local ring with maximal ideal pW and residue field k. Let σ be the automorphism of $W/\mathbb{Z}_p$ which reduces mod p to the pth-power Frobenius automorphism of $k/\mathbb{F}_p$. Associated with any proper, smooth variety Z/k of dimension d are finitely generated W-modules $H^i(Z) := H^i_{\mathrm{crys}}(Z)$ which are trivial except for $0 \leqslant i \leqslant 2d$. In our case, $H^1(X)$ is a free W-module of rank $2g = q(q-1)$. It is naturally isomorphic to $H^1(J_X)$ and also to the algebraic deRham cohomology $H^1_{dR}(X^*)$, where X^*/W is the natural lifting of X, with the same equation. On this module the absolute pth-power Frobenius morphism of schemes induces a σ-linear, injective map F, so $F(av) = a^\sigma F(v)$ for $a \in W, v \in H^1(X)$. Also there is a σ^{-1}-linear map V such that $FV = VF = p$. Since in our case the eigenvalues of Frobenius over k are all $-q$, we have $F^{2f} = V^{2f} = -q = -p^f$. Let A be the Dieudonné ring, generated over W by two elements F and V satisfying the relations $FV = VF = p$, $Fa = a^\sigma F$, $Va = a^{\sigma^{-1}} V$ for all $a \in W$. Then $H^1(X)$ is naturally an A-module. According to [11], if B/k is an Abelian variety then there is a natural isomorphism of A-modules $H^1_{\mathrm{crys}}(B) \simeq D^*(B)$. Here $D^*(B) := \varprojlim D^*(\ker p^i)$ and D^* is the contravariant functor which, to a commutative group-scheme over k of p-power rank, associates a certain finite A-module, its Dieudonné module. $D^*(\ker p^i)$ may be recovered from the inverse limit as $D^*(B)/p^i D^*(B)$. In our case this implies that

$$D^*(\ker p^i) \simeq H^1(X)/p^i H^1(X).$$

It follows (see [6]) from the fact that V is nilpotent on the right-hand side that, in our case, the definition of D^* is such that

$$D^*(\ker p^i) = \mathrm{Hom}_{k-Gp}(\ker p^i, C\mathbb{W}),$$

the set of k-group scheme homomorphisms from $\ker p^i$ to the co-Witt vectors $C\mathbb{W}$. $C\mathbb{W}$ is defined to be the direct limit of the Witt vector-group schemes $\mathbb{W}_n$, with respect to the shift maps $V\colon (a_1, a_2, \ldots, a_n) \mapsto (0, a_1, \ldots, a_n)$. Recall the operator $F\colon (a_1, \ldots, a_n) \mapsto (a_1^p, \ldots, a_n^p)$ on $\mathbb{W}_n$. The action of $W = \varprojlim \mathbb{W}_n(k)$ on $\mathbb{W}_n$ by

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

multiplication maps is twisted by σ^{-n} to give (with F and V) an action of A on $C\mathbb{W}$. See [6] or [19] for more on Witt vectors.

The point of all this is that we now know the Dieudonné module $D^*(\ker p^i)$ in terms of $H^1(X)$, and the group-scheme $\ker p^i$ may be recovered from this as the object representing the functor $S \mapsto \mathrm{Hom}_A(D^*(\ker p^i), C\mathbb{W}(S))$. Here S ranges over schemes locally of finite type over Spec$k$. We will use this characterisation of $\ker p^i$ in the next section to obtain a simple expression for $\mathrm{Sel}\, p^i$.

3. F-Orbits and the Selmer Groups

We need some preliminaries on the structure of $H^1(X)$. When we identify this module with $H^1_{dR}(X^*)$ it attains a Hodge filtration $H^1_{dR}(X^*) = M_0 \supset M_1 \supset M_2 = \{0\}$ with $M_0/M_1 \simeq H^1(X^*, O_{X^*})$ and $M_1/M_2 \simeq H^0(X^*, \Omega^1)$. Let T be the diagonal subgroup of $U_3(q)$. T has order $(q+1)^3$ and its action on X/k lifts to X^*/W, replacing elements of k^* by their Teichmüller representatives in W^*.

PROPOSITION 1.

(1) *$H^0(X^*, \Omega^1)$ is a free W-module with a basis of elements which may be labelled as $w_{mnl} = x^m y^n z^l \,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z$ for all $0 \leqslant m, n, l \leqslant q-1$ with $m+n+l = q-2$.*
(2) *$H^1(X^*, O_{X^*})$ is a free W-module with a basis of elements which may be labelled as $w_{mnl} = x^m y^n z^l \,\mathrm{d}x\,\mathrm{d}y\,\mathrm{d}z$ for all $0 \leqslant m, n, l \leqslant q-1$ with $m+n+l = 2q-1$.*
(3) *Each w_{mnl} is an eigenvector for T with character* $\mathrm{diag}(a, b, c) \mapsto a^{m+1} b^{n+1} c^{l+1}$.
(4) *These characters are all distinct.*
(5) *The w_{mnl} naturally lift to a basis (also called $\{w_{mnl}\}$) for the free W-module $H^1(X) = H^1_{dR}(X^*)$, consisting of eigenvectors for T with characters as above.*

This is just Proposition 5 in Section 6 of [2].

DEFINITION 1. We define w_{mnl} to be of type k_{mnl} where

$$k_{mnl} = \begin{cases} 0 & \text{if } m+n+l = 2q-1, \\ 1 & \text{if } m+n+l = q-2. \end{cases}$$

If $0 \leqslant r \leqslant q-1$ and $r = r_0 + r_1 p + \cdots + r_{f-1} p^{f-1}$ with $0 \leqslant r_i \leqslant p-1$ then we write $r = (r_0, r_1, \ldots, r_{f-1})$ for this p-adic expansion.

PROPOSITION 2.

(1) *$F w_{mnl} = c_{mnl} w_{m'n'l'}$ with $c_{mnl} \in \mathbb{Z}_p$ and*

$$m' = (p-1-m_{f-1}, m_0, m_1, \ldots, m_{f-2}),$$

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

$$n' = (p-1-n_{f-1}, n_0, n_1, ..., n_{f-2}),$$

$$l' = (p-1-l_{f-1}, l_0, l_1, ..., l_{f-2}).$$

(2) $\mathrm{ord}_p(c_{mnl}) = k_{mnl}$.

This is Proposition 6 in Section 6 of [2]. It follows from [9] and the fact that F must multiply characters of T by p.

We introduce some useful alternative notation. Choose some element in our standard basis $\{w_{mnl}\}$ for $H^1(X)$ and call it w_1. Let $Fw_1 = c_1 w_2$, $Fw_2 = c_2 w_3$, ... with all the w_j standard basis elements. Since F^{2f} acts on $H^1(X)$ as multiplication by $-q$ we have $w_{2f+1} = w_1$ and the subscripts should really be taken $\bmod 2f$. We say that $\{w_1, w_2, ..., w_{2f}\}$ is an F-orbit of basis elements. Sometimes the length of the orbit may be a proper divisor of $2f$. Since F^f multiplies characters of T by -1 ($p^f \equiv -1 \bmod q+1$, the exponent of T), the length of the orbit does not divide f so will always be of the form $2l$ for some $l|f$.

DEFINITION 2.

(1) Define k_i to be the type of w_i.
(2) Given an F-orbit $J = \{w_1, w_2, ..., w_{2l}\}$ let $H_J := \oplus_{j=1}^{2l} W w_j \subset H^1(X)$.

LEMMA 1. *$\mathbb{W}_n$ has the same cohomology over X/k whether considered as a sheaf for the flat topology or the Zariski topology.*

Proof. H^*_{fl} and H^*_{Zar} are known to be the same for O_X-modules [14] [Ch. 3, Prop. 3.7] so the case $n = 1$ of the lemma is known to be true (note that the sheaf $\mathbb{W}_1$ on X is the same as the structure sheaf O_X). For $n > 1$ there are exact sequences (one for Zariski, one for flat) of sheaves

$$0 \to \mathbb{W}_1 \xrightarrow{V^{n-1}} \mathbb{W}_n \xrightarrow{R} \mathbb{W}_{n-1} \to 0,$$

where $R : (a_1, ..., a_{n-1}, a_n) \mapsto (a_1, ..., a_{n-1})$ is the restriction map. The long exact sequences in cohomology fit together in a commutative diagram thanks to the morphism of sites $X_{fl} \to X_{Zar}$. Now it is possible to prove the lemma using induction and a five-lemma-style argument. □

Henceforth $H^1(X, \mathbb{W}_n)$ will denote $H^1_{fl}(X, \mathbb{W}_n) = H^1_{Zar}(X, \mathbb{W}_n)$. Let $\mathbb{A}$ = adeles of $k(X)$, $\mathbb{A}(0)$ = those integral at each place of the function field $k(X)$. See [20] (II.5) for adeles (or répartitions) and for the case $n = 1$ of the next lemma.

LEMMA 2.

$$H^1(X, \mathbb{W}_n) \simeq \frac{\mathbb{W}_n(\mathbb{A})}{\mathbb{W}_n(k(X)) + \mathbb{W}_n(\mathbb{A}(0))}.$$

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

Proof. There is an exact sequence of Zariski sheaves

$$0 \to \mathbb{W}_n \to \mathbb{W}_n(k(X)) \to \mathbb{W}_n(k(X))/\mathbb{W}_n \to 0.$$

(The middle term is a constant sheaf and the next one the sheaf cokernel.) $H^1(X, \mathbb{W}_n(k(X))) = 0$ so from the long exact sequence we get

$$H^1(X, \mathbb{W}_n) \simeq \frac{H^0(X, \mathbb{W}_n(k(X))/\mathbb{W}_n)}{H^0(X, \mathbb{W}_n(k(X)))}.$$

To prove the lemma we note that

$$H^0(X, \mathbb{W}_n(k(X))/\mathbb{W}_n) \simeq \mathbb{W}_n(\mathbb{A})/\mathbb{W}_n(\mathbb{A}(0)). \qquad \square$$

PROPOSITION 3. $H^1(X, \mathbb{W}_n) \simeq H^1(X)/V^n H^1(X)$ *as A-modules.*

Proof. The restriction operator $R: \mathbb{W}_{n+1} \to \mathbb{W}_n$ induces a map $R: H^1(X, \mathbb{W}_{n+1}) \to H^1(X, \mathbb{W}_n)$ for each $n \geqslant 1$. The inverse limit of the resulting inverse system of W-modules is denoted $H^1(X, WO_X)$. It is Serre's first Witt vector cohomology [21] and is a torsion-free W-module, in fact naturally an A-module. There is a comparison theorem relating Serre's Witt vector cohomology to a part of crystalline cohomology. This was proved by Bloch [1] using algebraic K-theory, under the assumption that $p \neq 2$. Without this assumption, it was proved by Illusie using the deRham–Witt complex (and a result of Nygaard, see [8], 4.4.2). The theorem is that, up to W-torsion, $H^1(X, WO_X)$ is naturally isomorphic, as an A-module, to the largest quotient of $H^1(X)$ (crystalline) for which the 'slopes of Frobenius' lie in the interval $[0, 1)$. This is the top subfactor of the slope filtration of $H^1(X)$. In our case the eigenvalues of Frobenius on $H^1(X)$ are all $-q$. Since $\mathrm{ord}_p(-q) = (1/2)\mathrm{ord}_p(|k|)$, in our case the slopes are all $1/2$ and the top subfactor is the whole of $H^1(X)$. Hence $H^1(X) \simeq H^1(X, WO_X)$.

From the adelic description of $H^1(X, \mathbb{W}_n)$ in the previous lemma, it is clear that the restriction maps $R: H^1(X, \mathbb{W}_{n+1}) \to H^1(X, \mathbb{W}_n)$ are surjective and that $H^1(X, \mathbb{W}_n)$ may be recovered from the inverse limit by modding out by V^n. Hence the proposition. $\square$

Recall that $\mathrm{Sel}\, p^i = H^1_{fl}(X, \ker p^i)$.

PROPOSITION 4. $\mathrm{Sel}\, p^i \simeq \mathrm{Hom}_A(H^1(X), H^1(X)/p^i) = \mathrm{End}_A(H^1(X)/p^i)$.

Proof. Fix i. Since $V^{2f} = -q$ (on $H^1(X)$) we can choose some n such that $V^n = p^{i'}$ with $i' \geqslant i$. Any homomorphism from $H^1(X)/p^i H^1(X)$ to $C\mathbb{W}(S)$ is killed by V^n so factors through $\mathbb{W}_n(S)$. *Temporarily we assume that* $i = i'$. Recovering the group-scheme $\ker p^i$ from its Dieudonné module, $H^1(X)/p^i H^1(X)$, we find $\ker p^i = \oplus G_J$, a sum over F-orbits, where, for any scheme S locally of finite type over $\mathrm{Spec}k$, $G_J(S) = \mathrm{Hom}_A(H_J/p^i H_J, \mathbb{W}_n(S))$. Choose a particular F-orbit $J = \{w_1, w_2, ..., w_{2l}\}$. In the case when $S = \mathrm{Spec}R$ is affine, let ϕ be such

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

a homomorphism and for j mod $2l$ let $a_j = \phi(w_j) \in \mathbb{W}_n(R)$. There are various conditions that the a_j must satisfy in order for ϕ to be an A-homomorphism. Define $d_j = p/c_j^{\sigma^{-1}}$ so that (since $VF = p$) we have $Vw_{j+1} = d_j w_j$.

(1) ϕ is W-linear so is determined by the a_j.
(2) $\phi(Fw_j) = F\phi(w_j)$ so $c_j a_{j+1} = Fa_j$ for all j.
(3) $\phi(Vw_{j+1}) = V\phi(w_{j+1})$ so $d_j a_j = Va_{j+1}$ for all j.

Had we not assumed $i = i'$, we would also need the condition $p^i a_j = 0$ for each j. Since $FV = VF = p$, (2) and (3) will hold for all j iff (2) holds whenever $k_j = 0$ (in which case $\mathrm{ord}_p(c_j) = 0$) and (3) holds whenever $k_j = 1$ (in which case $\mathrm{ord}_p(d_j) = 0$). Thus it is necessary and sufficient (assuming (1)) that $(a_1, a_2, ..., a_{2l})$ is in the kernel of the map ψ: $(\mathbb{W}_n(R))^{2l} \to (\mathbb{W}_n(R))^{2l}$ defined by $\psi(a_1, a_2, ..., a_{2l}) = (b_1, ..., b_{2l})$ where

(1) $b_j = c_j a_{j+1} - Fa_j$ if $k_j = 0$.
(2) $b_j = d_j a_j - Va_{j+1}$ if $k_j = 1$.

Of course, the subscripts here are mod $2l$. Now ψ gives a homomorphism from the group-scheme $(\mathbb{W}_n)^{2l}$ to itself, and clearly G_J is isomorphic to the group-scheme kernel. To prove the proposition it suffices to show that $H^1_{fl}(X, G_J) \simeq \mathrm{Hom}_A(H_J, H^1(X)/p^i)$ for each F-orbit J.

The following sequence of sheaves for the flat topology is exact since, given a set of $b_j \in \mathbb{W}_n(R)$ for $1 \leqslant j \leqslant 2l$, the equations (1) and (2) above for the a_j define a finite flat extension of $\mathbb{W}_n(R)$.

$$0 \to G_J \to (\mathbb{W}_n)^{2l} \xrightarrow{\psi} (\mathbb{W}_n)^{2l} \to 0.$$

Taking the long exact sequence in cohomology we find that

$$H^1_{fl}(X, G_J) \simeq \ker(\psi) \subset \oplus_{r=1}^{2l} H^1(X, \mathbb{W}_n) = \oplus_{r=1}^{2l} H^1(X)/p^i.$$

Here we have used the fact that $H^0(X, (\mathbb{W}_n)^{2l}) = (\mathbb{W}_n(k))^{2l}$, on which the map ψ is surjective (because it is injective, $\ker p$ having no nontrivial points over k). But the conditions for an element $(v_1, ..., v_{2l}) \in \oplus_{r=1}^{2l} H^1(X)/p^i$ to be in $\ker(\psi)$ are exactly those for the W-linear map from H_J to $H^1(X)/p^i$ defined by $w_j \mapsto v_j$ to be an A-module homomorphism. Thus, in the case that $i = i'$, we get the desired isomorphisms $H^1_{fl}(X, G_J) \simeq \mathrm{Hom}_A(H_J, H^1(X)/p^i)$ and $H^1_{fl}(X, \ker p^i) \simeq \mathrm{Hom}_A(H^1(X), H^1(X)/p^i)$.

Now consider the case $i < i'$. Taking the long exact sequence in flat cohomology coming from the exact sequence of sheaves

$$0 \to \ker p^i \to \ker p^{i'} \xrightarrow{p^i} \ker p^{i'-i} \to 0,$$

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

for which the H^0's vanish, we identify $H^1_{fl}(X, \ker p^i)$ with the kernel of p^i on $H^1_{fl}(X, \ker p^{i'})$. But this is $\mathrm{Hom}_A(H^1(X),\, p^{i'-i}H^1(X)/p^{i'}H^1(X))$, and simply dividing by $p^{i'-i}$ gives us what we want. □

Notice that $\mathrm{Sel}p^i \simeq \mathrm{Hom}_A(H^1(X)/p^i, H^1(X)/p^i) \simeq \mathrm{Hom}_A\ (D^*(\ker p^i), D^*(\ker p^i))$. But D^* is an anti-equivalence of categories between the category of finite unipotent group schemes over k and the category of A-modules of finite length on which V is nilpotent (see [6]) so we have

$$\mathrm{Sel}p^i \simeq \mathrm{End}_k(\ker p^i).$$

The descent map from $J_X(k(X))/tors. \simeq \mathrm{End}_k(J_X)$ to $\mathrm{Sel}p^i$ is now obviously just restriction of endomorphisms.

4. Double-Rowed Circle Diagrams and $\mathbb{F}_p[H]$-Modules

It is our aim to give the multiplicities in each $Ш_{p^i}/Ш_{p^{i-1}}$ of the irreducible $\mathbb{F}_p[H]$-modules occurring. Recall that $H = G \times G$ and $G = \mathrm{SU}_3(q)$. These irreducible $\mathbb{F}_p[H]$-modules will be described in terms of the irreducible $k[G]$-modules occurring as composition factors of the k-vector space $H^1_{dR}(X)$. The standard basis $\{w_{mnl}\}$ for $H^1_{dR}(X^*)$ reduces mod p to a standard basis $\{v_{mnl}\}$ for $H^1_{dR}(X)$.

Let U^* be the $k[G]$-module coming from the standard action of the matrix group G on column vectors of length three. Let U be the dual $k[G]$-module. Given a $k[G]$-module V, let V^{p^i} be the $k[G]$-module obtained from V by composing the action of G with the p^i-power automorphism of $k/\mathbb{F}_p$ on matrix entries ($A \mapsto A^{(p^i)}$). If $A \in G$ then $A^{(q)} = ({}^tA)^{-1}$, so $U^q \simeq U^*$. We summarise some facts discussed in more detail in Sections 7, 8 and 9 of [2].

(1) $H^1_{dR}(X)$ has 2^f irreducible $k[G]$-module composition factors, each occurring with multiplicity one. Each is isomorphic to something of the form

$$V_0 \otimes V_1^p \otimes V_2^{p^2} \otimes \cdots \otimes V_{f-1}^{p^{f-1}},$$

where each V_i is $\mathrm{Sym}^{t_i}(U)$ or $\mathrm{Sym}^{t_i}(U^*)$ with $t_i = p-1$ or $p-2$.

(2) An irreducible factor as above is labelled by a 'string diagram' $d_0d_1...d_{f-1}$ where $d_i = X$ or O according as $t_i = p-2$ or $p-1$ respectively. The total number of X's is odd.

(3) There is a further restriction which ensures that each of the 2^{f-1} string diagrams labels precisely two composition factors, one occurring in each of the subfactors of the Hodge filtration. Namely, $d_i = X$ marks a switch from U to U^* or vice versa. For example, when $f = 4$ the string diagram $XXOX$ labels the irreducibles

$$\mathrm{Sym}^{p-2}(U) \otimes \mathrm{Sym}^{p-2}(U^{*p}) \otimes \mathrm{Sym}^{p-1}(U^{*p^2}) \otimes \mathrm{Sym}^{p-2}(U^{p^3}),$$

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

and

$$\mathrm{Sym}^{p-2}(U^*) \otimes \mathrm{Sym}^{p-2}(U^p) \otimes \mathrm{Sym}^{p-1}(U^{p^2}) \otimes \mathrm{Sym}^{p-2}(U^{*p^3}).$$

(4) If an irreducible V 'belongs' to the string diagram $d_0 d_1 ... d_{f-1}$ then V^p belongs to the string diagram $d_{f-1} d_0 ... d_{f-2}$. Hence, the two factors belonging to a single string diagram are of the form V, $V^q \simeq V^*$.

(5) There is a composition series for $H^1_{dR}(X)$ with each composition factor generated by a subset of the v_{mnl} as a k-vector space. There are f conditions on the base-p digits of m, n and l for v_{mnl} to be one of the generators for the subfactor isomorphic to a particular 'twisted tensor product'. The $(i+1)^{st}$ condition is

$$m_i + n_i + l_i = p-2 \quad \text{or} \quad p-1 \quad \text{or} \quad 2p-1 \quad \text{or} \quad 2p-2,$$

according as the $(i+1)^{st}$ factor in the twisted tensor product is

$$\mathrm{Sym}^{p-2}(U^{p^i}) \quad \text{or} \quad \mathrm{Sym}^{p-1}(U^{p^i}) \quad \text{or} \quad \mathrm{Sym}^{p-2}(U^{*p^i}) \quad \text{or} \quad \mathrm{Sym}^{p-1}(U^{*p^i})$$

respectively.

If one forgets the k-linear structure, $H^1_{dR}(X)$ becomes an $\mathbb{F}_p$-vector space of dimension $4fg$. Its irreducible composition factors as $\mathbb{F}_p[G]$-module each occur with multiplicity $2f$. These factors are labelled (up to isomorphism) by 'circle diagrams', in a one-to-one fashion. A circle diagram is what you get from a string diagram by rolling it up and joining the ends. Let's say left-to-right on the string becomes anticlockwise on the circle. If V is an irreducible $\mathbb{F}_p[G]$-module labelled by a circle diagram C then the $k[G]$-module composition factors of $V \otimes_{\mathbb{F}_p} k$ form a single $\mathrm{Gal}(k/\mathbb{F}_p)$ orbit of $2f/r$ irreducibles, where r is the order of rotational symmetry of the circle diagram. These $k[G]$-irreducibles belong to the f/r distinct string diagrams obtained by unrolling the circle. Each one, when considered as an $\mathbb{F}_p[G]$-module (forgetting the k-linear structure), contains only the composition factor labelled by C, with multiplicity r. We denote a circle diagram by placing one of its unrollings inside square brackets. For example, when $f = 3$, $[XOO] = [OXO] = [OOX]$. It is time to pass from $k[G]$-modules and $\mathbb{F}_p[G]$-modules to a consideration of $k[H]$-modules and $\mathbb{F}_p[H]$-modules.

Note that all the irreducible $k[G]$-modules considered above are absolutely irreducible. If V_1 and V_2 are irreducible $k[G]$-modules belonging to string diagrams S^1 and S^2 respectively then $\mathrm{Hom}_k(V_1, V_2)$ is an irreducible $k[H]$-module with the action of H given by $((g_1, g_2)(\phi))(x) = g_2(\phi(g_1^{-1}(x)))$. We label $\mathrm{Hom}_k(V_1, V_2)$ by the double-rowed string diagram obtained by placing S^1 directly on top of S^2. This string diagram also labels $\mathrm{Hom}_k(V_1, V_2^q)$, $\mathrm{Hom}_k(V_1^q, V_2)$ and $\mathrm{Hom}_k(V_1^q, V_2^q)$.

The double-rowed string diagram may be rolled up into a double-rowed circle diagram (again let's say that left-to-right becomes anticlockwise). This double-rowed circle diagram naturally labels an irreducible $\mathbb{F}_p[H]$-module M such that

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

the $k[H]$-module $M \otimes_{\mathbb{F}_p} k$ has composition factors labelled by the string diagrams which roll up into the circle. In fact it labels two distinct irreducible $\mathbb{F}_p[H]$-modules. $\mathrm{Hom}_k(V_1, V_2)$ and $\mathrm{Hom}_k(V_1^q, V_2^q)$ lie in one $\mathrm{Gal}(k/\mathbb{F}_p)$-orbit while $\mathrm{Hom}_k(V_1^q, V_2)$ and $\mathrm{Hom}_k(V_1, V_2^q)$ lie in another.

Since $\mathrm{Sel}p \simeq \mathrm{Hom}_A(H^1_{dR}(X), H^1_{dR}(X))$, it is clear that all the $\mathbb{F}_p[H]$-module composition factors of $Ш_{p^i}/Ш_{p^{i-1}}$ will be among those labelled by double-rowed circle diagrams.

5. The Multiplicities

We recall from [2] a way to associate a sequence of numbers, $N_1, N_2, N_3, \ldots$ to a single-rowed circle diagram C. Firstly define N_1 to be the number of X's on C. For $i \geqslant 2$, N_i depends upon the exact arrangement of these X's on the circle. The X's come in continuous unbroken runs which we may call odd runs and even runs depending on the parity of the number of crosses in a run. Distinct runs of X's are separated from each other by runs of O's. Now define a sequence $C_2, C_3, \ldots$ of circle diagrams of non-increasing size in the following way. Let $C_2 = C$. Then, for each $i \geqslant 2$, C_{i+1} is obtained from C_i by deleting all the even runs and any O which is one place clockwise of an odd run, then closing up the gaps. Define N_i to be the number of odd runs on C_i.

The N_i are all odd, and they form a non-increasing sequence which eventually stabilises in 1 when all the surviving crosses merge into a single odd run.

EXAMPLE. If $f = 19$ and $C = [OOXOOOXOOOXOXXXOXOXXO]$ then $C_3 = [OXOXOXXXXXOO]$, $C_4 = [XXXXXXXOO]$, $C_5 = [XXXXXXXO]$ and $C_6 = [XXXXXXX]$. $N_1 = 9$, $N_2 = 5$, $N_3 = 3$ and $N_i = 1$ for $i \geqslant 4$.

Recall that J_X is isogenous over k to E^g for some elliptic curve E/k, determined up to isogeny. For each $i \geqslant 1$ there is a p^i-power map $\pi^i : E \to E^{(p^i)}$, where $E^{(p^i)}$ is obtained from E by raising the coefficients of a defining equation to the p^ith power. For the statement of the following theorem, Ш denotes the Shafarevich–Tate group of $E/k(X)$.

THEOREM 1. *The multiplicity in* $Ш_{\pi^i}/Ш_{\pi^{i-1}}$ *of the irreducible* $\mathbb{F}_p[G]$*-module labelled by the circle diagram* C *is* $N_i - 1$.

Now we return to the case of $J_X/k(X)$, where we are concerned with the multiplicities in $Ш_{p^i}/Ш_{p^{i-1}}$ of the two irreducible $\mathbb{F}_p[H]$-modules labelled by a given double-rowed circle diagram. For each such circle diagram we need two sequences of numbers, (N_i^1) and (N_i^2), one for each irreducible. We get these by converting the double-rowed circle diagram C into two different single-rowed circle diagrams D^1 and D^2 (which will generally be of smaller circumference than C). Then for $r = 1, 2$, (N_i^r) is the sequence of numbers already defined for the circle diagram D^r.

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

THEOREM 2. *The irreducible $\mathbb{F}_p[H]$-modules associated with the double-rowed circle diagram C may be labelled M_1 and M_2 in such a way that the multiplicity of M_r in $Ш_{p^i}/Ш_{p^{i-1}}$ is $N_i^r - 1$.*

It remains to describe how to obtain the single-rowed circle diagrams D^1 and D^2 from the double-rowed circle diagram C (and to prove the theorem, but that is for later sections).

Recall that C is obtained by putting a string diagram S^1 on top of a string diagram S^2 then rolling up the double-rowed string diagram into a double-rowed circle diagram, left-to-right becoming anticlockwise. S^1 becomes the inner circle C^1 while S^2 becomes the outer circle C^2. For $r = 1, 2$ let $s_2^r, ..., s_f^r, s_1^r$ be the symbols (X's and O's) on S^r, listed *from right to left*, that is, moving clockwise on the circle. Just as in the single-rowed case, we use square brackets to write a circle diagram. Thus $C = \begin{bmatrix} s_1^1, s_f^1, ..., s_2^1 \\ s_1^2, s_f^2, ..., s_2^2 \end{bmatrix}$. We say that the symbols s_j^1 and s_j^2 are positioned at the jth locus, where j is considered modulo f. The double-rowed string diagram $\begin{matrix} s_j^1, s_{j-1}^1, ..., s_{j+2}^1, s_{j+1}^1 \\ s_j^2, s_{j-1}^2, ..., s_{j+2}^2, s_{j+1}^2 \end{matrix}$ is said to be the jth unrolling of C. Of course, the choice of the first unrolling (i.e. the labelling of the symbols) is somewhat arbitrary.

DEFINITION 3. Each s_j^r is either X or O. Define s_j^r to be an isolated cross iff $s_j^r = X$ but $s_j^{3-r} = O$. The double-rowed circle diagram C is said to be pure iff it has no isolated crosses.

The total number of isolated crosses on C is even, since C^1 and C^2 each has an odd number of crosses. As we move clockwise around C we get a repeating sequence of isolated crosses. Assuming the circle diagram is not pure, there are precisely two distinct ways to arrange these isolated crosses into pairs of consecutive isolated crosses. Any particular isolated cross may be paired with either the previous one or the next one. Suppose that we have chosen such a pairing. Let $s_{j_1}^{r_1}$ and $s_{j_2}^{r_2}$ form one of our pairs of consecutive isolated crosses. All symbols positioned at loci from j_1 to j_2 inclusive will be said to form a 'chunk'. Each chunk contains an even number of crosses and will be called an even chunk or an odd chunk according as it has even or odd numbers of crosses on each row.

Now we describe how to get the single-rowed circle diagrams D^1 and D^2 from C, one for each way of pairing the isolated crosses. Delete each even chunk and replace it by $\begin{matrix} O \\ O \end{matrix}$. Also delete each odd chunk and replace it by $\begin{matrix} X \\ X \end{matrix}$. At this point we have a pure circle diagram. Replacing now $\begin{matrix} X \\ X \end{matrix}$ by X and $\begin{matrix} O \\ O \end{matrix}$ by O, we get the single-rowed circle diagram. We have to proceed slightly differently if C is already pure. Get D^1 by replacing $\begin{matrix} O \\ O \end{matrix}$ by O and $\begin{matrix} X \\ X \end{matrix}$ by X, and just let $D^2 = [X]$.

EXAMPLE. When $f = 15$ consider $C = \begin{bmatrix} XOXXOXXOXXOXOOX \\ OOXOXXXOOOOXXOX \end{bmatrix}$. C may be chunked as follows (with round brackets about each chunk):

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

$$C = \left[\begin{matrix}(XOXX)(OXXOX)(XOXO)OX\\(OOXO)(XXXOO)(OOXX)OX\end{matrix}\right].$$

This leads to the pure circle diagram $\left[\begin{smallmatrix}XXOOX\\XXOOX\end{smallmatrix}\right]$ then to $D^1 = [XXOOX]$.

Unrolling three places further clockwise we may write

$$C = \left[\begin{matrix}OOXXOXXOXXOXXOX\\XOXOOXOXXXOOOOX\end{matrix}\right],$$

then the other chunking is

$$C = \left[\begin{matrix}(OOXX)OX(XO)XXO(XX)OX\\(XOXO)OX(OX)XXO(OO)OX\end{matrix}\right].$$

This leads to the pure circle diagram $\left[\begin{smallmatrix}OOXXXXOOOX\\OOXXXXOOOX\end{smallmatrix}\right]$, then to

$$D^2 = [OOXXXXOOOX].$$

Notice that the lengths of D^1 and D^2 add up to f. The reader will easily confirm that this always happens. Also, each D^r has an odd number of crosses on it, since in the passage from C to the pure circle diagram, an even number of crosses is deleted from each row.

Now $N_1^1 = 3$ and $N_i^1 = 1$ for $i \geqslant 2$, while $N_1^2 = 5$ and $N_i^2 = 1$ for $i \geqslant 2$. According to Theorem 2, the two irreducible $\mathbb{F}_p[H]$-modules belonging to C may be labelled M_1 and M_2 in such a way that the multiplicities of M_1 and M_2 as composition factors of $Ш_p$ are 2 and 4 respectively. Both have multiplicity zero in $Ш_{p^i}/Ш_{p^{i-1}}$ for any $i \geqslant 2$.

In general, exactly which $\mathbb{F}_p[H]$-module corresponds to which chunking of C should become apparent during the proof of Theorem 2. For now we just deal with the previous example to illustrate the recipe. Recall that each irreducible $\mathbb{F}_p[H]$-module corresponds to a $\mathrm{Gal}(k/\mathbb{F}_p)$-orbit of irreducible $k[H]$-modules. In the above example, the chunking leading to D^1 corresponds to the irreducible $\mathbb{F}_p[H]$-module whose associated orbit of irreducible $k[H]$-modules contains

$$\mathrm{Hom}_k(\mathrm{Sym}^{p-2}(U) \otimes \cdots \otimes \mathrm{Sym}^{p-2}(U^{p^{14}}),$$
$$\mathrm{Sym}^{p-1}(U^*) \otimes \cdots \otimes \mathrm{Sym}^{p-2}(U^{p^{14}})).$$

The chunking leading to D^2 corresponds to the irreducible $\mathbb{F}_p[H]$-module whose associated orbit of irreducible $k[H]$-modules contains

$$\mathrm{Hom}_k(\mathrm{Sym}^{p-1}(U) \otimes \cdots \otimes \mathrm{Sym}^{p-2}(U^{*p^{14}}),$$
$$\mathrm{Sym}^{p-2}(U^*) \otimes \cdots \otimes \mathrm{Sym}^{p-2}(U^{*p^{14}})).$$

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

We use here the same unrollings as above. The important thing is that at the clockwise (left) end of a chunk the symmetric powers involve both U and U^*.

6. Equations for the Selmer Groups

The proof of Theorem 2 will be spread across this and the following two sections. Recall that there is a finite descent filtration

$$\mathrm{Sel}p \supset p\mathrm{Sel}p^2 \supset p^2\mathrm{Sel}p^3 \supset \cdots \supset L/pL.$$

Suppose that we could show that the multiplicity of M_r in $p^{i-1}\mathrm{Sel}p^i$ is N_i^r. Since the N_i^r's eventually become 1, this would show that the multiplicity of M_r in L/pL is one. Then the exact sequence

$$0 \to L/pL \to p^{i-1}\mathrm{Sel}p^i \to p^{i-1}Ш_{p^i} \to 0$$

would imply that the multiplicity of M_r in $Ш_{p^i}/Ш_{p^{i-1}}$ is $N_i^r - 1$, as desired. Hence our aim is to show that the multiplicity of M_r in $p^{i-1}\mathrm{Sel}p^i$ is N_i^r. We know from Section 3 that $\mathrm{Sel}p^i \simeq \mathrm{End}_A(H^1(X)/p^i)$. Before exploring the consequences of this, we set some notation.

Let $C = \begin{bmatrix} s_1^1, s_f^1, \ldots, s_2^1 \\ s_1^2, s_f^2, \ldots, s_2^2 \end{bmatrix}$ be some particular double-rowed circle diagram. The first unrolling of C is a double-rowed string diagram labelling an irreducible $k[H]$-module $\mathrm{Hom}_k(V_1, V_2)$ (and three others). Here V_1 and V_2 are subfactors of $H^1_{dR}(X)$, each generated by a subset of the set $\{v_{mnl}\}$ of standard basis elements for $H^1_{dR}(X)$. These lift to subsets of the set $\{w_{mnl}\}$ of standard basis elements for $H^1(X)$.

Let w_1^1 be the standard basis element for $H^1(X)$ lifting some standard basis element v_1^1 for an irreducible $k[G]$-module V_1 labelled by the first unrolling of the inner circle C^1. There are, of course, many possible choices for v_1^1. Once chosen, w_1^1 generates an F-orbit $\{w_1^1, \ldots, w_{2f}^1\}$. Say $Fw_1^1 = c_1^1 w_2^1$, $Fw_2^1 = c_2^1 w_3^1$, ... For $j \bmod 2f$ we say that w_j^1 *belongs* to the symbol s_j^1 on C^1. Recall that for symbols the subscripts run $\bmod f$, so w_j^1 and w_{j+f}^1 both belong to s_j^1. Similarly we choose w_1^2 lifting a basis element v_1^2 for an irreducible $k[G]$-module V_2 labelled by the first unrolling of the outer circle C^2. Then we get an F-orbit of w_j^2's belonging to the symbols s_j^2, with $Fw_j^2 = c_j^2 w_{j+1}^2$.

DEFINITION 4. Define $d_j^r := p/c_j^{r\sigma^{-1}}$ so that $Vw_{j+1}^r = d_j^r w_j^r$. Also define $k_j^r := \mathrm{ord}_p(c_j^r)$. This is all for $r = 1$ or 2. Let $k_j := k_j^2 - k_j^1$. It may be 0, 1 or -1.

The basis $\{w_{mnl}\}$ for $H^1(X)$ gives rise to a dual basis $\{w_{mnl}^*\}$ for $\mathrm{Hom}_W(H^1(X), W)$. Starting from $w_1^{1*} \otimes w_1^2$ we get an 'F-orbit' $\{w_j^{1*} \otimes w_j^2\}$ of standard basis elements for $\mathrm{End}_W(H^1(X))$ or $\mathrm{End}_W(H^1(X)/p^i)$. $w_j^{1*} \otimes w_j^2$ 'belongs' to the jth locus.

Since $\mathrm{Sel}p^i = \mathrm{End}_A(H^1(X)/p^i)$, each element of $\mathrm{Sel}p^i$ is a sum of elements of $\mathrm{Sel}p^i$ supported on single F-orbits of standard basis elements for $\mathrm{End}_W(H^1(X)/p^i)$.

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

Therefore we choose a fixed F-orbit and just consider elements of $\mathrm{Sel}p^i$ supported on that F-orbit. Let $\phi = \sum a_j w_j^{1*} \otimes w_j^2$ be such an element. So for each j modulo the length of the orbit, $\phi(w_j^1) = a_j w_j^2$. Each coefficient a_j is in W/p^iW.

DEFINITION 5. If $a_j \neq 0$, let b_j be the image of $a_j/p^{\mathrm{ord}_p(a_j)}$ in $W/pW \simeq k$ (this is well-defined). If $a_j = 0$ then set $b_j = 0$. If $a_j \neq 0$ then $\mathrm{ord}_p(a_j) < i$ is well-defined. If we say $\mathrm{ord}_p(a_j) = n$ for some $n \geqslant i$, we shall mean that $a_j = 0$.

For the W-endomorphism ϕ to be an A-endomorphism it is necessary and sufficient that it commute with F and V. This is equivalent to certain equations for the coefficients a_j. $Fw_j^1 = c_j^1 w_{j+1}^1$ so $\phi(Fw_j^1) = c_j^1 a_{j+1} w_{j+1}^2$. On the other hand, $\phi(w_j^1) = a_j w_j^2$ so $F\phi(w_j^1) = a_j^\sigma c_j^2 w_{j+1}^2$. Comparing coefficients gives us

$$a_{j+1} c_j^1 = a_j^\sigma c_j^2. \tag{1}$$

A similar computation using V instead of F leads to the equation

$$a_j d_j^1 = a_{j+1}^{\sigma^{-1}} d_j^2. \tag{2}$$

Formally either equation gives us

$$\mathrm{ord}_p(a_{j+1}) = \mathrm{ord}_p(a_j) + k_j \tag{3}$$

but we have to be careful about things becoming 0 in W/p^iW. The cases are examined below.

(1) If $k_j = 0$ (i.e. $k_j^1 = k_j^2$) then one of the equations (1) and (2) genuinely links a_j with a_{j+1}. Either $\mathrm{ord}_p(a_j) = \mathrm{ord}_p(a_{j+1})$ or $a_j = a_{j+1} = 0$. Either one of a_j and a_{j+1} determines the other, and of course a similar statement is true of b_j and b_{j+1}.
(2) If $k_j = 1$ (i.e. $k_j^1 = 0$ and $k_j^2 = 1$) then a_j determines a_{j+1} and $\mathrm{ord}_p(a_{j+1}) = \mathrm{ord}_p(a_j)+1$. b_j determines b_{j+1}. If $a_{j+1} = 0$ then $b_{j+1} = 0$ does not determine b_j, though $\mathrm{ord}_p(a_j)$ must be at least $i-1$. If $a_{j+1} \neq 0$ then b_{j+1} determines b_j.
(3) If $k_j = -1$ (i.e. $k_j^2 = 0$ and $k_j^1 = 1$) then a_{j+1} determines a_j and $\mathrm{ord}_p(a_j) = \mathrm{ord}_p(a_{j+1}) + 1$. b_{j+1} determines b_j. If $a_j = 0$ then $b_j = 0$ does not determine b_{j+1}, though $\mathrm{ord}_p(a_{j+1})$ must be at least $i-1$. If $a_j \neq 0$ then b_j determines b_{j+1}.

7. Pure Circle Diagrams

Recall that a pure circle diagram is one with no isolated crosses, so the inner and

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

outer circles C^1 and C^2 are the same. The following fact is implied by (3) of Section 4, and will be of the utmost importance in all that follows.

LEMMA 3. *For $r = 1$ or 2, $k_j^r \neq k_{j-1}^r$ iff $s_j^r = X$.*

Thus, as we move clockwise along the r^{th} row of the circle diagram, k_j^r switches from 0 to 1 or vice versa precisely whenever we hit a cross. If C happens to be a pure circle diagram, this implies that k_j^1 and k_j^2 will either always be equal or always be unequal.

PROPOSITION 5. *If our chosen F-orbit $\{w_j^{1*} \otimes w_j^2\}$ is such that $k_j^1 = k_j^2$ for all j, then for all i, the multiplicity of the associated $\mathbb{F}_p[H]$-module in $p^{i-1}\mathrm{Sel}p^i$ is* 1.

Proof. $k_j = 0$ for all j, so by (1) of the previous section, a_j determines a_{j+1} and $\mathrm{ord}_p(a_j) = \mathrm{ord}_p(a_{j+1})$ for all j. In fact we get a continuous chain of equations linking all the a_j to each other. Suppose that $\sum a_j w_j^{1*} \otimes w_j^2$ is an element of $\mathrm{Sel}p^i = \mathrm{End}_A(H^1(X)/p^i)$. To map it to $p^{i-1}\mathrm{Sel}p^i$ inside $\mathrm{Sel}p = \mathrm{End}_A(H^1(X)/p)$ we simply reduce the coefficients modulo p. From all the elements of $\mathrm{Sel}p^i$ for which $\mathrm{ord}_p(a_j) = 0$ (for all j) we get a one-dimensional $\mathbb{F}_{p^{2l}}$-vector subspace of $p^{i-1}\mathrm{Sel}p^i$, where $2l$ is the length of the F-orbit. Note that the chain of equations eventually links a_1 to itself $a_1^{\sigma^{2l}} = \gamma a_1$, for some $\gamma \in W$ which depends on the c_j^r. It follows from the fact that $F^{2f} = -q$ on $H^1(X)$ that $\mathrm{Norm}_{W/W(\mathbb{F}_{p^{2l}})}(\gamma) = 1$, then Hilbert's Theorem 90 provides us with the solutions we need to get the one-dimensional $\mathbb{F}_{p^{2l}}$-vector subspace of $p^{i-1}\mathrm{Sel}p^i$.

Notice that the $\mathbb{F}_p$-dimension contributed is $2l$, the same as the number of W-basis elements in the F-orbit. Therefore each irreducible $k[H]$-module (of the type labelled by a double-rowed string diagram) contributes an $\mathbb{F}_p$-dimension equal to its dimension d as a k-vector space. If r is the order of rotational symmetry of the circle diagram then there are $4f/r$ irreducible $k[H]$-modules. Half of these are in the $\mathrm{Gal}(k/\mathbb{F}_p)$-orbit associated with that irreducible $\mathbb{F}_p[H]$-module (M_2, say) belonging to C which is distinguished from the other one (M_1) by the condition $k_j^1 = k_j^2$. The total contribution from F-orbits belonging to M_2 is an $\mathbb{F}_p$-dimension of $d.2f/r$. Since this is exactly the $\mathbb{F}_p$-dimension of M_2, we see that the multiplicity of M_2 in $p^{i-1}\mathrm{Sel}p^i$ is one, the same as the number of chains of equations coming from each of the F-orbits involved. □

We convene that the single-rowed circle diagram associated to M_2 is $[X]$, so all the N_i^2 are equal to 1 and the above proposition is in accord with Theorem 2. The next proposition is the heart of the proof of Theorem 2.

PROPOSITION 6. *If our chosen F-orbit $\{w_j^{1*} \otimes w_j^2\}$ is such that for all j, $k_j^1 \neq k_j^2$, then for all i the multiplicity in $p^{i-1}\mathrm{Sel}p^i$ of the associated $\mathbb{F}_p[H]$-module M_1 is N_i^1.*

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

We need to make some preparations before embarking on the proof. The circle diagram C is pure, so $C^1 = C^2$. There are two single-rowed circle diagrams which may be derived from C. In the previous proposition we dealt with $D^2 = [X]$. Now we are dealing with $D^1 = C^1 = C^2$. Recall that there is a sequence $D^1 = D_2^1, D_3^1, D_4^1, \ldots$ of circle diagrams such that N_1^1 is the number of crosses on D^1 and, for $i \geqslant 2$, N_i^1 is the number of odd runs of crosses on D_i^1. For $i \geqslant 2$, D_{i+1}^1 is obtained from D_i^1 by deleting all the even runs of X's and deleting any O which is one place clockwise of an odd run of X's.

DEFINITION 6. For $j_1, j_2 \bmod 2f$ let $R(j_1, j_2) = \sum_{j_1 \leqslant j < j_2} k_j$. The inequality means all those j we encounter moving clockwise from j_1 before we hit j_2.

The point of this definition is that if $\sum a_j w_j^{1*} \otimes w_j^2$ is an element of $\mathrm{Sel}\, p^i$, and if a_{j_1} and a_{j_2} are linked by an unbroken chain of equations, then $\mathrm{ord}_p(a_{j_2}) = \mathrm{ord}_p(a_{j_1}) + R(j_1, j_2)$. This clearly follows from the relation $\mathrm{ord}_p(a_{j+1}) = \mathrm{ord}_p(a_j) + k_j$. Note that since $k_j^1 \neq k_j^2$, k_j is always ± 1.

Given any symbol on D^1 we may trace its history as we advance through the sequence $D_2^1, D_3^1, D_4^1, \ldots$. At some point it may be deleted, but we may talk of a cross on D^1 as being on D_i^1, if it survives that far.

Fix j_1 and imagine what happens to $R(j_1, j_2)$ as j_2 moves clockwise around the circle. When $k_{j_2} = 1$, $R(j_1, j_2)$ is increasing. When $k_{j_2} = -1$, $R(j_1, j_2)$ is decreasing. k_{j_2} switches sign whenever we pass a cross. So as we pass through a run of X's, $R(j_1, j_2)$ oscillates up and down in steps of size one, but as we pass through a run of O's, $R(j_1, j_2)$ steadily increases or decreases, according as k_{j_2} is stuck on 1 or -1. Bearing in mind these observations, the proof of the following lemma is straightforward.

LEMMA 4.

(1) *If $s_{j_1} = X$ and $s_{j_2} = X$ are the beginning and end of an even run of X's then $R(j_1 - 1, j_2) = 0$ and $k_{j_1 - 1} = k_{j_2}$. It is as if the even run wasn't there.*
(2) *If $s_{j_1} = X$ and $s_{j_2} = X$ are the beginning and end of an odd run of X's then $R(j_1, j_2) = 0$ and $k_{j_1 - 1} \neq k_{j_2}$.*
(3) *If $s_{j_1} = X$ and $s_{j_2} = X$ survive to be the beginnings of successive odd runs on D_i^1 then $k_{j_1} \neq k_{j_2}$.*
(4) *Suppose that $s_{j_1} = X$ and $s_{j_2} = X$ survive to be the beginning and end of an odd run of X's on D_i^1. Let $s_{j_3} = X$ be the symbol which survives to be the beginning of the next odd run of X's on D_i^1. Suppose that $k_{j_1} = 1$. Then $R(j_1, j) < i$ for all $j_1 \leqslant j \leqslant j_2$, $R(j_1, j) \geqslant 0$ for all $j_1 \leqslant j \leqslant j_3$ and $R(j_1, j_3) \geqslant i$.*
(5) *Same hypotheses as previous item except $k_{j_1} = -1$. Then $R(j_1, j) > -i$ for all $j_1 \leqslant j \leqslant j_2$, $R(j_1, j) \leqslant 0$ for all $j_1 \leqslant j \leqslant j_3$ and $R(j_1, j_3) \leqslant -i$.*

Note that (3), (4) and (5) hold even for $i = 1$ if we make the convention that $D_1^1 = D^1$, with every X considered to be an odd run.

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

Proof of Proposition 6. Again we focus on elements $\sum a_j w_j^{1*} \otimes w_j^2$ of $\mathrm{Sel}p^i$ supported on a single F-orbit. Only coefficients a_j such that $\mathrm{ord}_p(a_j) = 0$ will contribute anything to $p^{i-1}\mathrm{Sel}p^i \subset \mathrm{Sel}p$. (Recall that the map from $\mathrm{End}_A(H^1(X)/p^i)$ to $\mathrm{End}_A(H^1(X)/p)$ is given by reduction mod p of coefficients.) Let $s_{j_0}, s_{j_1}, s_{j_3} = X$ be symbols on D^1 which survive to be the beginnings of successive odd runs of X's on D_i^1 (possibly with even runs in between). Let $s_{j_2} = X$ be the symbol on D^1 which survives to be the (clockwise) end of the odd run which starts with s_{j_1}. Choose $k_{j_1} = 1$, so $k_{j_0} = k_{j_3} = -1$ and $k_{j_2} = 1$.

For $j < j' \bmod 2f$, $\mathrm{ord}_p(a_{j'}) = \mathrm{ord}_p(a_j) + R(j, j')$ if $a_{j'} \neq 0$ in W/p^iW for all $j \leqslant j' \leqslant j'$. Bearing in mind this and the above lemma, we may argue as follows. $0 \leqslant R(j_1, j) < i$ for $j_1 \leqslant j \leqslant j_2$. Hence, if $\mathrm{ord}_p(a_{j_1}) = 0$ then all the a_j for $j_1 \leqslant j \leqslant j_2$ are non-zero and are linked to a_{j_1} in a chain of equations. In fact b_{j_1} determines all the b_j for $j_1 \leqslant j \leqslant j_2$. However, $\mathrm{ord}_p(a_j) > 0$ for $j_2 < j \leqslant j_3$, and, using case (2) at the end of the previous section, $a_{j_3} = 0$ since $R(j_1, j_3) \geqslant i$. Hence the chain of equations gets broken. Now we look at what happens anticlockwise of j_1. Since $R(j_0, j_1) \leqslant -i$ we find that $a_{j_0} = 0$. Another way of looking at this is that the condition $a_{j_0} = 0$ forced by the previous equation break is consistent with allowing $\mathrm{ord}_p(a_{j_1}) = 0$. Also, $\mathrm{ord}_p(a_j) > 0$ for $j_0 \leqslant j < j_1$ so even though some of these coefficients may be non-zero and independent of a_{j_1}, they do not contribute anything to $p^{i-1}\mathrm{Sel}p^i$.

For each odd run of X's on D_i^1 we have a single chain of equations. All the coefficients contributing to $p^{i-1}\mathrm{Sel}p^i$ depend upon a_{j_1}. It follows that the multiplicity of the irreducible $\mathbb{F}_p[H]$-module M_1 in $p^{i-1}\mathrm{Sel}p^i$ is the number of odd runs on D_i^1, namely N_i^1. Note that this argument works even when $i = 1$, when the multiplicity is the number of X's on D^1. If a single chain of equations goes right around the circle we may use Hilbert 90 as before. □

8. Non-Pure Circle Diagrams

We complete the demonstration of Theorem 2 by reducing the general case to that dealt with in the previous section. We now consider an element $\sum a_j w_j^{1*} \otimes w_j^2$ of $\mathrm{Sel}p^i$, supported on an F-orbit belonging to a circle diagram C which is not pure. In fact the F-orbit belongs to a particular chunking of C (recall that there are two, one for each irreducible $\mathbb{F}_p[H]$-module labelled by C). This chunking is determined by the condition that $k_j^1 \neq k_j^2$ if the jth locus is the last in a chunk (i.e. at the clockwise end of a chunk). Using the fact that $k_j^r \neq k_{j-1}^r$ iff $s_j^r = X$, it is easy to see that this condition does not depend on the particular chunk (for a given chunking). In fact we easily verify the following lemma.

LEMMA 5. *Let j_0 and j_1 be the first and last loci in a chunk (so the j_0^{th} locus is at the anticlockwise end, the j_1^{th} locus is at the clockwise end).*

(1) $k_{j_1}^1 \neq k_{j_1}^2$.
(2) $k_j^1 = k_j^2$ *for* $j_0 \leqslant j < j_1$.

https://doi.org/10.1023/A:1001721808335 Published online by Cambridge University Press

(3) *(Hence)* $\mathrm{ord}_p(a_j)$ *is constant for* $j_0 \leqslant j \leqslant j_1$.

(4) $(k^1_{j_1}, k^2_{j_1}) = \begin{cases} (k^1_{j_0-1}, k^2_{j_0-1}) & \text{if the chunk is even;} \\ (1-k^1_{j_0-1}, 1-k^2_{j_0-1}) & \text{if the chunk is odd.} \end{cases}$

(3) shows that nothing happens to $\mathrm{ord}_p(a_j)$ within a chunk. (4) shows that the effect of the whole chunk on the k^r_j is the same as that of $\begin{smallmatrix} O \\ O \end{smallmatrix}$ if it is an even chunk, or $\begin{smallmatrix} X \\ X \end{smallmatrix}$ if it is an odd chunk. Hence we may replace each chunk by $\begin{smallmatrix} O \\ O \end{smallmatrix}$ or $\begin{smallmatrix} X \\ X \end{smallmatrix}$ as appropriate, and we are reduced to the case of a pure circle diagram with all the $k^1_j \neq k^2_j$.

9. Remarks on the Elliptic Curve Case

We make some brief remarks on the proof of Theorem 1. For simplicity we assume that we are in the case where E is defined over $\mathbb{F}_p$, though this is not necessary for the truth of the theorem. Then the pth-power isogeny π maps E to itself. Arguments similar to those in Section 3 show that $\mathrm{Sel}\pi^i \simeq \mathrm{Hom}_A(H^1(E), H^1(X)/V^i)$ which in turn is the kernel of $F+V$ on $H^1(X)/V^i$. We can focus on elements which are supported on an F-orbit (of standard basis elements for $H^1(X)$), and obtain chains of equations as before. Then we just have to count the chains of equations to get the desired multiplicities. The fact that we are modding out by V^i rather than p^i causes some difficulty, though on the whole things are a little simpler.

When $i = 1$ or 2 a different approach can be made to work. As in [5] (Section 14), $\mathrm{Sel}\pi$ may be identified with the space of exact holomorphic differentials on X, which can be calculated as the kernel of the Cartier operator. $\ker \pi^i$ may be recovered from the Dieudonné module of E as the kernel of $F+V$ on the group-scheme $\mathbb{W}_i$. $\mathrm{Sel}\pi^i$ is then identified with the kernel of $F+V$ on $H^1_{Zar}(X, \mathbb{W}_i)$. To determine $\pi\,\mathrm{Sel}\pi^2$ inside $\mathrm{Sel}\pi$ we may apply Serre duality, using an observation of Ulmer ([27], Section 4, between (4.4) and (4.5)). Using an explicit basis for $H^0(X, \Omega^1)$, all residues may be moved to the point at infinity, then an elaborate calculation with Laurent series recovers the case $i = 2$ of Theorem 1. The details are in [3]. The case $i > 2$ does not yield to the same method.

Acknowledgements

I attempted to solve the descent problem in the elliptic curve case for my PhD thesis, which was supervised by B. Gross. The idea that it should be possible to proceed using crystalline cohomology is due to him, as is the recognition that representations modulo p are important. The first descent appears in Section 14 of [5]. I acknowledge the generous help on this problem provided to me by him and also by N. Elkies and D. Ulmer.

References

1. Bloch, S.: Algebraic K-theory and crystalline cohomology, *IHES Publ. Math.* **47** (1977), 187–268.
2. Dummigan, N.: The determinants of certain Mordell–Weil lattices, *Amer. J. Math.* **117** (1995), 1409–1429.
3. Dummigan, N.: The second descent for certain families of Mordell–Weil lattices, PhD thesis, Harvard University, April 1993.
4. Elkies, N. D.: Papers in preparation on Mordell–Weil lattices.
5. Gross, B. H.: Group representations and lattices, *J. Amer. Math. Soc.* **3** (1990), 929–960.
6. Grothendieck, A.: *Groupes de Barsotti-Tate et Cristaux de Dieudonné*, Les Presses de l'Université de Montréal, 1974.
7. Illusie, L.: Report on crystalline cohomology, *Proc. Symp. Pure Math.* **29** (1975), 459–478.
8. Illusie, L.: Complexe de de Rham-Witt, *Asterisque* **63** (1979), 83–112.
9. Mazur, B.: Frobenius and the Hodge filtration, *Bull. Amer. Math. Soc.* **78** (1972), 653–667.
10. Mazur, B.: Frobenius, and the Hodge filtration (estimates), *Ann. Math.* **98** (1973), 58–95.
11. Mazur, B. and Messing, W.: *Universal Extensions and One Dimensional Crystalline Cohomology*, Lecture Notes in Math. 370, Springer-Verlag, New York, 1970.
12. Milne, J. S.: The Tate-Shafarevich group of a constant abelian variety, *Invent. Math.* **6** (1968), 91–105.
13. Milne, J. S.: Jacobian varieties, In: G. Cornell and J. H. Silverman (eds), *Arithmetic Geometry*, Springer-Verlag, New York, 1986.
14. Milne, J. S.: *Étale Cohomology*, Princeton University Press, 1980.
15. Milne, J. S.: On a conjecture of Artin and Tate, *Ann. Math.* **102** (1975), 517–533.
16. Kolyvagin, V. A.: On the structure of Shafarevich–Tate groups. In: *Algebraic Geometry (Chicago, IL, 1989)*, Lecture Notes in Math. 1479, Springer, Berlin, 1991, pp. 94–121.
17. Kolyvagin, V. A. and Logachev, D. Y.: Finiteness of the Shafarevich–Tate group and group of rational points for some modular abelian varieties (Russian), *Algebra i Analiz* **1**(5) (1989), 171–196; English translation in *Leningrad Math. J.* **1**(5) (1990), 1229–1253.
18. Ogus, A.: Griffiths transversality in crystalline cohomology, *Ann. Math.* **108** (1978), 395–419.
19. Serre, J.-P.: *Local Fields*, Springer-Verlag, New York, 1979.
20. Serre, J.-P.: *Algebraic Groups and Class Fields*, Springer-Verlag, New York, 1988.
21. Serre, J.-P.: Sur la topologie des variétés algébriques en caractéristique p, *Symp. Int. Top. Algebra*, Mexico, 1958, pp. 24–53.
22. Shioda, T.: Mordell–Weil lattices and sphere-packings, *Amer. J. Math.* **113** (1991), 931–948.
23. Shioda, T. and Katsura, T.: On Fermat varieties, *Tohoku Math. J. (2)* **31** (1979), 97–115.
24. Tate, J.: Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966), 134–144.
25. Tate, J.: Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda), *Sém. Bourbaki* **352** (1968).
26. Tate, J.: Algebraic cycles and poles of zeta functions, In: O. F. G. Schilling (ed.), *Arithmetical Algebraic Geometry*, Harper and Row, New York, 1965, pp. 93–110.
27. Ulmer, D. L.: p-descent in characteristic p, *Duke Math. J.* **62** (1991), 237–265.
28. Weil, A.: Numbers of solutions of equations in finite fields, *Bull. Amer. Math. Soc.* **55** (1949), 497–508.