Mathematical Research Letters **10**, 747–762 (2003)

TAMAGAWA FACTORS FOR SYMMETRIC SQUARES OF TATE CURVES

Neil Dummigan

Abstract. We consider the l-part of the Bloch-Kato conjecture for $L(\mathrm{Sym}^2(E), 2)$, where E is an elliptic curve with multiplicative reduction at l. Determining the l-part of the Tamagawa factor at l allows us to deduce a partial result and obtain some numerical evidence.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Consider first the case that N is square-free, i.e. that E is semi-stable. For each prime number $p \nmid N$ let α_p and β_p be the eigenvalues of a geometric Frobenius element Frob_p acting on an l-adic Tate module $T_l(E)$, for any prime $l \neq p$. If $p \mid N$ let $\beta_p = 0$ and

$$\alpha_p = \begin{cases} +1 & \text{if } E \text{ has split multiplicative reduction at } p; \\ -1 & \text{if } E \text{ has non-split multiplicative reduction at } p. \end{cases}$$

The L-function attached to E is described by the following Euler product for $\Re(s) > 3/2$:

$$L(E, s) = \prod_p \frac{1}{(1 - \alpha_p p^{-s})(1 - \beta_p p^{-s})}.$$

Thanks to the modularity of E [Wi],[TW], it is known that $L(E, s)$ is entire and satisfies a functional equation relating its values at s and $2 - s$.

The symmetric square L-function attached to E is described by the following Euler product for $\Re(s) > 2$.

$$L(\mathrm{Sym}^2(E), s) = \prod_p \frac{1}{P_p(p^{-s})} := \prod_p \frac{1}{(1 - \alpha_p^2 p^{-s})(1 - \alpha_p \beta_p p^{-s})(1 - \beta_p^2 p^{-s})}.$$

It is known [Sh1] that it is entire and satisfies the functional equation

$$\Lambda(\mathrm{Sym}^2(E), s) = \Lambda(\mathrm{Sym}^2(E), 3 - s), \tag{1}$$

where

$$\Lambda(s) := N^s (2\pi)^{-s} \Gamma(s) \pi^{-s/2} \Gamma(s/2) L(\mathrm{Sym}^2(E), s).$$

Received September 10, 2002.
2000 *Mathematics Subject Classification.* 11G40, 14G10.
Key words and phrases. elliptic curve, symmetric square L-function, Bloch-Kato conjecture.

The gamma factors in the functional equation force $L(\mathrm{Sym}^2(E), s)$ to vanish at all integer points $s \leq 0$. These points at which there are trivial zeros, together with the integer points $s \geq 3$ with which they are paired by the functional equation, are said to be non-critical. The remaining integer points $s = 1$ and $s = 2$ (which are, of course, paired by the functional equation) are the critical points.

In the case where N is not square-free, the Euler factors in $L(\mathrm{Sym}^2(E), s)$ at primes p such that $p^2 \mid N$ are a bit more tricky to make explicit. See [CS] and [Wa]. The proof of the modularity of E was completed in [BCDT]. For the proof in general of the functional equation for $L(\mathrm{Sym}^2(E), s)$ see [GJ] or [CS]. In general, the factor N^{-s} in the functional equation is replaced by $\tilde{N}^{-s}$, where $\tilde{N}$ may differ from N at primes p such that $p^2 \mid N$.

The special value $L(\mathrm{Sym}^2(E), 2)$ may be evaluated using the Rankin-Selberg method, see (2.5) of [Sh2]. Flach [Fl1] was the first to compare this with the conjectural Bloch-Kato formula [BK] and to obtain some evidence for this special case of their conjecture [Fl2], which is closely related to a key result in the famous work of Taylor and Wiles [Wi],[TW]. Building on [Wi],[TW], Diamond, Flach and Guo [DFG1],[DFG2] have now proved a general result on the Bloch-Kato conjecture (at $s = 1$) for the adjoint L-function of a newform of weight $k \geq 2$. In the case that the newform has trivial character, this is equivalent to the symmetric square L-function (at $s = k$). Applying their result to $L(\mathrm{Sym}^2(E), 2)$ proves the l-part of the Bloch-Kato conjecture for primes $l \geq 5$ where E has *good* reduction and the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[l]$ is irreducible. (It also proves it for $l = 3$ if E has good reduction at 3 and the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))$ on $E[3]$ is absolutely irreducible.)

The purpose of this paper is to deduce a partial result (when $E[l]$ is irreducible, Proposition 8.2) and to obtain some numerical evidence (when $E[l]$ is reducible) concerning the l-part of the Bloch-Kato conjecture for $L(\mathrm{Sym}^2(E), 2)$, where $l \geq 5$ is a prime of *multiplicative* reduction. The key step is to determine the l-part of the Tamagawa factor c_l occurring in the conjectural formula for $L(\mathrm{Sym}^2(E), 2)$. Using the functional equation and results of Fontaine and Perrin-Riou [P1],[P2] we reduce the problem to that of determining the l-part of the Tamagawa factor $c_l(-1)$ occurring in the conjectural formula for $L(\mathrm{Sym}^2(E), 1)$. Our main result (Theorem 5.1) is that this is simply $|\mathrm{ord}_l(j(E))|_l^{-1}$. Thus in the case of split multiplicative reduction it is exactly the same as the l-part of the factor c_l' in the original Birch and Swinnerton-Dyer conjecture for E.

The proof relies on the theories of ordinary and semi-stable p-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and Fontaine's filtered (ϕ, N)-modules [Fo2],[P1], and especially on Breuil's integral refinements [Br1],[Br2]. I thank the referee for helpful comments concerning both the exposition and the substance of an earlier version of this paper, in particular for pointing out the necessity of Proposition 6.1 and giving hints towards the proof.

2. Some definitions

$E/\mathbb{Q}$ is an elliptic curve of conductor N. Let l be a prime number, let $T_l' = \varprojlim E[l^n]$ be the l-adic Tate module of E, and $V_l' = T_l' \otimes \mathbb{Q}_l$. Let $A_l' = V_l'/T_l' = \cup_{n=1}^{\infty} E[l^n]$. The absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts continuously on all of these modules, in a natural way. As Galois modules, $V_l' \simeq H^1_{et}(\overline{E}, \mathbb{Q}_l)(1)$ (a Tate twist).

Let $V_l = \mathrm{Sym}^2(V_l'), T_l = \mathrm{Sym}^2(T_l')$ and $A_l = V_l/T_l = \cup_{n=1}^{\infty} A[l^n]$, where $A[l^n] := \mathrm{Sym}^2(E[l^n])$. As Galois modules, $V_l \simeq \mathrm{Sym}^2(H^1_{et}(\overline{E}, \mathbb{Q}_l))(2)$. Let $A = \oplus_l A_l$.

Following [BK] (Section 3), for $p \neq l$ (including $p = \infty$) let

$$H^1_f(\mathbb{Q}_p, V_l) = \ker(H^1(D_p, V_l) \to H^1(I_p, V_l)).$$

D_p is a decomposition subgroup at a prime above p, I_p is the inertia subgroup, and the cohomology is for continuous cocycles and coboundaries. For $p = l$ let

$$H^1_f(\mathbb{Q}_l, V_l) = \ker(H^1(D_l, V_l) \to H^1(D_l, V_l \otimes B_{\mathrm{crys}}))$$

(see Section 1 of [BK] for a definition of Fontaine's ring B_{crys}). Let $H^1_f(\mathbb{Q}, V_l)$ be the subspace of elements of $H^1(\mathbb{Q}, V_l)$ whose local restrictions lie in $H^1_f(\mathbb{Q}_p, V_l)$ for all primes p. There is a natural exact sequence

$$0 \longrightarrow T_l \longrightarrow V_l \xrightarrow{\pi} A_l \longrightarrow 0.$$

Let $H^1_f(\mathbb{Q}_p, A_l) = \pi_* H^1_f(\mathbb{Q}_p, V_l)$. Define the l-Selmer group $H^1_f(\mathbb{Q}, A_l)$ to be the subgroup of elements of $H^1(\mathbb{Q}, A_l)$ whose local restrictions lie in $H^1_f(\mathbb{Q}_p, A_l)$ for all primes p. Note that the condition at $p = \infty$ is superfluous unless $l = 2$. Define the Shafarevich-Tate group

$$Ш = \bigoplus_l \frac{H^1_f(\mathbb{Q}, A_l)}{\pi_* H^1_f(\mathbb{Q}, V_l)}.$$

Note that, since $s = 2$ is a non-central critical point for $L(\mathrm{Sym}^2 E, s)$, it is conjectured that $H^1_f(\mathbb{Q}, V_l)$ is trivial, so the l-Selmer group should be identified with the l-part of the Shafarevich-Tate group. Likewise one can define a Shafarevich-Tate group $Ш(-1)$ corresponding to the point $s = 1$, using the $V_l(-1)$ and $T_l(-1)$.

3. The Bloch-Kato conjecture

Let ω be a Néron differential on E, coming from a global minimal Weierstrass model, and let

$$\Omega := \int_{E(\mathbb{C})} \omega \wedge \overline{\omega}.$$

The Bloch-Kato conjecture for $L(\mathrm{Sym}^2(E), s)$ at $s = 2$ amounts to the following (see (9) in [Fl1]):

$$\frac{L(\mathrm{Sym}^2(E), 2)}{\pi i \Omega} = \frac{\#Ш}{\#H^0(\mathbb{Q}, A)\#H^0(\mathbb{Q}, A(-1))} \prod_{p \leq \infty} c_p. \tag{2}$$

Here the c_p are certain rational "Tamagawa factors", almost all of which are equal to 1. If p is a finite prime and $l \neq p$ then the l-part of c_p is by definition $\#H^1_f(\mathbb{Q}_p, T_l)|P_p(p^{-2})|_l = \#H^0(\mathbb{Q}_p, A_l)|P_p(p^{-2})|_l$. The p-part of c_p depends on the choice of a $\mathbb{Z}_p$-lattice in $\mathrm{Sym}^2 H^1_{\mathrm{dR}}(E/\mathbb{Q}_p)$. (Strictly speaking, it only depends on the choice of a basis for the top exterior power of $\mathrm{Sym}^2 H^1_{\mathrm{dR}}(E/\mathbb{Q}_p)/F^2$.) To get the c_p appearing in (2), with Ω as described above, we follow Flach. Let ω be a Néron differential, as above. Let η be an element of $H^1_{\mathrm{dR}}(E/\mathbb{Q})$ whose image in $H^1_{\mathrm{dR}}(E/\mathbb{Q})/F^1 \simeq H^1(E, O_E)$ is Serre dual to ω. There are various choices for η, but together with ω they all span the same $\mathbb{Z}$-lattice L'. Let $L = \mathrm{Sym}^2 L'$. Given the choice of L, the exact definition of the p-parts of the c_p will be described in the next section.

Lemma 3.1.

1. *c_∞ is at worst a power of 2.*
2. *For any prime p of good reduction, c_p is at worst a power of p, and if $p \geq 5$ it is trivial.*
3. *If p is a prime of multiplicative reduction and $d_p := -\mathrm{ord}_p(j(E))$ then, up to a power of p,*
$$c_p = \#E(\mathbb{Q}_p)[d_p].$$

This is due to Flach, and follows from a corrected version of Lemma 1 in [Fl1]. The main goal of this paper is to determine the p-part of c_p when p is a prime of multiplicative reduction.

4. The Bloch-Kato exponential map

For the definitions of Fontaine's rings B_{dR} and B_{crys} one may consult Chapter 1 of [BK], for example. Alternatively see [Fo1], where there is also the definition of B_{st}. All these rings come equipped with actions of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, and B_{st} has operators ϕ (Frobenius) and N (monodromy) satisfying $N\phi = p\phi N$, such that $B_{\mathrm{crys}} = B_{\mathrm{st}}^{N=0}$. Let V be a finite-dimensional $\mathbb{Q}_p$-vector space with a continuous action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Let $H^1(\mathbb{Q}_p, V)$ be defined with respect to continuous cocycles and coboundaries. Bloch and Kato (Chapter 3 of [BK]) define subspaces

$$H^1_e(\mathbb{Q}_p, V) \subset H^1_f(\mathbb{Q}_p, V) \subset H^1_g(\mathbb{Q}_p, V) \subset H^1(\mathbb{Q}_p, V),$$

as follows (we already defined $H^1_f(\mathbb{Q}_p, V)$ in the previous section):

$$H^1_e(\mathbb{Q}_p, V) = \mathrm{Ker}(H^1(\mathbb{Q}_p, V) \to H^1(\mathbb{Q}_p, B_{\mathrm{crys}}^{\phi=1} \otimes V));$$
$$H^1_f(\mathbb{Q}_p, V) = \mathrm{Ker}(H^1(\mathbb{Q}_p, V) \to H^1(\mathbb{Q}_p, B_{\mathrm{crys}} \otimes V));$$
$$H^1_g(\mathbb{Q}_p, V) = \mathrm{Ker}(H^1(\mathbb{Q}_p, V) \to H^1(\mathbb{Q}_p, B_{\mathrm{dR}} \otimes V)).$$

Let $D_{\mathrm{dR}}(V) = (B_{\mathrm{dR}} \otimes V)^{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$. It has a natural filtration $D_{\mathrm{dR}}(V) \supset D_{\mathrm{dR}}(V)^0 \supset D_{\mathrm{dR}}(V)^1 \supset \ldots$ arising from the filtration of B_{dR} by powers of its maximal ideal B_{dR}^+. V is said to be a deRham representation of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q})$ if the $\mathbb{Q}_p$-vector spaces V and $D_{\mathrm{dR}}(V)$ have the same dimension. Similarly one may define crystalline and semi-stable representations using B_{crys} and B_{st} respectively. By Proposition 1.17 of [BK] there is an exact sequence

$$0 \longrightarrow \mathbb{Q}_p \xrightarrow{\alpha} B_{\mathrm{crys}} \oplus B_{\mathrm{dR}}^+ \xrightarrow{\beta} B_{\mathrm{crys}} \oplus B_{\mathrm{dR}} \longrightarrow 0, \tag{3}$$

where $\alpha(x) = (x, x)$ and $\beta(x, y) = (x - \phi(x), x - y)$. Tensoring with V and taking $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-invariants leads to a map

$$\exp : D_{\mathrm{dR}}(V)/D_{\mathrm{dR}}(V)^0 \to H_e^1(\mathbb{Q}_p, V).$$

Now for V we substitute V_p from §2, with p a prime of multiplicative reduction. It follows from Proposition 6.5 below that $\det(1 - \phi u : D_{\mathrm{crys}}(V_p)) = 1 - p^{-2}u$ $(= P_p(p^{-2}u))$, which does not vanish at $u = 1$. Further, V_p, being 'ordinary' (see the end of §5 below) is semi-stable (by the proposition in 3.1 of [P1]) hence deRham. It then follows from Theorem 4.1(ii) of [BK] that in this case exp is an isomorphism, and that $H_e^1(\mathbb{Q}_p, V_p) = H_f^1(\mathbb{Q}_p, V_p)$.

Define D to be the 3-dimensional $\mathbb{Q}_p$-vector space $\mathrm{Sym}^2 H_{\mathrm{dR}}^1(E/\mathbb{Q}_p)$ with its Hodge filtration

$$D = D^0 \supset D^1 \supset D^2 \supset D^3 = \{0\}.$$

A comparison theorem naturally identifies $D_{\mathrm{dR}}(V_p)$ with D, with the filtration shifted by 2 (see the comment following Corollary 6.4 below), so that we get an isomorphism of 2-dimensional $\mathbb{Q}_p$-vector spaces

$$\exp : D/D^2 \to H_f^1(\mathbb{Q}_p, V_p). \tag{4}$$

On the left hand side we have an integral structure M/M^2, where $M := L \otimes \mathbb{Z}_p$ (L as in the previous section) and $M^i = M \cap D^i$. We may assign measure 1 to its image in $H_f^1(\mathbb{Q}_p, V_p)$. Thus we obtain a measure μ of $H_f^1(\mathbb{Q}_p, T_p)$. (Multiply the size of its torsion subgroup by the measure of its image in $H_f^1(\mathbb{Q}_p, V_p)$.) The p-part of c_p is defined to be $\mu(H_f^1(\mathbb{Q}_p, T_p))|P_p(p^{-2})|_p$.

Using instead $V_p(-1)$, $P_p(p^{-1}u)$ and the isomorphism

$$\exp : D/D^1 \to H_f^1(\mathbb{Q}_p, V_p(-1)), \tag{5}$$

of 1-dimensional $\mathbb{Q}_p$-vector spaces, we may likewise define the p-part of $c_p(-1)$, a Tamagawa factor appearing in the Bloch-Kato conjecture at $s = 1$. Even though $s = 1$ is left of the central point of the functional equation, the conjecture makes sense in this instance. Apart from [FP], see [Fo3] for the Fontaine-Perrin-Riou generalisation of the conjecture to arbitrary integer points, especially §11 for the relation with the original conjecture of [BK].

5. An isomorphism of finite parts

Define D' to be the 2-dimensional $\mathbb{Q}_p$-vector space $H^1_{\mathrm{dR}}(E/\mathbb{Q}_p)$ with its Hodge filtration

$$D' = D'^0 \supset D'^1 \supset D'^2 = \{0\}.$$

Let $M' := L' \otimes \mathbb{Z}_p$, with L' as in §3, and $M'^i = M' \cap D'^i$. $D_{\mathrm{dR}}(V'_p)$ is naturally identified with D', with the filtration shifted by 1 (see the comment following Corollary 6.4 below), so that we get an isomorphism of 1-dimensional $\mathbb{Q}_p$-vector spaces

$$\exp : D'/D'^1 \to H^1_f(\mathbb{Q}_p, V'_p). \tag{6}$$

(Note that V'_p is ordinary and $\det(1-\phi u : D_{\mathrm{crys}}(V'_p)) = 1 - p^{-1}u$.) This is used, as above, to define the p-part of a Tamagawa factor c'_p.

Theorem 5.1. *Assume that $p \geq 5$ and that E has split multiplicative reduction at p. There is an injection $T'_p \to T_p(-1)$ of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules which induces a commutative diagram*

$$\begin{array}{ccc}
H^1_f(\mathbb{Q}_p, T'_p) & \longrightarrow & H^1_f(\mathbb{Q}_p, T_p(-1)) \\
\downarrow & & \downarrow \\
H^1_f(\mathbb{Q}_p, V'_p) & \longrightarrow & H^1_f(\mathbb{Q}_p, V_p(-1)) \\
{\scriptstyle \exp}\uparrow & & {\scriptstyle \exp}\uparrow \\
D'/D'^1 & \xrightarrow{f} & D/D^1
\end{array}$$

All the horizontal maps are isomorphisms, and f identifies M'/M'^1 with M/M^1. Hence the p-part of $c_p(-1)$ is equal to the p-part of c'_p, namely $|\mathrm{ord}_p(j(E))|_p^{-1}$. Even when the multiplicative reduction at p is non-split, the p-part of $c_p(-1)$ is equal to $|\mathrm{ord}_p(j(E))|_p^{-1}$.

The proof of this theorem will occupy this section and the next.

For the proof of the following proposition, due to Tate, see [Si] (Chapter V, Lemma 5.1, Lemma 5.2 and Theorem 5.3).

Proposition 5.2. *Let E be an elliptic curve defined over $\mathbb{Q}_p$, with $\mathrm{ord}_p(j) =: -d_p < 0$. There is a unique $q \in \mathbb{Q}_p$ such that $j(E) = \frac{1}{q} + 744 + 196884q + \ldots$.*

There is an isomorphism of groups:

$$E(\overline{\mathbb{Q}}_p) \simeq \overline{\mathbb{Q}}_p^*/q^{\mathbb{Z}}.$$

The actions of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ are the same in the case of split multiplicative reduction and differ only by an unramified quadratic character in the case of non-split multiplicative reduction.

It suffices to prove the above theorem in the case of split multiplicative reduction. In the non-split case, we may replace $E/\mathbb{Q}_p$ by an unramified quadratic twist with (the same j-invariant and) split multiplicative reduction. Twisting E

by this quadratic character leaves invariant the symmetric squares V_p and T_p, and changes M by at worst a p-unit.

Proposition 5.3. *Assume that $p \geq 3$ and that E has split multiplicative reduction at p. The Tate parametrisation provides a natural injection $T_p' \to T_p(-1)$ of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules. The top two horizontal arrows of the diagram in Theorem 5.1 are isomorphisms.*

Proof. The above proposition gives us an exact sequence of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules:

$$0 \longrightarrow \mathbb{Q}_p(1) \longrightarrow V_p' \longrightarrow \mathbb{Q}_p \longrightarrow 0, \tag{7}$$

We get an exact sequence

$$0 \longrightarrow V_p' \longrightarrow V_p(-1) \longrightarrow \mathbb{Q}_p(-1) \longrightarrow 0. \tag{8}$$

Since $H^0(\mathbb{Q}_p, \mathbb{Q}_p(-1))$ is trivial we then get an injective map from $H^1(\mathbb{Q}_p, V_p')$ to $H^1(\mathbb{Q}_p, V_p(-1))$ which, as is clear from the definition, maps $H^1_f(\mathbb{Q}_p, V_p')$ to $H^1_f(\mathbb{Q}_p, V_p(-1))$. Since these are both 1-dimensional $\mathbb{Q}_p$-vector spaces, we have an isomorphism from $H^1_f(\mathbb{Q}_p, V_p')$ to $H^1_f(\mathbb{Q}_p, V_p(-1))$. Likewise using the exact sequence

$$0 \longrightarrow T_p' \longrightarrow T_p(-1) \longrightarrow \mathbb{Z}_p(-1) \longrightarrow 0,$$

(which includes the injection of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules referred to in Theorem 5.1) we obtain an injection from $H^1_f(\mathbb{Q}_p, T_p')$ to $H^1_f(\mathbb{Q}_p, T_p(-1))$, which I claim is an isomorphism. It is easy to see (bearing in mind that $H^1_f(\mathbb{Q}_p, V_p') \simeq H^1_f(\mathbb{Q}_p, V_p(-1))$) that the inverse image of $H^1_f(\mathbb{Q}_p, T_p(-1))$ in $H^1(\mathbb{Q}_p, T_p')$ is $H^1_f(\mathbb{Q}_p, T_p')$. Hence if our claim were false there would exist a non-zero element of $H^1_f(\mathbb{Q}_p, \mathbb{Z}_p(-1))$ (coming from something in $H^1_f(\mathbb{Q}_p, T_p(-1))$ which is not in the image of $H^1(\mathbb{Q}_p, T_p')$). But by the table in Example 3.9 of [BK], $H^1_f(\mathbb{Q}_p, \mathbb{Q}_p(-1))$ is trivial, therefore $H^1_f(\mathbb{Q}_p, \mathbb{Z}_p(-1))$ is in the image of $H^0(\mathbb{Q}_p, (\mathbb{Q}_p/\mathbb{Z}_p)(-1))$, which is trivial since $p \geq 3$. □

A p-adic representation V of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is said to be *ordinary* if there is a decreasing, exhaustive and separated filtration $(\mathrm{Fil}^i V)_{i\in\mathbb{Z}}$ by subspaces of V, stable under $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, such that on the quotient $\mathrm{Fil}^i V/\mathrm{Fil}^{i+1}V$ the inertia subgroup I_p acts by χ^i, where χ is the cyclotomic character. The exact sequences (7) and (8) arising from the Tate parametrisation show that V_p' and V_p are ordinary.

6. A strongly divisible (ϕ, N)-filtered module

A (ϕ, N)-filtered module (over $\mathbb{Q}_p$) is a $\mathbb{Q}_p$-vector space D (temporarily suspend the notation of §4) with a decreasing, exhaustive, separated filtration by subspaces D^i ($i \in \mathbb{Z}$), a linear isomorphism ϕ and an endomorphism N satisfying $N\phi = p\phi N$. Among all (ϕ, N)-filtered modules, some are said to be *weakly admissible,* and among these, some are said to be *ordinary.* For definitions see (for

example) 1.2 of [P1]. Our restriction to modules over $\mathbb{Q}_p$ is not really necessary, but they are all we need.

From a p-adic representation V of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ one obtains a (ϕ, N)-filtered module

$$D^*_{\mathrm{st}}(V) := \mathrm{Hom}_{\mathbb{Q}_p}(V, B_{\mathrm{st}})^{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}.$$

Conversely, from a (ϕ, N)-filtered module D one obtains a p-adic representation

$$V^*_{\mathrm{st}}(D) = \mathrm{Hom}_{\mathbb{Q}_p,\phi,N,\mathrm{Fil}^\cdot}(D, B_{\mathrm{st}}),$$

i.e. the set of morphisms from D to B_{st} in the category of (ϕ, N)-filtered modules.

It has been proved by Colmez and Fontaine [CF] that these functors set up an anti-equivalence between the category of semi-stable p-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and the category of finite-dimensional, weakly admissible (ϕ, N)-filtered modules over $\mathbb{Q}_p$. It had earlier been proved by Perrin-Riou (the theorem in 1.5 of [P1]) that they set up an anti-equivalence between the category of finite-dimensional, ordinary p-adic representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and the category of finite-dimensional, ordinary (ϕ, N)-filtered modules over $\mathbb{Q}_p$.

Let S be the p-adic completion of the divided-power algebra $\mathbb{Z}_p\langle u\rangle$, as in 2.1.1 of [Br1]. Breuil (see 4.2 of [Br3]) associates to any "strongly divisible" module $\mathcal{M}$ in $S \otimes_{\mathbb{Z}_p} D$ (where D is a (ϕ, N)-filtered module) a $\mathbb{Z}_p[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$-module $T^*_{\mathrm{st}}(\mathcal{M}) := \mathrm{Hom}_{S,\phi,N,\mathrm{Fil}^{p-1}}(\mathcal{M}, \widehat{A_{\mathrm{st}}})$. The ring $\widehat{A_{\mathrm{st}}}$ is defined in 3.1.1 of [Br1] (or 2.4 of [Br3]).

Let $\mathcal{E}/\mathbb{Z}_p$ be a minimal proper, regular model for E and let $\mathcal{E}_n/(\mathbb{Z}/p^n\mathbb{Z})$ be its reduction modulo p^n. For each $n \geq 1$ we may use the homomorphism of S/p^nS to $\mathbb{Z}/p^n\mathbb{Z}$ which sends u to p, to consider $\mathcal{E}_n$ as a log-scheme over S/p^nS, where $\mathcal{E}_n$ has the canonical log-structure associated to the special fibre and S/p^nS is endowed with the log-structure $(1 \mapsto u)$. (See [K2] or Section 2 of [HK] for more on log-structures.) Then, following Breuil, we may consider the S-module

$$H^1_{\mathrm{st}}(\mathcal{E}/\mathbb{Z}_p) := \varprojlim H^1_{\mathrm{crys}}(\mathcal{E}_n/(S/p^nS)).$$

Here we are using log-crystalline cohomology for the structure sheaf. Let $f_p : S \to \mathbb{Z}_p$ be the homomorphism which maps u to p.

Proposition 6.1. *There is a natural isomorphism between $H^1_{st}(\mathcal{E}/\mathbb{Z}_p) \otimes_{S,f_p} \mathbb{Z}_p$ and M', with M' as defined at the beginning of §5.*

Proof. Firstly, in the definition of $H^1_{\mathrm{st}}(\mathcal{E}/\mathbb{Z}_p)$, we may replace each $\mathcal{E}_n$ by $\mathcal{E}_1$. (See the paragraph preceding Definition 2.1.1.1 in [Br2].) As explained in 2.1.1 of [Br2], $H^1_{\mathrm{crys}}(\mathcal{E}_1/(S/p^nS))$ may be identified with the cohomology of a certain sheaf O^{st}_n on the small syntomic site of $\mathcal{E}_1$, so

$$H^1_{\mathrm{st}}(\mathcal{E}/\mathbb{Z}_p) \simeq \varprojlim H^1((\mathcal{E}_1)_{\mathrm{syn}}, O^{\mathrm{st}}_n).$$

This allows one to define ϕ and N acting on $H^1_{\mathrm{st}}(\mathcal{E}/\mathbb{Z}_p)$, and also a filtration, in fact $H^1_{\mathrm{st}}(\mathcal{E}/\mathbb{Z}_p)$ becomes a strongly divisible S-module (Proposition 4.1.5 of [Br2]).

Now the second isomorphism in Corollaire 4.3.1.4 of [Br2] shows that the $\mathbb{Z}_p$-modules $H^1_{\mathrm{st}}(\mathcal{E}/\mathbb{Z}_p)\otimes_{S,f_p}\mathbb{Z}_p$ and $M^{HK}:=\varprojlim H^1_{\mathrm{crys}}(\mathcal{E}_1/(\mathbb{Z}/p^n\mathbb{Z}))$ are canonically isomorphic. This $H^1_{\mathrm{crys}}(\mathcal{E}_1/(\mathbb{Z}/p^n\mathbb{Z}))$ is log-crystalline cohomology for the structure sheaf, where the base has log-structure $(1\mapsto p)$.

M^{HK} is in turn equated with the modified deRham cohomology $H^1(\mathcal{E},\omega^{\cdot}_{\mathcal{E}/\mathbb{Z}_p})$ of Hyodo, which comes from a complex (of étale sheaves) involving differentials with log poles. This follows from Theorem 6.4 of [K2], with $X=Y=\mathcal{E}_1$ and $\mathcal{F}$ the structure sheaf. Note that the log-structures involved are fine, by (2.5)(1) of [K2]. See also (3.7)(2) of [K2] for the required log-smoothness.

It is an important fact, proved in Proposition 4.3.2.3 of [Br2], that the filtration on M^{HK} which is the image under f_p of the filtration on $H^1_{\mathrm{st}}(\mathcal{E}/\mathbb{Z}_p)$, is the Hodge filtration.

It remains to identify $H^1(\mathcal{E},\omega^{\cdot}_{\mathcal{E}/\mathbb{Z}_p})$ with M'. But Corollaire 2.6 (a) of [I] shows that $H^1(\mathcal{E},\omega^{\cdot}_{\mathcal{E}/\mathbb{Z}_p})$ has filtration with submodule $H^0(\mathcal{E},\omega^1_{\mathcal{E}/\mathbb{Z}_p})$ and quotient $H^1(\mathcal{E},O_{\mathcal{E}/\mathbb{Z}_p})$. Note that $\mathcal{E}/\mathbb{Z}_p$ is ordinary in the sense required by Corollaire 2.6 of [I]. Also note that it is alright to use the Zariski topology for these subfactors. Here, $\omega^1_{\mathcal{E}/\mathbb{Z}_p}$ is a sheaf of differentials with log poles, which, by p. 95 (and (Du1) on p. 93) of [Hi] is a dualizing sheaf. These subfactors of $H^1(\mathcal{E},\omega^{\cdot}_{\mathcal{E}/\mathbb{Z}_p})$ are then in Grothendieck-Serre duality to each other (see Theorem 2.1.1 of [Hi]). To complete the identification of $H^1(\mathcal{E},\omega^{\cdot}_{\mathcal{E}/\mathbb{Z}_p})$ with M' it suffices to observe that $H^0(\mathcal{E},\omega^1_{\mathcal{E}/\mathbb{Z}_p})$ is generated by a Néron differential (see III.10 of [N]). □

Corollary 6.2. *Under the equivalence of categories in §6 of* [Br4]*, the $S\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$-module (with filtration and actions of ϕ and N) $H^1_{\mathrm{st}}(\mathcal{E}/\mathbb{Z}_p)\otimes_{\mathbb{Z}_p}\mathbb{Q}_p$ corresponds to D', in particular D' is naturally a filtered (ϕ,N)-module. $H^1_{\mathrm{st}}(\mathcal{E}/\mathbb{Z}_p)$ may be viewed as lying inside $S\otimes_{\mathbb{Z}_p}D'$.*

For the rest of this section assume that $p\geq 3$.

Proposition 6.3. *$T^*_{\mathrm{st}}(H^1_{\mathrm{st}}(\mathcal{E}/\mathbb{Z}_p))$ is isomorphic to T'_p.*

This follows from Théorème 1.4 of [Br2] ($p\geq 3$ ensures that $\mathrm{Fil}^{p-1}=0$).

Corollary 6.4. *$V^*_{\mathrm{st}}(D')$ is isomorphic to V'_p and $D^*_{\mathrm{st}}(V'_p)$ is isomorphic to D'*

$D'\simeq D^*_{\mathrm{st}}(V'_p)\simeq D_{st}(V'^*_p)\simeq D_{\mathrm{st}}(V'_p(-1))\simeq D_{\mathrm{dR}}(V'_p(-1))$. We could also have got this from the comparison theorem of Kato and Tsuji [K1], [Ts], or even from the special case of abelian varieties proved earlier by Fontaine [Fo4]. An isomorphism between D' and $D_{\mathrm{dR}}(V'_p(-1))$ is used in §4 above, in connection with the exponential map. This isomorphism should be taken to be the one constructed above.

Our aim now is to obtain explicit descriptions of D' and M', which we shall then use to finish off the proof of Theorem 5.1.

Proposition 6.5. *Let $E/\mathbb{Q}$ be an elliptic curve with split multiplicative reduction at p, and Tate parameter q. Let $\alpha := \mathrm{ord}_p(q)$ and $\lambda := \log_p(q)$. Then the 2-dimensional p-adic representation V_p' corresponds (via D^*_{st}) to a (ϕ, N)-filtered module D'' with $\mathbb{Q}_p$-basis $\{e_0, e_1\}$, defined by*

$$\phi e_1 = pe_1,\ \phi e_0 = e_0,$$
$$Ne_1 = \alpha e_0\ ,\ Ne_0 = 0,$$
$$D''^0 = D'',\ D''^1 = \langle e_1 - \lambda e_0\rangle\ ,\ D''^2 = \{0\}.$$

This follows from the proposition in 3.5 of [P1].

Remark 6.6. *The quantity λ/α is nothing other than the "$\mathcal{L}$-invariant" appearing in the conjecture of Mazur, Tate and Teitelbaum (theorem of Greenberg and Stevens)* [MTT], [GS]. *The connection with (ϕ, N)-modules was used by Fontaine and Mazur* [M] *to generalise the $\mathcal{L}$-invariant, for example to modular forms of higher weight.*

For the rest of this section assume that $p \geq 5$.

Proposition 6.7. *Let M'' be the $\mathbb{Z}_p$-span of e_0 and e_1 and let $\mathcal{M}'' = S \otimes_{\mathbb{Z}_p} M''$. Then $\mathcal{M}''$, with a natural filtration and operators ϕ and N, is a strongly divisible S-module, in the sense of* [Br1].

To prove this, one notes that we are in "le cas naif" of §5 of [Br1], and follows the recipe there for construction of a strongly divisible module. In his notation, $\hat{e}_1 = e_1 - \lambda e_0$, and $\frac{\phi}{p}(e_1 - \lambda e_0) = (e_1 - \lambda e_0) + \lambda\left(1 - \frac{1}{p}\right)e_0$. The coefficient $\lambda\left(1 - \frac{1}{p}\right)$ does belong to $\mathbb{Z}_p$, since the series for $\log_p(x)$ shows that p divides λ. The condition about the length of the filtration not exceeding $p-2$ (just before Proposition 5.3 in [Br1]) is satisfied since $p \geq 5$.

It is worth remarking that, since we are in "le cas naif" ($N(\mathrm{Fil}^i) \subset \mathrm{Fil}^{i-1}$), the canonical filtration on $\mathcal{M}'' = S \otimes_{\mathbb{Z}_p} M''$ (in the sense of §6 of [Br4]) is simply the tensor product of the filtration on M'' and the filtration $\{(u-p)^i S\}$ on S. Under the equivalence of categories in §6 of [Br4], $\mathcal{M}'' \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ corresponds to D''.

Proposition 6.8. *$T^*_{\mathrm{st}}(\mathcal{M}'')$ is isomorphic to T_p'.*

Proof. In the proof of the proposition in 3.5 of [P1], Perrin-Riou constructs a $\mathbb{Q}_p$-basis $\{f_1, f_2\}$ for $V^*_{\mathrm{st}}(D'')$ (or rather for something which includes $V^*_{\mathrm{st}}(D'')$ as a special case). As elements of $V^*_{\mathrm{st}}(D'') = \mathrm{Hom}_{\mathbb{Q}_p,\phi,N,\mathrm{Fil}\cdot}(D'', B_{\mathrm{st}})$ they are

$$f_1(e_0) = 0,\ f_1(e_1) = t;$$
$$f_2(e_0) = 1,\ f_2(e_1) = \mathrm{LOG}(q),$$

where t and $\mathrm{LOG}(q)$ are defined on p.202 in [P1]. We have used for Proposition 6.5 the fact that the $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-action on $V^*_{\mathrm{st}}(D'')$ (described explicitly in [P1]) is visibly the same as that on V_p'. But it is just as easy to see that the $\mathbb{Z}_p$-lattice spanned by f_1 and f_2 is isomorphic (with $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-action) to T_p'. Moreover,

$f_1, f_2 : D'' \to B_{\mathrm{st}}$ map e_0 and e_1 to $\widehat{A_{\mathrm{st}}}$, in fact, f_1 and f_2 span $T^*_{\mathrm{st}}(\mathcal{M}'')$ (over $\mathbb{Z}_p$). So $\mathcal{M}'' = S \otimes_{\mathbb{Z}_p} M''$ corresponds (via T^*_{st}) to T'_p. □

Lemma 6.9. *There is an isomorphism between the filtered (ϕ, N)-modules D' and D'' which identifies M' with M''.*

Proof. By Corollary 6.4 we have $V^*_{\mathrm{st}}(D') \simeq V'_p$. But Proposition 6.5 gave us also $V^*_{\mathrm{st}}(D'') \simeq V'_p$, hence the isomorphism between D' and D''. According to Theorem 4.2.7 of [Br3], T^*_{st} gives an anti-equivalence of categories between strongly divisible lattices in $S \otimes_{\mathbb{Z}_p} D'$ and $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-stable lattices in V'_p. Hence, by Propositions 6.8 and 6.3, $S \otimes_{\mathbb{Z}_p} M''$ and $H^1_{\mathrm{st}}(\mathcal{E}/\mathbb{Z}_p)$ are the same. Applying $\otimes_{S,f_p}\mathbb{Z}_p$ and Proposition 6.1, we see that M'' and M' are the same, inside D'. □

Proposition 6.10. *The injection $V'_p \to V_p(-1)$ induces a map $f : D' \to D$ which fits into the commutative diagram of Theorem 5.1 and identifies $M'/{M'}^1$ with M/M^1.*

Proof. Above we mentioned the $\mathbb{Z}_p$-basis $\{f_1, f_2\}$ for T'_p. Recall that as elements of $V^*_{\mathrm{st}}(D')$ they are

$$f_1(e_0) = 0,\ f_1(e_1) = t;$$

$$f_2(e_0) = 1,\ f_2(e_1) = \mathrm{LOG}(q),$$

where t and $\mathrm{LOG}(q)$ are defined on p.202 in [P1]. Note that $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts on $\mathbb{Z}_p t$ by the cyclotomic character. In fact, considering the exact sequence

$$0 \longrightarrow \mathbb{Q}_p(1) \longrightarrow V'_p \longrightarrow \mathbb{Q}_p \longrightarrow 0,$$

f_1 generates the submodule $\mathbb{Q}_p(1)$ and the image of f_2 generates the quotient.

The embedding of V'_p into $V_p(-1)$ which appears in the exact sequence

$$0 \longrightarrow V'_p \longrightarrow V_p(-1) \longrightarrow \mathbb{Q}_p(-1) \longrightarrow 0,$$

is just multiplication by $f_1(-1)$, where we consider a basis $\{f_1(-1), f_2(-1)\}$ for $T'_p(-1) \simeq H^1_{et}(\overline{E}, \mathbb{Q}_p)$ in the obvious way. Now $f_1(-1)$ is fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ so $1 \otimes f_1(-1) \in B_{\mathrm{dR}} \otimes V'_p(-1)$ is an element of $D_{\mathrm{dR}}(V'_p(-1)) \simeq D'$. I claim that the element of D' to which it corresponds is e_0. To see this, note that under the duality between V'_p and $V'_p(-1)$ (coming from the Weil pairing), $f_1(f_1(-1)) = 0$ and $f_2(f_1(-1)) = 1$, which is exactly what f_1 and f_2 do to e_0. Hence $e_0 \in D' = D^*_{\mathrm{st}}(V'_p) \subset \mathrm{Hom}_{\mathbb{Q}_p}(V'_p, B_{\mathrm{dR}}) = V'_p(-1) \otimes B_{\mathrm{dR}}$ is the same as $f_1(-1)$.

Hence the associated map (f) from D' to D (in fact from M' to M) which identifies $D'/{D'}^1$ with D/D^1 is just multiplication by e_0. Recall now that ${D'}^1$ is generated by the element $e_1 - \lambda e_0$, with λ integral at p. Hence $M'/{M'}^1$ is generated (over $\mathbb{Z}_p$) by the image of e_0. Similarly M/M^1 is generated by the image of e_0^2. But multiplication by e_0 maps our generator for $M'/{M'}^1$ to our generator for M/M^1, which is what we need. □

7. The p-part of c_p

We have now completed the proof of Theorem 5.1, which tells us (for $p \geq 5$ a prime of multiplicative reduction) that the p-part of $c_p(-1)$ is equal to $|\mathrm{ord}_p(j(E))|_p^{-1}$. Recall that $c_p(-1)$ is a Tamagawa factor in the Bloch-Kato formula for $L(\mathrm{Sym}^2(E), 1)$. It is somewhat more convenient to test the Bloch-Kato conjecture for $L(\mathrm{Sym}^2(E), 2)$.

Proposition 7.1. *Suppose that p is a prime of multiplicative reduction. Then* $\mathrm{ord}_p(c_p) = \mathrm{ord}_p(c_p(-1)) - 1$.

Proof. (Sketch.) We refer heavily to Appendix C of [P2], which concerns the compatibility of the Bloch-Kato conjecture with the functional equation. By C.2.10, Perrin-Riou's conjecture $C_{EP,\mathbb{Q}_p}(V_p)$ holds, because V_p is ordinary. Then, by C.3.8, the equation (C.2) after Lemma C.3.6 holds locally at p, where the "M" in that equation is the motive associated with $L(\mathrm{Sym}^2(E), 2)$ and its dual $M^*(1)$ is associated with $L(\mathrm{Sym}^2(E), 1)$. It follows from the proof of Proposition 5.1 in [De] that (with the natural choices of lattices used throughout this paper) the factor "$\tilde{\zeta}_{M(\infty)}$" in the equation (C.2) is trivial. The term $\pm\epsilon(M)$ on the right of (C.2) comes from the exponential factor in the functional equation, and in our case is $\tilde{N}/\tilde{N}^2 = 1/\tilde{N}$. The p-part of the ratio $c_p/c_p(-1)$ appears on the left of (C.2), and all the other factors contribute nothing locally at p. Since $p \,||\, \tilde{N}$, the result follows. □

Remark 7.2. *It was already observed by Flach (see the example after Theorem 1 in* [Fl1]*) that if the Bloch-Kato conjecture is true then sometimes the p-part of c_p has to be non-integral.*

8. The irreducible case

The following is Theorem 3.53 of [DDT].

Theorem 8.1. *Suppose that $E/\mathbb{Q}$ is an elliptic curve of square-free conductor N. Let l be a prime number. Recall that $d_p := -\mathrm{ord}_p(j(E))$. Suppose that*

1. *$A'[l]$ is an irreducible representation of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*;*
2. *l does not divide $2\prod_{p|N} d_p$.*

Then the l-part of

$$N\frac{L(\mathrm{Sym}^2(E), 2)}{\pi i \Omega},$$

is equal to the order of

$$H^1_\phi(\mathbb{Q}, A_l(-1)).$$

Note that in [DDT] (just before Theorem 2.41), $H^1_\phi(\mathbb{Q}, A_l(-1))$ is defined as a direct limit of $H^1_\phi(\mathbb{Q}, A[l^n](-1))$, where for each n the latter is defined by certain local conditions. However, it follows from (1.7) of [Wi] and from the last line of p.56 of [DDT] that the Selmer group $H^1_\phi(\mathbb{Q}, A_l(-1))$ is defined by the usual

Bloch-Kato local conditions $\mathrm{res}_p(x) \in H^1_f(\mathbb{Q}_p, A_l(-1))$ (as in §2) for $p \neq l$, and by $\mathrm{res}_l(x) \in H^1_{\mathrm{Se}}(\mathbb{Q}_l, A_l(-1))$, where $H^1_{\mathrm{Se}}(\mathbb{Q}_l, A_l(-1))$ is as in [Wi].

Proposition 8.2. *If $l \geq 5$ is a prime of multiplicative reduction and the hypotheses of Theorem 8.1 are satisfied, then that theorem confirms the l-part of the Bloch-Kato conjecture for $L(\mathrm{Sym}^2(E), 2)$.*

Proof. Recall that the Bloch-Kato conjecture predicts that

$$\frac{L(\mathrm{Sym}^2(E), 2)}{\pi i \Omega} = \frac{\#Ш}{\#H^0(\mathbb{Q}, A)\#H^0(\mathbb{Q}, A(-1))} \prod_{p \leq \infty} c_p.$$

It is easy to show (as in Lemma 4.1 of [Du]) that, due to the irreducibility of $A'[l]$,$\#H^0(\mathbb{Q}, A_l)\#H^0(\mathbb{Q}, A_l(-1)) = 1$. Since $l \geq 5$ and does not divide $\prod_{p|N} d_p$, it follows from Lemma 3.1 that the l-part of $\prod_{p \neq l} c_p$ is trivial, and, from Theorem 5.1 and Proposition 7.1, that the l-part of c_l is $1/l$. This matches the power of l in the $1/N$ which comes from rearranging the equality in Theorem 8.1, so we just need to show that $H^1_\phi(\mathbb{Q}, A_l(-1))$ and the l-part of Ш have the same order.

By (the proof of) Proposition 1.3 (ii) of [Wi], $H^1_f(\mathbb{Q}_l, V_l(-1)) \subset H^1_{\mathrm{Se}}(\mathbb{Q}_l, V_l(-1))$ (which projects onto $H^1_{\mathrm{Se}}(\mathbb{Q}_l, A_l(-1))$). Clearly then

$$\#H^1_f(\mathbb{Q}, A_l(-1)) \leq \#H^1_\phi(\mathbb{Q}, A_l(-1)),$$

and since $H^1_f(\mathbb{Q}, A_l(-1))$ is finite, it is equal to the l-part of Ш(-1). Similarly $H^1_\phi(\mathbb{Q}, A_l(-1))$ is equal to the l-part of a modified Shafarevich-Tate group $\widetilde{Ш}(-1)$ defined using the weaker local condition at l. See [Fl3], where it is shown that the order of a general Shafarevich-Tate group is equal to the order of another defined using "dual" local conditions. Now $H^1_f(\mathbb{Q}_p, V_l(-1))$ is dual to $H^1_f(\mathbb{Q}_p, V_l)$ for all p, so the l-parts of the orders of Ш(-1) and Ш are the same. Let $\widetilde{Ш}$ be defined using local conditions dual to those which define $\widetilde{Ш}(-1)$ and let $H^1_{\phi^*}(\mathbb{Q}, A_l)$ be the associated Selmer group. $H^1_{\mathrm{Se}}(\mathbb{Q}_l, V_l(-1))$ is dual to something *contained in* $H^1_f(\mathbb{Q}_l, V_l)$, so

$$\#H^1_{\phi^*}(\mathbb{Q}, A_l) \leq \#H^1_f(\mathbb{Q}, A_l),$$

if they are finite. But they are finite, in fact this reads

$$|\#\widetilde{Ш}|_l^{-1} \leq |\#Ш|_l^{-1},$$

because in this case the triviality of $H^1_f(\mathbb{Q}, V_l(-1))$ implies that of $H^1_f(\mathbb{Q}, V_l)$, using II.2.2.2 of [FP] as in the proof of Theorem 8.2 of [DFG2].

We have

$$|\#\widetilde{Ш}|_l^{-1} \leq |\#Ш|_l^{-1} = |\#Ш(-1)|_l^{-1} \leq |\#\widetilde{Ш}(-1)|_l^{-1},$$

but we have equality of the terms at either end of this sequence of inequalities, therefore equality throughout, and $|\#Ш|_l^{-1} = \#H^1_\phi(\mathbb{Q}, A_l(-1))$, as required. □

9. The reducible case, examples

In [Du] we looked at many examples of semi-stable elliptic curves for which the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $A'[l]$ is reducible and therefore the theorem of [DFG2] does not apply. In fact we concentrated on examples where E possesses a rational point of order $l = 5$. The formula (10) of [Fl1], in the case where E is semi-stable (i.e. N is square-free), shows that the Bloch-Kato conjecture for $L(\mathrm{Sym}^2(E), 2)$ is equivalent to

$$\frac{\deg \phi}{Nc^2} = \frac{\#Ш}{\#H^0(\mathbb{Q}, A)\#H^0(\mathbb{Q}, A(-1))} \prod_{p \leq \infty} c_p. \tag{9}$$

Here, ϕ is a modular parametrisation of E and c is the associated Manin constant. If (semi-stable) E is a strong Weil curve within its isogeny class (as in the following examples) then c is at worst a power of 2, so has trivial l-part for odd prime l, in fact if N is also odd then it is known that $c = 1$ [AU]. In [Du] we had to restrict to the case where $l \nmid N$ so that E has good reduction at l, but now, armed with Proposition 7.1, we may consider examples where $l \mid N$ and E has multiplicative reduction at l, using (9) to predict the l-part of the order of Ш. The examples below were the first few found in the tables of [Cr]. In all cases there is (by choice) a rational point of order 5. $[a_1, a_2, a_3, a_4, a_6]$ are the coefficients in a minimal Weierstrass equation for E, and Δ is the minimal discriminant. C is the 5-part of the product $\prod c_p$ (determined using Lemma 3.1 (with Lemma 3.3 of [Du]) and Proposition 7.1), D is the 5-part of $\#H^0(\mathbb{Q}, A)\#H^0(\mathbb{Q}, A(-1))$ (determined using Lemmas 4.3 and 4.4 of [Du]), deg is the 5-part of $\deg \phi$ and #5-Ш ? is the order of the 5-part of Ш predicted by (9) by plugging in all the other quantities.

Name	$[a_1, a_2, a_3, a_4, a_6]$	Δ	C	D	deg	Rank	#5-Ш ?
110A1	$[1, 1, 1, 10, -45]$	$-2^5 5^5 11$	5	5	5	0	1
155A1	$[0, -1, 1, 10, 6]$	$-5^5 31$	1	5	5	1	5
395C1	$[0, -1, 1, -50, 156]$	$-5^5 79$	1	5	1	0	1
665D1	$[0, -1, 1, -210, 6798]$	$-5^5 7^5 19^2$	5	5	5^2	1	5
710D1	$[1, 1, 1, -1105, 11727]$	$2^5 5^{10} 71$	5	5	5	0	1
885D1	$[0, 1, 1, -280, 1684]$	$3^5 5^5 59$	5	5	5^2	1	5
890G1	$[1, 1, 1, 10, 147]$	$-2^5 5^5 89$	5	5	5^2	1	5
1155N1	$[0, 1, 1, -8940, 378056]$	$-3^5 5^5 7^5 11^3$	5^2	5	5^3	1	5
1310C1	$[1, 1, 1, -95, 357]$	$-2^5 5^5 131$	5	5	5	0	1
1745E1	$[0, -1, 1, -4420, 114556]$	$5^{10} 349$	1	5	5^3	0	5^3
1790D1	$[1, 1, 1, -1455, 20725]$	$2^{10} 5^5 179$	5	5	5^2	1	5
1870H1	$[1, 1, 1, -2439835, 1467522537]$	$-2^{15} 5^5 11^4 17^5$	5^2	5	5^3	1	5
2090N1	$[1, 1, 1, -485, 3915]$	$-2^5 5^5 11 \cdot 19$	5	5	5^2	0	5
2110E1	$[1, 1, 1, -90, 1255]$	$-2^{10} 5^5 211$	5	5	5	0	1
2170Q1	$[1, 1, 1, -9995, -160455]$	$2^{15} 5^5 7^5 31$	5^2	5	5^3	1	5
2235F1	$[0, 1, 1, -20, 506]$	$-3^5 5^5 149$	5	5	5^2	1	5
2290D1	$[1, 1, 1, -180, 1525]$	$-2^{10} 5^5 229$	5	5	5^2	1	5
2370M1	$[1, 0, 0, -3280, -517600]$	$-2^5 3^{15} 5^5 79$	5^2	5	5^2	0	1
2715C1	$[0, 1, 1, -140, 806]$	$-3^5 5^5 181$	5	5	5	0	1

Observe that, in all but two of these examples, $\#5\text{-Ш}\,? = 5^{\mathrm{Rank}}$. When E has a rational point of order $l \geq 5$, it is shown in §5 of [Du] (under certain conditions) how to use rational points of infinite order to produce elements of order l in Ш, in the case when E has *good reduction* at l. If this construction still works in the case of multiplicative reduction, it would provide some sort of explanation for the above observation. However, now it seems to be more difficult to deal with the local condition at l.

References

[AU] A. Abbes, S. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires,* Compositio Math. **103** (1996), 269–286.

[BK] S. Bloch, K. Kato, *L-functions and Tamagawa numbers of motives,* The Grothendieck Festschrift Volume I, 333–400, Progress in Mathematics, **86**, Birkhäuser, Boston, 1990.

[Br1] C. Breuil, *Construction de représentations p-adiques semi-stables,* Ann. Sci. École Norm. Sup. 4^e série, **31** (1998), 281–327.

[Br2] ———, *Cohomologie étale de p-torsion et cohomologie cristalline en réduction semi-stable,* Duke Math. J. **95** (1998), 523–620.

[Br3] ———, *p-adic Hodge theory, deformations and local Langlands, informal notes of lectures at Barcelona,* July 2001, http://www.math.u-psud.fr/~breuil/liste-prepub.html

[Br4] ———, *Representations p-adiques semi-stables et transversalite de Griffiths,* Math. Ann. **307** (1997), 191–224.

[BCDT] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises,* J. Amer. Math. Soc. **14** (2001), 843–939.

[CF] P. Colmez, J.-M. Fontaine, *Construction des représentations p-adiques semi-stables,* Invent. Math. **140** (2000), 1–43.

[CS] J. Coates, C.G. Schmidt, *Iwasawa theory for the symmetric square of an elliptic curve,* J. Reine Angew. Math. **375/376** (1987), 104–156.

[Cr] J. Cremona, *Elliptic curve data,* http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html.

[DDT] H. Darmon, F. Diamond, R. Taylor, *Fermat's Last Theorem. Elliptic Curves, Modular Forms and Fermat's Last Theorem (2nd ed.),* 2–140, International Press, Cambridge MA, 1997.

[De] P. Deligne, *Valeurs de Fonctions L et Périodes d'Intégrales,* AMS Proc. Symp. Pure Math., **33** (1979), part 2, 313–346.

[DFG1] F. Diamond, M. Flach, L. Guo, *On the Bloch-Kato conjecture for adjoint motives of modular forms,* Math. Res. Lett. **8** (2001), 237–242.

[DFG2] ———, *Adjoint motives of modular forms and the Tamagawa number conjecture, preprint.* http://www.andromeda.rutgers.edu/~liguo/lgpapers.html

[Du] N. Dummigan, *Symmetric squares of elliptic curves: rational points and Selmer groups,* Experiment. Math., **11** (2002), 457–464.

[Fl1] M. Flach, *On the degree of modular parametrisations, Séminaire de Théorie des Nombres,* Paris 1991-92 (S. David, ed.), 23–36, Progress in mathematics, **116**, Birkhäuser, Basel Boston Berlin, 1993.

[Fl2] ———, *A finiteness theorem for the symmetric square of an elliptic curve,* Invent. Math. **109** (1992), 307–327.

[Fl3] ———, *A generalisation of the Cassels-Tate pairing,* J. reine angew. Math. **412** (1990), 113–127.

[Fo1] J.-M. Fontaine, *Le corps de périodes p-adiques,* Astérisque **223** (1994), 59–111.

[Fo2] ———, *Représentations p-adiques semi-stables,* Astérisque **223** (1994), 113–184.

[Fo3] ———, *Valeurs spéciales des fonctions L des motifs, Séminaire Bourbaki, Vol. 1991/92.* Astérisque **206** (1992), Exp. No. 751, 4, 205–249.

[Fo4] ———, Letter to U. Jannsen, Nov. 26, 1987.

[FP] J.-M. Fontaine, B. Perrin-Riou, *Autour des conjectures de Bloch et Kato: cohomologie galoisienne et valeurs de fonctions L,* In: Motives, A.M.S. Proc. Symp. Pure Math. **55**, Part 1 (1994), 599–706.

[GJ] S. Gelbart, H. Jacquet, *A relation between automorphic representations of $GL(2)$ and $GL(3)$,* Ann. Sci. École Norm. Sup. 4^e série, **11** (1978), 471–542.

[GS] R. Greenberg, G. Stevens, *p-adic L-functions and p-adic periods of modular forms,* Invent. Math. **111** (1993), 407–447.

[Hi] H. Hida, *Geometric modular forms and elliptic curves,* World Scientific, Singapore, 2000.

[HK] O. Hyodo, K. Kato, *Semi-stable reduction and crystalline cohomology with logarithmic poles,* Astérisque **223** (1994), 221–268.

[I] L. Illusie, *Réduction semi-stable ordinaire, cohomologie étale p-adique et cohomologie de de Rham d'aprés Bloch-Kato et Hyodo, appendix to* [P1]*,* Astérisque **223** (1994), 209–220.

[K1] K. Kato, *Semi-stable reduction and p-adic étale cohomology,* Astérisque **223** (1994), 269–293.

[K2] ———, *Logarithmic structures of Fontaine-Illusie,* in *Algebraic analysis, geometry and number theory (J. Igusa, ed.),* 191–224, Johns Hopkins University Press, Baltimore, 1989.

[M] B. Mazur, *On monodromy invariants occurring in global arithmetic, and Fontaine's theory,* Contemp. Math. **165** (1994), 1–20.

[MTT] B. Mazur, J. Tate, J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer,* Invent. Math. **84** (1986), 1–48.

[N] A. Néron, *Modèles minimaux des variétés abéliennes sur les corps locaux et globaux,* IHES Publ. Math. **21** (1964), 361–482.

[P1] B. Perrin-Riou, *Représentations p-adiques ordinaires,* Astérisque **223** (1994), 185–207.

[P2] ———, *p-adic L-functions and p-adic representations,* SMF/AMS Texts and Monographs, **3**, 2000 (Astérisque 229, 1995).

[Sh1] G. Shimura, *On the holomorphy of certain Dirichlet series,* Proc. London Math. Soc. (3) **31** (1975), 79–98.

[Sh2] ———, *The special values of the zeta functions associated with cusp forms,* Comm. Pure Appl. Math. **29** (1976), 783–804.

[Si] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves,* GTM 151, Springer-Verlag, New York, 1994.

[TW] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras,* Ann. Math. **141** (1995), 553–572.

[Ts] T. Tsuji, *p-adic étale cohomology and crystalline cohomology in the semi-stable reduction case,* Invent. Math. **137** (1999), 233–411.

[Wa] M. Watkins, *Computing the modular degree of an elliptic curve,* Experiment. Math. **11** (2002), 487–502

[Wi] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem,* Ann. Math. **141** (1995), 443–551.

University of Sheffield, Department of Pure Mathematics, Hicks Building, Hounsfield Road, Sheffield, S3 7RH, U.K.

E-mail address: n.p.dummigan@shef.ac.uk