Symmetric Squares of Elliptic Curves: Rational Points and Selmer Groups

Neil Dummigan

CONTENTS

2000 AMS Subject Classification: Primary 11G40, 14G10;

Keywords: Elliptic curve, symmetric square L-function, Bloch-Kato conjecture

We consider the Bloch-Kato conjecture applied to the symmetric square L-function of an elliptic curve over $\mathbb{Q}$, at $s = 2$. In particular, we use a construction of elements of order l in a generalised Shafarevich-Tate group, which works when E has a rational point of infinite order and a rational point of order l. The existence of the latter places us in a situation where the recent theorem of Diamond, Flach, and Guo does not apply, but we find that the numerical evidence is quite convincing.

1. INTRODUCTION

Let E be an elliptic curve defined over $\mathbb{Q}$ and let $L(E, s)$ be the associated L-function. (It is now known that E is modular, so that $L(E, s)$ has an analytic continuation to the whole complex plane.) The conjecture of Birch and Swinnerton-Dyer predicts that the order of vanishing of $L(E, s)$ at $s = 1$ is the rank of the group $E(\mathbb{Q})$ of rational points, and also gives an interpretation of the leading term in the Taylor expansion in terms of various quantities, including the order of the Shafarevich-Tate group.

The Bloch-Kato conjecture [Bloch and Kato 90] is the generalisation to arbitrary motives of the leading term part of the Birch and Swinnerton-Dyer conjecture. Let $L(\mathrm{Sym}^2(E), s)$ be the symmetric square L-function attached to an elliptic curve $E/\mathbb{Q}$. Flach [Flach 93] looked at the Bloch-Kato conjecture for $L(\mathrm{Sym}^2(E), s)$ at $s = 2$, and translated it into a formula involving only rational numbers, such as the degree of a modular parametrisation, and the order of a generalised Shafarevich-Tate group. In [Flach 92] he applied Kolyvagin's technique for bounding Selmer groups, to $\mathrm{Sym}^2(E)$ at $s = 2$. Theorem 1 of [Flach 93] applies the result of [Flach 92] to prove the l-part of the Bloch-Kato formula for all primes $l > 3$ such that E has good reduction at l, l does not divide the degree of the modular parametrisation, and the representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{F}_l)$ arising from

1058-6458/2001 $0.50 per page

the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the l-torsion points of E is surjective. (Under these conditions, the l-part of the generalised Shafarevich-Tate group is trivial.)

Modified l-Selmer groups associated to $\mathrm{Sym}^2(E)$ at $s = 2$ are intimately connected with the deformation theory of the above Galois representation. This connection lies at the heart of Wiles's approach to the Shimura-Taniyama-Weil conjecture, that every elliptic curve $E/\mathbb{Q}$ is modular. Although the work of Taylor and Wiles [Wiles 95], [Taylor and Wiles 95] does not actually prove the relevant cases of the Bloch-Kato conjecture (the Selmer groups are defined differently), it is clearly closely related.

Diamond, Flach and Guo [Diamond et al. 01a, Diamond et al. 01b] 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.)

In [Dummigan 01a], I looked at $L(\mathrm{Sym}^2(f), s)$, where f is a Hecke eigenform of level one and weight k, concentrating on the weights $k = 12, 16, 18, 20, 22, 26$, for which f has rational Fourier coefficients. For $k = 18, 22, 26$ (when $k/2$ is odd), the Bloch-Kato conjecture turns out to be especially interesting at the point $s = (k-1)+(k/2)$. It is possible to construct elements of order l in the relevant Selmer groups, where l is an "Eisenstein" prime, and these primes do appear, at $s = (k-1)+(k/2)$, when the critical values of the L-function are calculated. [Dummigan 01b] deals with something similar for a Hilbert modular form.

The point $s = (k-1)+(k/2)$ coincides with the point $s = k$ dealt with in [Diamond et al. 01a] only when $k = 2$. (Of course, if $k = 2$, there are no nonzero modular forms of level one, but the level one restriction is no longer necessary when we have an elliptic curve to work with.) The construction of [Dummigan 01a] can be made to work in the case that $E(\mathbb{Q})$ has both a point of order l and a point of infinite order. A suitable point of infinite order gives rise, via the "descent" map, to a nonzero element of $H^1(\mathbb{Q}, E[l])$. Thanks to the existence of the rational point of order l, $E[l]$ is isomorphic to a Galois submodule of $\mathrm{Sym}^2(E[l])$, and we get a nonzero element $c \in H^1(\mathbb{Q}, \mathrm{Sym}^2(E[l]))$. The main problem we face is to show that c (or rather its image in another group) satisfies all the local conditions required for it to belong to the appropriate Bloch-Kato Selmer group. To facilitate this, we assume that E has good reduction at l, and impose some technical conditions which are satisfied by most of the examples we look at (see the precise statement of Theorem 5.1).

Cremona and Mazur [2000] look, among all strong Weil elliptic curves over $\mathbb{Q}$ of conductor $N \leq 5500$, at those with nontrivial Shafarevich-Tate group (according to the Birch and Swinnerton-Dyer conjecture). Suppose that the Shafarevich-Tate group has predicted elements of prime order m. In most cases, they find another elliptic curve, often of the same conductor, whose m-torsion is Galois-isomorphic to that of the first one, and which has rank two. The rational points on the second elliptic curve produce classes in the common $H^1(\mathbb{Q}, E[m])$. They show [Cremona and Mazur 02] that these lie in the Shafarevich-Tate group of the first curve, so rational points on one curve explain elements of the Shafarevich-Tate group of the other curve. Clearly, the construction of the present paper is analogous to this.

Ironically, the rational point of order l which allows the construction to proceed causes the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to be reducible, so the results of [Flach 92] and [Diamond et al. 01a] do not apply to the l-part of the Bloch-Kato conjecture for $L(\mathrm{Sym}^2(E), 2)$. Therefore, it is appropriate to consider numerical evidence. We must take $l > 3$, since the 2- and 3-parts of the fudge factors occurring in this instance of the Bloch-Kato formula are not well understood. Since there cannot be a rational l-torsion point for $l > 7$ [Mazur 78], the only relevant l are $l = 5$ and $l = 7$. We concentrate on the case $l = 5$, which occurs with much greater frequency in lists of elliptic curves ordered by conductor. With the exception of the order of the (generalised) Shafarevich-Tate group, all the quantities appearing in the l-part of the Bloch-Kato formula appear in, or may be calculated from, the elliptic curve data in Cremona's tables, for all conductors $N \leq 8000$. These tables may be found at http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html. We find that the data fit well with both the conjecture and our construction.

2. THE SYMMETRIC SQUARE L-FUNCTION

Let $E/\mathbb{Q}$ be 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, $V_l \simeq H^1(\overline{E}, \mathbb{Q}_l)(1)$.

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 $A'[l^n] := \mathrm{Sym}^2(E[l^n])$. Note that if $a \otimes b \in E[l^{n+1}] \otimes E[l^{n+1}]$, then $l(a \otimes b) = la \otimes b = a \otimes lb$ is identified with $la \otimes lb \in E[l^n] \otimes E[l^n]$. As Galois modules, $V_l' \simeq \mathrm{Sym}^2(H^1(\overline{E}, \mathbb{Q}_l))(2)$. Let $A' = \oplus_l A_l'$.

The L-function of the motive $\mathrm{Sym}^2 h^1(E)$ is defined, for $\Re(s) > 2$, by a Dirichlet series given by an Euler product

$$L(\mathrm{Sym}^2 E, s) = \prod_r P_r(r^{-s})^{-1}.$$

The product is over all primes r, and the polynomial $P_r(X) := \det(1 - \mathrm{Frob}_r^{-1} X \mid V_l'^{I_r})$, where I_r is an inertia subgroup at r, Frob_r is an arithmetic Frobenius element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and l is any prime different from r. These Euler factors may be determined explicitly, see [Coates and Schmidt 87] and [Watkins 02]. Suffice it to say here that if r is a prime of good reduction of E, then $P_r(X) = (1 - \alpha_r^2 X)(1 - \beta_r^2 X)(1 - rX)$, α_r and β_r being the eigenvalues of Frob_r^{-1} on T_l.

Following [Bloch and Kato 90] (Section 3), for $p \neq l$ (including $p = \infty$) let

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

The subscript f stands for "finite part." 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

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

(see Section 1 of [Bloch and Kato 90] for definitions of Fontaine's ring B_{cris}). Let $H_f^1(\mathbb{Q}, V_l')$ be the subspace of elements of $H^1(\mathbb{Q}, V_l')$ whose local restrictions lie in $H_f^1(\mathbb{Q}_p, V_l')$ for all primes p. There is a natural exact sequence

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

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

$$Ш = \oplus_l \frac{H_f^1(\mathbb{Q}, A_l')}{\pi_* H_f^1(\mathbb{Q}, V_l')}.$$

Note that, since $s = 2$ is a noncentral critical point for $L(\mathrm{Sym}^2 E, s)$, it is conjectured that $H_f^1(\mathbb{Q}, V_l')$ is trivial, so the l-Selmer group should be identified with the l-part of the Shafarevich-Tate group.

3. THE BLOCH-KATO FORMULA: FUDGE FACTORS

Let $f(z) = \sum_{n=1}^{\infty} a_n q^n$ $(q = e^{2\pi i z})$ be the normalised $(a_1 = 1)$ newform of weight 2 and level N associated with the elliptic curve E. (For $p \nmid N$, the number of points of $E(\mathbb{F}_p)$ is $1 + p - a_p$.) Let $\phi : X_0(N) \to E$ be a modular parametrisation. Let c be the associated Manin constant, i.e., $\phi^* \omega = c \cdot 2\pi i f(z) dz$, where ω is a Néron differential on E, chosen so that c is positive.

The symmetric square L-function $L(\mathrm{Sym}^2 E, s)$ is closely related to the Rankin convolution $\sum_{n=1}^{\infty} a_n^2 n^{-s}$, and $L(\mathrm{Sym}^2 E, 2)$ may be evaluated using the Rankin-Selberg method [Rankin 39], [Shimura 76]. Careful comparison of this with the conjectural formula of Bloch and Kato [Bloch and Kato 90] leads to formula (10) of [Flach 93]:

$$\frac{\deg \phi}{Nc^2} \prod_{r \in S^{\pm}} \frac{r}{r \pm 1} = \frac{\#Ш}{\#H^0(\mathbb{Q}, A') \#H^0(\mathbb{Q}, A'(-1))} \prod_{r \leq \infty} c_r. \tag{3–1}$$

Here, $S^{\pm}$ are certain sets of primes of bad additive reduction. In the examples we look at later, E is always semistable, so $S^{\pm}$ are empty. For precise definitions, see [Flach 93]. Likewise, the c_r are certain "fudge factors." The following corrected Lemma 1 of [Flach 93] provides us with what we need to know about them. If j is the j-invariant of the elliptic curve E and r is a finite prime, let $d_r = -\mathrm{ord}_r(j)$.

Lemma 3.1. *$c_r = 1$ for all but finitely many r. Up to powers of 2 and 3, and powers of r if r is a prime of bad reduction, we have*

$$c_r = \begin{cases} 1 & \text{if } d_r \leq 0 \text{ or } r = \infty; \\ \#E(\mathbb{Q}_r)[d_r] & \text{if } d_r > 0. \end{cases}$$

The proof is essentially identical to the proof of Lemma 1 in [Flach 93]. To apply the lemma, we need to be able to calculate $\#E(\mathbb{Q}_r)[d_r]$ in the case $d_r > 0$. In the proof of Lemma 1 of [Flach 93], the l-part of $E(\mathbb{Q}_r)[d_r]$ is isomorphic to $\mathbb{Z}_l(1)/d_r \oplus \mathbb{Z}_l/d_r$ as an I_r-module, but not necessarily as a $\mathrm{Gal}(\overline{\mathbb{Q}}_r/\mathbb{Q}_r)$-module, so the formula given there is not always correct.

We need to use the following proposition, due to Tate. A published proof may be found in [Silverman 94] (see Lemma 5.1, Theorem 5.3, and Corollary 5.4).

Proposition 3.2. *Let E be an elliptic curve defined over $\mathbb{Q}_r$, with $\mathrm{ord}_r(j) =: -d_r < 0$. There is a unique $q \in \mathbb{Q}_r$ such that $j(E) = \frac{1}{q} + 744 + 196884q + \ldots$.*

(i) If E has split multiplicative reduction, then there is an isomorphism of groups, respecting the actions of $\mathrm{Gal}(\overline{\mathbb{Q}}_r/\mathbb{Q}_r)$*:*

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

(ii) If E has either nonsplit multiplicative reduction or additive reduction, then there exists a quadratic extension L of $\mathbb{Q}_r$ such that

$$E(\mathbb{Q}_r) \simeq \{u \in L^*/q^{\mathbb{Z}} : N_{L/\mathbb{Q}_r}(u) \in q^{\mathbb{Z}}/q^{2\mathbb{Z}}\}.$$

In the case of nonsplit multiplicative reduction, the extension is unramified.

With little trouble one may deduce the following lemma, which tells us the l-part of c_r in certain cases.

Lemma 3.3. *As above, suppose that $E/\mathbb{Q}_r$ with $d_r > 0$. Let $l \neq r$ be an odd prime with l^a exactly dividing d_r.*

(i) If E has split multiplicative reduction, then $\#E(\mathbb{Q}_r)[l^a] = l^{a+\min\{b,c\}}$, where $l^b = \gcd(l^a, r-1)$ and $c = \max\{e \leq a : (q/r^{d_r}) \text{ is a } l^e\text{-power} \pmod r\}$.

(ii) If E has nonsplit multiplicative reduction, then

$$\#E(\mathbb{Q}_r)[l^a] = \gcd(l^a, r+1).$$

Note that j is the product of $1/q$ and a 1-unit in $\mathbb{Q}_r$. Since 1-units in $\mathbb{Q}_r$ are l^e-powers, "q/r^{d_r}" may be replaced by "jr^{d_r}" in the above lemma. It may not be replaced by or "Δ/r^{d_r}," where Δ is the minimal discriminant of $E/\mathbb{Q}$, since this may differ from $q\prod_{n=1}^{\infty}(1-q^n)^{24}$ by multiplication by the 12^{th} power of some r-adic number which is not an l^{th} power. This is illustrated by the example 506D1 in Section 6.3.

Cremona's table of Hecke eigenvalues includes the eigenvalues of the Atkin-Lehner involutions W_p for $p \mid N$. If p is a prime of multiplicative reduction, that reduction is split or nonsplit according as the eigenvalue of W_p is -1 or $+1$ respectively.

In the examples we look at later, l is a prime of good reduction, so certainly $l \neq r$ when $d_r > 0$. Also, since $l \nmid N$, the factor N in (3–1) has trivial l-part. By Corollary 4.2 of [Mazur 78], if N is square-free and E is a strong Weil curve within its isogeny class (as in all the examples of conductor ≤ 8000 that we examine later), then the Manin constant c is at worst a power of 2, and has trivial l-part for odd prime l. In fact, if N is also odd, it is now known that $c = 1$ [Abbes and Ullmo 96].

4. GLOBAL TORSION

Next we look at the factors appearing in the denominator of (3–1).

Lemma 4.1. *If l is an odd prime and $E[l]$ is an irreducible representation of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *over $\mathbb{F}_l$, then $\#H^0(\mathbb{Q}, A')$ and $\#H^0(\mathbb{Q}, A'(-1))$ both have trivial l-part.*

Proof: Via the Weil pairing, $E[l]$ is dual to $E[l](-1)$, as a Galois module. Hence

$$E[l] \otimes E[l](-1) \simeq \mathrm{Hom}_{\mathbb{F}_l}(E[l], E[l])$$

as modules for $\mathbb{F}_l[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$. Symmetric tensors correspond to linear maps of zero trace. $H^0(\mathbb{Q}, E[l]\otimes E[l](-1))$ corresponds to $\mathrm{Hom}_{\mathbb{F}_l[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]}(E[l], E[l])$, which by Schur's Lemma consists of scalar multiples of the identity. (Note that, since l is odd, $E[l]$, as an odd, irreducible representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, is absolutely irreducible.) The only such map having zero trace is the zero map. Hence the l-part of $\#H^0(\mathbb{Q}, A'(-1))$ is trivial. Since $E[l]$ is not isomorphic to $E[l](1)$ as a Galois module, $\#H^0(\mathbb{Q}, A')$ also has trivial l-part. □

The following comes from Proposition 21 of [Serre 72], and provides us with a practical way of applying the previous lemma.

Proposition 4.2. *Suppose that N is square-free (i.e., E is semistable). If $l > 3$ is a prime, then $E[l]$ is irreducible unless $a_p \equiv 1 + p \pmod l$ for all primes $p \nmid lN$.*

If E is semistable and $a_p \equiv 1 + p \pmod l$ for all primes $p \nmid lN$, then the composition factors of $E[l]$ are $\mathbb{F}_l$ and $\mathbb{F}_l(1)$ (by Proposition 21 of [Serre 72]). Using $E[l] \otimes E[l](-1) \simeq \mathrm{Hom}_{\mathbb{F}_l}(E[l], E[l])$, it is easy to prove the following lemma.

Lemma 4.3. *Let l be an odd prime, $E/\mathbb{Q}$ an elliptic curve.*

(i) If $E[l] \simeq \mathbb{F}_l \oplus \mathbb{F}_l(1)$, then $l \mid \#H^0(\mathbb{Q}, A'(-1))$ and $l \mid \#H^0(\mathbb{Q}, A')$.

(ii) If $E[l]$ has a submodule, but not a quotient isomorphic to $\mathbb{F}_l$ (i.e., if E has a rational point of order l, but is not l-isogenous to an elliptic curve with a rational point of order l), then $l \mid \#H^0(\mathbb{Q}, A'_l)$, but the l-part of $\#H^0(\mathbb{Q}, A'(-1))$ is trivial.

(iii) If $E[l]$ has a submodule, but not a quotient isomorphic to $\mathbb{F}_l(1)$ (i.e., if E has no rational point of order l, but is l-isogenous to an elliptic curve

with a rational point of order l), then the l-part of $\#H^0(\mathbb{Q}, A'(-1))$ is trivial. If $l > 3$, then so is the l-part of $\#H^0(\mathbb{Q}, A')$.

Lemma 4.4. *Let l be an odd prime, $E/\mathbb{Q}$ an elliptic curve with a prime r of split multiplicative reduction such that $l \nmid (r-1)$ and $l^2 \nmid \mathrm{ord}_r(j)$. Then the divisibilities in the above lemma are exact. (For the case of $\#H^0(\mathbb{Q}, A')$ in (i), we must also assume that $l > 3$.)*

Proof: We just prove part (ii) to illustrate the idea. There is an obvious $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant map from $E[l]$ to $E[l](1)$ which maps the quotient of $E[l]$ isomorphic to $\mathbb{F}_l(1)$ to the submodule of $E[l](1)$ isomorphic to $\mathbb{F}_l(1)$, and this spans $H^0(\mathbb{Q}, A'[l])$. We need to show it is not divisible by l. Suppose for a contradiction that $\theta : E[l^2] \to E[l^2](1)$ is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant map dividing it by l. Choose a $\mathbb{Z}/l^2\mathbb{Z}$-basis $\{v_1, v_2\}$ for $E[l^2]$ such that under the Tate parametrisation of $E(\overline{\mathbb{Q}}_r)$, v_1 corresponds to a primitive l^2-root of unity, and v_2 corresponds to a chosen q^{1/l^2}, q being the Tate parameter of E. Since $l \nmid (r-1)$, the $\mathrm{Gal}(\overline{\mathbb{Q}}_r/\mathbb{Q}_r)$-modules $\mathbb{F}_l$ and $\mathbb{F}_l(1)$ are nonisomorphic, and lv_1 must generate the quotient of $E[l]$ isomorphic to $\mathbb{F}_l(1)$, and maps under $l\theta$ to a point of order l in $E(\mathbb{Q}_r)(1)$. Hence $\theta(v_1)$, untwisted, is a point of order l^2 in $E(\mathbb{Q}_r)$, but the hypotheses preclude the existence of such a point. □

Remark 4.5. If E has a rational point of order l and r is a prime of multiplicative reduction such that $l \nmid (r+1)$, then necessarily it is split multiplicative reduction, by something like (ii) of Lemma 3.3.

5. THE CONSTRUCTION OF ELEMENTS IN A SELMER GROUP

Theorem 5.1. *Let $l > 3$ be a prime, $E/\mathbb{Q}$ an elliptic curve with a prime r of split multiplicative reduction such that $l \nmid (r-1)$ and $l^2 \nmid \mathrm{ord}_r(j)$. Suppose that E has a rational point Q of order l. Suppose also that E has good reduction at l, and that for any prime p of bad reduction, $E[l^\infty](\mathbb{Q}_p)$ has order l. Then the l-torsion subgroup of the Selmer group $H^1_f(\mathbb{Q}, A'_l)$ has dimension greater than or equal to the rank of $E(\mathbb{Q})$.*

Proof: There is a natural injection ψ from $E(\mathbb{Q})/lE(\mathbb{Q})$ into $H^1(\mathbb{Q}, E[l])$. Since $E(\mathbb{Q})$ contains the point Q of order l, $E[l]$ has a submodule isomorphic to $\mathbb{F}_l$, with quotient $\mathbb{F}_l(1)$. Hence $A'[l] := \mathrm{Sym}^2(E[l])$ has a submodule isomorphic to $E[l]$, with quotient $\mathbb{F}_l(2)$. Since $H^0(\mathbb{Q}, \mathbb{F}_l(2))$ is trivial, we get an injection θ from $H^1(\mathbb{Q}, E[l])$ to $H^1(\mathbb{Q}, A'[l])$. Given the assumptions we have made, as in the proof of Lemma 4.4, $H^0(\mathbb{Q}, A'_l) = H^0(\mathbb{Q}, A'[l])$. It follows that the image in $H^1(\mathbb{Q}, A'[l])$ of $H^0(\mathbb{Q}, A'_l)/lH^0(\mathbb{Q}, A'_l)$ (i.e., the kernel of the natural map from $H^1(\mathbb{Q}, A'[l])$ to $H^1(\mathbb{Q}, A'_l)$) is one-dimensional. Hence the image of $E(\mathbb{Q})/lE(\mathbb{Q})$ in the l-torsion of $H^1(\mathbb{Q}, A'_l)$ has dimension at least as big as the rank of $E(\mathbb{Q})$. For $P \in E(\mathbb{Q})$, let $c = \psi(P), c' = \theta(c)$ and let d' be the image in $H^1(\mathbb{Q}, A'_l)$ of c'. Assume P is chosen in such a way that $d' \neq 0$. We need to show that, for every finite prime p, $\mathrm{res}_p(d') \in H^1_f(\mathbb{Q}_p, A'_l)$.

Since $l > 3$ is a prime of good reduction, one may prove the local condition at $p = l$ using Fontaine-Lafaille modules, as in the proof of Proposition 9.2 of [Dummigan 01a].

Next consider a prime $p \neq l$ of good reduction. As is well-known (Proposition 2.1 in Chapter 8 of [Silverman 86]), the class $c \in H^1(\mathbb{Q}, E[l])$ is unramified at p. Hence the class $d' \in H^1(\mathbb{Q}, A'_l)$ is unramified at p. Since A'_l is unramified at p (a prime of good reduction), $H^1_f(\mathbb{Q}_p, A'_l)$ is equal to (not just contained in) the kernel of the map from $H^1(\mathbb{Q}_p, A'_l)$ to $H^1(I_p, A'_l)$, where I_p is an inertia subgroup at p (see line 3 of p. 125 of [Flach 90]). Hence $d' \in H^1_f(\mathbb{Q}_p, A'_l)$.

Finally, suppose that $p \neq l$ is a prime of bad reduction. It is easy to check (using Tate curves) that $H^1_f(\mathbb{Q}_p, V'_l) = \{0\}$, so we need to show that $\mathrm{res}_p(d') = 0$. Let $E_1(\mathbb{Q}_p)$ be the kernel of reduction $\pmod p$. Then $E_1(\mathbb{Q}_p)/lE_1(\mathbb{Q}_p)$ is trivial, and $E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p)$ is finite, so the class of P in $E(\mathbb{Q}_p)/lE(\mathbb{Q}_p)$ may be represented by some l-power torsion point $R \in E(\mathbb{Q}_p)$. (What we have really done here is just to confirm that the image of $E(\mathbb{Q}_p)$ in $H^1(\mathbb{Q}_p, A_l)$ is $H^1_f(\mathbb{Q}_p, A_l) = \{0\}$.) By assumption, R must be a multiple of Q, so it suffices to consider the case $R = Q$.

Let $\pi_n : E[l^n] \otimes E[l^n] \to \mathrm{Sym}^2 E[l^n] = A'[l^n]$ be the projection map, $\pi_n(a \otimes b) = \frac{1}{2}(a \otimes b + b \otimes a)$. Choose $S \in E[l^2]$ such that $lS = Q$. Since $Q \in E(\mathbb{Q})$, we also have $lS^\sigma = Q$ for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ (or $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$). Then $\mathrm{res}_p(c') \in H^1(\mathbb{Q}_p, A'[l])$ is represented by the cocycle $\sigma \mapsto \pi_1((S^\sigma - S) \otimes Q)$. Viewing it as an element of $H^1(\mathbb{Q}_p, A'[l^2])$ via the natural inclusion, it is represented by the cocycle $\sigma \mapsto \pi_2((S^\sigma - S) \otimes S)$ and also by $\sigma \mapsto \pi_2((S^\sigma - S) \otimes S^\sigma)$, since both $lS = Q$ and $lS^\sigma = Q$. Expanding out the left-hand factor, adding these expressions, and exploiting the symmetry of π_2, we see that $2\mathrm{res}_p(c') \in H^1(\mathbb{Q}_p, A'[l^2])$ is represented by the cocycle $\sigma \mapsto \pi_2(S^\sigma \otimes S^\sigma - S \otimes S)$, which is the image in

$H^1(\mathbb{Q}_p, A'[l])$ of $[\pi_1(Q \otimes Q)] \in H^0(\mathbb{Q}_p, A'_l)/lH^0(\mathbb{Q}_p, A'_l)$. This implies that $\mathrm{res}_p(d') \in H^1(\mathbb{Q}_p, A'_l)$ is zero, as required. □

6. EXAMPLES

6.1 Rank Zero with Rational Point of Order 5

We use Cremona's tables to examine the first 14 semistable strong Weil curves (ordered by conductor N) with $5 \nmid N$, rank zero and a rational point of order $l = 5$. We use his labelling for the curves. There would be too many to go all the way to $N = 7998$. "deg" is the 5-part of the degree of the modular parametrisation. Using Lemmas 3.1 and 3.3, we compute C, defined to be the 5-part of the product $\prod c_r$ of local fudge factors, and using Lemmas 4.3 and 4.4, we compute (or bound) D, defined to be the 5-part of $\#H^0(\mathbb{Q}, A')\#H^0(\mathbb{Q}, A'(-1))$. The minimal discriminant is Δ and "#5-Ш?" is the order of the 5-part of Ш predicted by the Bloch-Kato formula (3–1). Note that since any bad reduction is multiplicative, d_r, which was defined to be $-\mathrm{ord}_r(j)$, is also $\mathrm{ord}_r(\Delta)$.

Name	Δ	C	D	deg	#5-Ш?
$11A1$	-11^5	5^2	$\geq 5^2$	1	≥ 1
$38B1$	$-2^5 19$	5	5	1	1
$57C1$	$-3^{10}19$	5	5	1	1
$58B1$	$-2^{10}29$	5	5	1	1
$66C1$	$2^{10}3^5 11$	5^2	5	5	1
$118B1$	$-2^{10}59$	5	5	1	1
$158C1$	$2^{20}79$	5	5	1	1
$186B1$	$-2^5 3^5 31$	5^2	5	5	1
$203A1$	$-7^5 29$	5	5	1	1
$246B1$	$-2^{25}3^5 41$	5^3	5	5^2	1
$286D1$	$-2^5 11^2 13^5$	5^2	5	5	1
$366B1$	$-2^5 3^5 61$	5^2	5	5	1
$426A1$	$-2^5 3^5 71$	5^2	5	5	1
$537E1$	$-3^{10}179$	5	5	1	1

By (3–1), the exponents of 5 in C and #5-Ш? add up to the same as those in D and deg. There is no particular reason to expect elements of order 5 in Ш, and in each case the predicted order of the 5-part of Ш is 1. The presence of rational 5-torsion forces $\#E(\mathbb{Q}_r)[5]$ to be divisible by 5. This produces powers of 5 dividing those c_r such that $5 \mid d_r$. These are beautifully balanced by powers of 5 dividing $\deg(\phi)$. See especially the example $246B1$.

6.2 No Rational Point of Order 5, Modular Parametrisation Degree Not Divisible by 5

This seems to apply to most curves, and is not a very interesting case. A random selection of ten is $14A1$, $26A1$, $38A1$, $57B1$, $66A1$, $69A1$, $82A1$, $102C1$, $122A1$, and $138B1$. For each of these there is no bad r such that $5 \mid d_r$, hence $C = 1$. Also, in each example there is no congruence $a_p \equiv 1 + p \pmod 5$ for all $p \nmid 5N$ (this may be checked using Cremona's table of Hecke eigenvalues), so by Lemmas 4.2 and 4.1, we find that $D = 1$. Hence, the 5-part of #Ш is predicted to be trivial in all these examples.

6.3 5 Dividing Modular Parametrisation Degree

Here are the first nine for which $5 \mid \deg(\phi)$, followed by the first five for which $5^2 \mid \deg(\phi)$. As before, we look only at semistable, strong Weil curves with $5 \nmid N$.

Name	Δ	$\#E(\mathbb{Q})_{\mathrm{tors.}}$	C	D	deg	#5-Ш?
$46A1$	$-2^{10}23$	2	1	1	5	5
$66C1$	$2^{10}3^5 11$	10	5^2	5	5	1
$67A1$	-67	1	1	1	5	5
$77B1$	$-7^6 11^3$	3	1	1	5	5
$78A1$	$-2^{16}3^5 13$	2	1	1	5	5
$89B1$	-89^2	2	1	1	5	5
$106D1$	$-2^5 53$	1	1	1	5	5
$114B1$	$2^2 3^5 19$	2	1	1	5	5
$114C1$	$2^{20}3^3 19$	4	5	1	5	1
$246B1$	$-2^{25}3^5 41$	5	5^3	5	5^2	1
$483A1$	$-3^5 7 \cdot 23^3$	1	5	1	5^2	5
$503C1$	-503	1	1	1	5^2	5^2
$506D1$	$2^5 11^5 23$	1	5	1	5^2	5
$573B1$	$3^5 191$	1	5	1	5^2	5

In the example $506D1$, which has split multiplicative reduction at 11, we find that $11^5 j = 3^3 13^3 1151^3/2^5 23$ is not a 5^{th} power (mod 11), so that $\#E(\mathbb{Q}_{11})[5]$ is only 5, not 5^2 (recall Lemmas 3.1 and 3.3). Also for $506D1$, the reduction at 2 is nonsplit, so $\#E(\mathbb{Q}_2)[5]$ is only 1, not 5. In several of the other examples, there are primes r of nonsplit multiplicative reduction such that $5 \mid d_r$.

In each of the above examples, since $5 \mid \deg(\phi)$, according to (3–1) either C or #Ш has to be divisible by 5, and it seems that it is sometimes one, sometimes the other (and sometimes both). In several cases, 5 divides some d_r without there being any rational point of order 5, though not always with the result that 5 divides C, since the reduction at r may be nonsplit.

Note also that Proposition 2 of [Flach 93] states that if $l > 3$ is a prime of good reduction such that the natural map from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{Aut}(E[l])$ is surjective, and if $l \mid d_r$, (for some bad r such that $d_r > 0$) then $l \mid \deg(\phi)$. He argues that since $l \mid d_r$, the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[l]$ is unramified at r. By work of Ribet,

the modular form f is then congruent (mod l) to some other modular form, of level dividing N/r. Hence l is a "congruence prime" and divides $\deg(\phi)$. The condition about the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is satisfied for semistable curves not satisfying $a_p \equiv 1+p \pmod{l}$ for all $p \nmid lN$, by Proposition 21 of [Serre 72]. In particular, it is satisfied in all the above examples except $66C1$. Of course, the main theorem of [Diamond et al. 01a] applies to all these examples (except $66C1$).

6.4 Positive Rank with Rational Point of Order 5

We examine all semistable strong Weil curves of conductor $N \leq 8000$, with $5 \nmid N$, rank at least one and a rational point of order 5. Amazingly, the very last curve in Cremona's main table is an example; in fact, it is the example with the largest value of C in Table 1. At the end of the table are several examples of larger conductor (and rank two or three), supplied by M. Watkins. (An asterisk signifies rank two, two asterisks signify rank three, otherwise the rank is one.) He found these using the parametrisation of elliptic curves with 5-torsion. He has checked in each case that the curve is not 5-isogenous to another one with rational 5-torsion. Though all the examples of conductor $N \leq 8000$ are definitely strong Weil curves, it is not certain that these examples of higher conductor are. See Section 3 of [Watkins 02] for a discussion of this problem, and Section 1 for his approach to calculating the modular degree. If some of these curves are not strong Weil, the numbers in the last two columns of the table should be multiplied by the 5-part of c^2. For the curves of rank three, that is the analytic rank, which we assume is equal to the rank of $E(\mathbb{Q})$.

In stark contrast to the examples in Section 6 (rank zero with a rational point of order 5), here the predicted order of Ш is always divisible by 5. This is in keeping with Theorem 5.1, which always produces a candidate for an element of order 5 in Ш, though in 5 out of the 26 rank-one examples the technical conditions of the theorem are not satisfied. For $2651C1$ there is no prime r of multiplicative reduction such that $5 \nmid (r-1)$. For each of $302A1$, $1717C1$, $2786D1$ and $2869B1$, there is a prime p (151, 101, 199 and 151 respectively) of bad reduction such that $E(\mathbb{Q}_p)$ has a point of order 25.

Looking at the examples of higher rank $R = 2$ or 3, it appears that the conditions of Theorem 5.1 are not merely a technical convenience. For most of these curves, the theorem produces 5^R elements of 5-torsion in the Selmer group, and the predicted order of the 5-part of Ш is at least 5^R. But the curve $5302I1$ and the curve of conductor 20042 fail the condition $\#E(\mathbb{Q}_{11})[5] = 5$, and the predicted order of the 5-part of Ш is only 5. It is easy to see in these two cases that the proof of Theorem 5.1 does at least supply 5 elements of 5-torsion in the Selmer group.

Watkins has also provided me with the following examples of curves of rank two with a rational point of order 7.

Name	Δ	C	D	deg	#5-Ш?
$123A1$	$-3^5 41$	5	5	5	5
$302A1$	$-2^{15}151$	5	5	5	5
$834G1$	$-2^{10}3^5139$	5^2	5	5^2	5
$862E1$	$-2^{20}431$	5	5	5	5
$874E1$	$2^5 19 \cdot 23^5$	5^2	5	5^2	5
$1147B1$	$31^2 37^5$	5	5	5	5
$1293E1$	$3^{15}431$	5	5	5	5
$1479F1$	$-3^5 17^5 29^2$	5^2	5	5^2	5
$1526E1$	$-2^5 7^5 109$	5^2	5	5^2	5
$1717C1$	$17^5 101$	5	5	5	5
$2651C1$	$-11^5 241$	5^2	≥ 5	5^2	≥ 5
$2786D1$	$-2^5 7^5 199$	5^2	5	5^2	5
$2869B1$	$19^5 151$	5	5	5	5
$3026D1$	$-2^5 17^5 89$	5^2	5	5^2	5
$3206E1$	$2^{10}7^{10}229$	5^2	5	5^2	5
$3542R1$	$2^{10}7^5 11^3 23^5$	5^3	5	5^3	5
$4043A1$	$-13^5 311$	5	5	5	5
$4774J1$	$-2^{15}7^5 11^2 31$	5^2	5	5^3	5^2
$4774K1$	$-2^{10}7^5 11 \cdot 31$	5^2	5	5^3	5^2
$4854C1$	$-2^{15}3^{10}809$	5^2	5	5^2	5
$4886F1$	$-2^5 7^5 349$	5^2	5	5^2	5
$5034E1$	$-2^{15}3^5 839$	5^2	5	5^3	5^2
$5074D1$	$-2^{10}43^5 59$	5^2	5	5^2	5
$*5302I1$	$2^5 11^5 241$	5^3	5	5^3	5
$6782E1$	$2^{30}3391$	5	5	5^2	5^2
$7914F1$	$-2^5 3^{15}1319$	5^2	5	5^2	5
$7998K1$	$-2^{25}3^5 31^3 43^5$	5^4	5	5^4	5
$*13881$	$-3^{10}7^5 661$	5^2	5	5^3	5^2
$*17963$	$-11 \cdot 23^5 71$	5	5	5^3	5^3
$*20042$	$-2^{15}11^5 911$	5^3	5	5^3	5
$*22847$	$11^2 31 \cdot 67^5$	5	5	5^3	5^3
$*42549$	$3^5 13^5 1091$	5^2	5	5^3	5^2
$*44878$	$-2^{10}19^5 1181$	5^2	5	5^3	5^2
$*53718$	$2^{15}3^5 7^5 1279$	5^3	5	5^4	5^2
$*86898$	$-2^{10}3^{10}7^5 2069$	5^3	5	5^4	5^2
$*99803$	$-11 \cdot 43^5 211$	5	5	5^3	5^3
$**3559178$	$-2^5 7^5 37^5 6871$	5^3	5	5^5	5^3
$**12969723$	$-3^5 13^5 19 \cdot 23^5 761$	5^3	5	5^6	5^4

TABLE 1. Positive rank with rational point of order 5.

Conductor	Δ	C	D	deg	#7-Ш?
513110	$-2^{21}5^{7}13^{7}3947$	7^3	7	7^4	7^2
816310	$-2^{28}5^{7}11^{7}41\cdot 181$	7^3	7	7^5	7^3
848370	$-2^{28}3^{14}5^{14}28279$	7^3	7	7^4	7^2

ACKNOWLEDGMENTS

I am grateful to J. Cremona, for making his data public and for double-checking one of the modular parametrisation degrees for me, and to M. Flach for correcting his Lemma 1 in [Flach 93], and for informing me of [Diamond et al. 01a]. I am indebted to M. Watkins for helpful comments and for the spectacular examples of large conductor mentioned in the last section. I thank also the referees for numerous useful comments and substantial corrections. I am especially grateful to one of them for finding a mistake which, in an earlier version of the paper, produced an apparent paradox which I had been unable to resolve.

REFERENCES

[Abbes and Ullmo 96] A. Abbes, S. Ullmo. "À propos de la conjecture de Manin pour les courbes elliptiques modulaires." *Compositio Math.* 103 (1996), 269–286.

[Bloch and Kato 90] S. Bloch and K. Kato. "L-Functions and Tamagawa Numbers of Motives." In *The Grothendieck Festschrift Volume I,* pp. 333–400, Progress in Mathematics 86. Boston, MA: Birkhäuser Boston, 1990.

[Cremona and Mazur 00] J. E. Cremona and B. Mazur. "Visualizing Elements in the Shafarevich-Tate Group." *Experiment. Math.* 9 (2000), 13–28.

[Cremona and Mazur 02] J. E. Cremona and B. Mazur. "Visible Evidence for the Birch and Swinnerton-Dyer Conjecture for Modular Abelian Varieties of Rank Zero." Appendix to A. Agashe and W. Stein. Preprint. Available from World Wide Web: (www.modular.fas.harvard.edu/papers/shacomp), 2002.

[Coates and Schmidt 87] J. Coates and C. G. Schmidt. "Iwasawa Theory for the Symmetric Square of an Elliptic Curve." *J. Reine Angew. Math.* 375/376 (1987), 104–156.

[Diamond et al. 01a] F. Diamond, M. Flach, and L. Guo. "On the Bloch-Kato Conjecture for Adjoint Motives of Modular Forms." *Math. Res. Lett.* 8 (2001), 237–242.

[Diamond et al. 01b] F. Diamond, M. Flach, and L. Guo. "Adjoint Motives of Modular Forms and the Tamagawa Number Conjecture." Preprint. Available from World Wide Web: (www.andromeda.rutgers.edu/~liguo/lgpapers.html), 2001.

[Dummigan 01a] N. Dummigan, "Symmetric Square L-Functions and Shafarevich-Tate Groups." *Experiment. Math.* 10 (2001), 383-400.

[Dummigan 01b] N. Dummigan. "Values of a Hilbert Modular Symmetric Square L-Function." In Preparation.

[Flach 93] M. Flach. "On the Degree of Modular Parametrisations." In *Séminaire de Théorie des Nombres, Paris 1991-92*, edited by S. David, pp. 23–36, Progress in Mathematics 116. Boston, MA: Birkhäuser Boston, 1993.

[Flach 92] M. Flach. "A Finiteness Theorem for the Symmetric Square of an Elliptic Curve." *Invent. Math.* 109 (1992), 307–327.

[Flach 90] M. Flach. "A Generalisation of the Cassels-Tate Pairing." *J. reine angew. Math.* 412 (1990), 113–127.

[Mazur 78] B. Mazur. "Rational Isogenies of Prime Degree." *Invent. Math.* 44 (1978), 129–62.

[Rankin 39] R. A. Rankin. "Contributions to the Theory of Ramanujan's Function $\tau(n)$ and Similar Arithmetical Functions." *Proc. Cambridge Philos. Soc.* 35 (1939), 351–372.

[Shimura 76] G. Shimura. "The Special Values of the Zeta Functions Associated with Cusp Forms." *Comm. Pure Appl. Math.* 29 (1976), 783–804.

[Serre 72] J.-P. Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.* 15 (1972), 259–331.

[Silverman 86] J. H. Silverman. *The Arithmetic of Elliptic Curves,* GTM 106. New York: Springer-Verlag, 1986.

[Silverman 94] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves,* GTM 151. New York: Springer-Verlag, 1994.

[Taylor and Wiles 95] R. Taylor and A. Wiles. "Ring-Theoretic Properties of Certain Hecke Algebras." *Ann. Math.* 141 (1995), 553–572.

[Watkins 02] M. Watkins. "Computing the Modular Degree of an Elliptic Curve." Preprint. Available from World Wide Web: (www.math.psu.edu/watkins/moddeg.ps), 2002

[Wiles 95] A. Wiles. "Modular Elliptic Curves and Fermat's Last Theorem." *Ann. Math.* 141 (1995), 443–551.

Neil Dummigan, University of Sheffield, Department of Pure Mathematics, Hicks Building, Hounsfield Road, Sheffield, S3 7RH, UK (n.p.dummigan@shef.ac.uk)

Received September 27, 2001; accepted in revised form April 2, 2002.