RATIONAL TORSION ON OPTIMAL CURVES

NEIL DUMMIGAN

Abstract. Vatsal has proved recently a result which has consequences for the existence of rational points of odd prime order ℓ on optimal elliptic curves over $\mathbb{Q}$. When the conductor N is square-free, $\ell \nmid N$ and the local root number $w_p = -1$ for at least one prime $p \mid N$, we offer a somewhat different proof, starting from an explicit cuspidal divisor on $X_0(N)$. We also prove some results linking the vanishing of $L(E,1)$ with the divisibility by ℓ of the modular parametrisation degree, fitting well with the Bloch-Kato conjecture for $L(\mathrm{Sym}^2 E, 2)$, and with an earlier construction of elements in Shafarevich-Tate groups. Finally (following Faltings and Jordan) we prove an analogue of the result on ℓ-torsion for cuspidal Hecke eigenforms of level one (and higher weight), thereby strengthening some existing evidence for another case of the Bloch-Kato conjecture.

1. Introduction

Let $E'/\mathbb{Q}$ be an elliptic curve, of conductor N. Let $X_0(N)/\mathbb{Q}$ be the modular curve whose non-cuspidal points classify elliptic curves with cyclic subgroups of order N, and let $J_0(N)$ be its Jacobian. It is known [BCDT], [Fa], [TW], [Wi] that there exists a morphism of finite degree, defined over $\mathbb{Q}$, $\phi' : X_0(N) \to E'$. This uniquely factors (via a fixed Albanese embedding of $X_0(N)$ in $J_0(N)$) through a homomorphism $\pi' : J_0(N) \to E'$. In any isogeny class of elliptic curves over $\mathbb{Q}$, of conductor N, there is a unique E which is maximal in the sense that there is a $\phi : X_0(N) \to E$ (determined up to sign, but we imagine that one has been chosen) with the following property. For any E', ϕ' as above, with E' in the given isogeny class and ϕ' mapping ∞ to O, there exists an isogeny $\theta : E \to E'$ such that $\phi' = \theta\phi$. This maximal elliptic curve is also characterised by the fact that if

Date: December 12th, 2005.

1991 *Mathematics Subject Classification.* 11G05, 14H52.

$\pi : J_0(N) \to E$ is the associated homomorphism then $\ker(\pi)$ is connected. We say that E is 'optimal', or a 'strong Weil curve'.

Let $\Theta : \mathfrak{H}^* \to X_0(N)(\mathbb{C})$ be the canonical map, where $\mathfrak{H}^*$ is the completed upper half plane, containing a fixed choice of $i = \sqrt{-1}$ in $\mathbb{C}$. If ω is a Néron differential on E then $\Theta^*\phi^*(\omega) = c\, f(z)\,(2\pi i)dz$, where $c \in \mathbb{Q}^*$ (conjectured to equal ± 1) is the Manin constant, and $f = \sum_{n=1}^{\infty} a_n q^n$ ($q = e^{2\pi i z}$) is a normalised newform for $\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : N \mid c \right\}$. Let $\mathbb{T}$ be the $\mathbb{Z}$-algebra generated by all the Hecke operators T_n ($n \geq 1$) acting on $S_2(\Gamma_0(N))$, the space of cusp forms of weight 2 for $\Gamma_0(N)$. The newform f is an eigenvector for $\mathbb{T}$, with a_n the eigenvalue for T_n. Let I_f be kernel of the homomorphism from $\mathbb{T}$ to $\mathbb{C}$ such that $T_n \mapsto a_n$. There is a natural action of $\mathbb{T}$ on $J_0(N)$ via Hecke correspondences on $X_0(N)$, defined over $\mathbb{Q}$, and the optimal curve E can be constructed as $J_0(N)/I_f J_0(N)$. The L-function $L_f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$ is the same as the L-function of E defined by the usual Euler product. For Euler factors at primes of good reduction, this follows from the Eichler-Shimura congruence relation which allows us to interpret a_p as a trace of Frobenius, while for Euler factors at primes of bad reduction it follows from work of Deligne-Langlands and Carayol [La], [Ca].

The following is Proposition 5.3 of [V].

Theorem 1.1. (Vatsal) *Let E, of conductor N, be the optimal curve in its isogeny class, and ℓ an odd prime. Suppose that $E[\ell]$ is reducible as a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module, and that E is ordinary at ℓ (i.e. $\ell \nmid a_\ell$). Then*

(1) *$\ell^2 \nmid N$ and*
(2) *there exists an étale isogeny of degree ℓ, defined over $\mathbb{Q}$, from E to some elliptic curve $E''/\mathbb{Q}$.*

Here, "étale" means that the extension to Néron models over $\mathbb{Z}$ is étale. The following is easily extracted from Vatsal's proof of the above (the case that the composition factors of $E[\ell]$ are $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ):

Theorem 1.2. *Let ℓ be a prime number. Let $E'/\mathbb{Q}$ be an elliptic curve of conductor N such that $\ell^2 \nmid N$, and let E be the optimal curve in the isogeny class of E'. If E' has a rational point of order ℓ then so has E.*

Note that the existence, in the isogeny class of E, of an E' with a rational point of odd prime order ℓ, is equivalent to the congruences $a_p \equiv 1 + p \pmod{\ell}$ for all primes $p \nmid N$. (This relies on the interpretation of a_p as a trace of Frobenius.) Also note that if $E'/\mathbb{Q}$ possesses a rational point of prime order ℓ then necessarily $\ell \leq 7$, by Theorem $7'$ of [Mz1].

The reader will easily find numerous examples in Cremona's tables to illustrate Theorem 1.2. In case the wording of Theorem 1.2 causes any confusion, I should point out that E and E' can be the same. In fact, in most examples E has the property of being the only curve in its isogeny class to possess a rational point of order ℓ. What is striking is the absence of other examples (with $\ell^2 \nmid N$) where a non-optimal E' has the same property. The first example in Cremona's tables where $\ell^2 \mid N$ and an optimal curve E of conductor N does not have a rational torsion point of order ℓ, despite some other curve in the same isogeny class having one, is the isogeny class $90C$, with $\ell = 3$.

Consider the case that N is squarefree, and for $d \mid N$ let W_d be the Atkin-Lehner involution [AL]. The newform f is an eigenvector for all the W_d. Let $w_d = \pm 1$ be such that $W_d f = w_d f$, and note that the w_d are multiplicative in d. The Euler factor in $L_f(s)$ at $p \mid N$ is $(1 + w_p p^{-s})^{-1}$, since $T_p f = -W_p f$ for the newform f [AL], so $w_p = -1$ or $+1$ according as the multiplicative reduction at p is split or non-split, respectively. We shall reprove Theorem 1.2 in the case (Theorem 4.1) that $\ell \nmid N$, N is square-free and $w_p = -1$ for at least one prime $p \mid N$, under a weak assumption which has to hold when $\ell = 7$, or when $\ell = 5$ and there is also a prime such that $w_p = 1$. Since E' has a rational point of order ℓ, the composition factors of $E''[\ell]$, for any E'' in the same isogeny class, are $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ, and certainly $E[\ell]$ is reducible. To show that E has a rational point of order ℓ is equivalent to showing that the composition factor $\mathbb{Z}/\ell\mathbb{Z}$ is a submodule of $E[\ell]$. If $\ell = 2$ then $\mathbb{Z}/\ell\mathbb{Z} \simeq \mu_\ell$ and there is nothing more to do, so from now we only consider the case that ℓ is odd.

To prove Theorem 4.1 we use a rational point R of order ℓ on $J_0(N)$, a multiple of the class of a certain divisor supported on the cusps of $X_0(N)$. When N is prime this divisor is just $(0) - (\infty)$. We show that R is contained in the image of E under

the injective map $\hat{\pi} : E \to J_0(N)$, dual to $\pi : J_0(N) \to E$. Note that the injectivity of $\hat{\pi}$ is equivalent to the optimality of E.

Originally I conjectured Theorem 1.2 on the basis of numerical evidence I had found in Cremona's tables, then proved the special case Theorem 4.1. Later I was shown Vatsal's preprint, which pre-dates my interest in this topic. His proof (in the case of composition factors $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ) is similar in that he uses a cuspidal divisor to construct a rational point of order ℓ on $J_0(N)$, then uses a multiplicity-one result to show that it lies in the image of E. (He attributes this kind of idea to Tang [T].) He proves the existence of the cuspidal divisor with the necessary properties in quite an indirect way. He uses his main Theorem 1.1 to avoid an assumption like the "$\ell \mid n$" in our Theorem 4.1. Assuming for a contradiction that E does not have a rational point of order ℓ, he constructs an Eisenstein series (of weight two for $\Gamma_0(N)$) which is congruent $\pmod{\ell}$ to f, so in particular has all the constant terms at the cusps divisible by ℓ. Following Stevens he attaches a cuspidal subgroup (of $J_0(N)$) to this Eisenstein series. Then, using a theorem of Washington, he proves that the ℓ-part is non-trivial. His ingenious proof has the advantage of applying in full generality. The proof of Theorem 4.1 that we present here constructs the cuspidal divisor in a more elementary and explicit manner, but only in a restricted case. However, our construction enables us to make an application to Theorem 6.2 (see the next paragraph). Comparing the two proofs, note that we use eta products to construct functions with zero orders divisible by ℓ, that the logarithmic derivative of the Dedekind eta function is formally an Eisenstein series of weight two, and that logarithmic differentiation (with respect to z) turns zero orders at cusps into constant terms.

In [Du2] we observed some numerical data which support the ℓ-part of the Bloch-Kato conjecture for the special value $L(\mathrm{Sym}^2 E, 2)$ of the symmetric square L-function attached to E. In particular, for many examples where $\mathrm{rank}(E(\mathbb{Q})) > 0$ and E is optimal with a rational point of order $\ell = 5$ or 7, we observed that $\ell \mid \deg(\phi)$. In §6 of the present paper, we prove, without assuming the Bloch-Kato conjecture, that under fairly general conditions this phenomenon must occur. First we prove the fairly weak Theorem 6.2, using the fact that cusps occur in both the

integral evaluating $L(E,1)$ and the divisor used to construct rational points of order ℓ. When $L(E,1)=0$, the map $\pi : J_0(N) \to E$ kills $[(0)-(\infty)]$.

Then, independent of the earlier construction of rational points of order ℓ, we prove the following.

Theorem 1.3. *Let $E/\mathbb{Q}$ be an optimal elliptic curve of conductor N. Suppose that E has a rational point of prime order $\ell = 5$ or 7. Suppose also that E has a prime p of split multiplicative reduction such that $p \not\equiv 1 \pmod{\ell}$. If $L(E,1) = 0$ then $\ell \mid \deg(\phi)$.*

In §§7 and 8 we shall consider newforms of level one and higher weight. In several cases examination of the critical value $L_f(1)$ (divided by a canonical period) shows an Eisenstein prime ℓ in the denominator. It can be explained by a global torsion factor in the conjectural Bloch-Kato formula. The existence of this global torsion is proved in §7, following Faltings and Jordan [FJ]. Its expected existence, and the search for an elliptic curve analogue, was the motivation for the examination of Cremona's tables which led me to conjecture Theorem 1.2. The kind of argument used in the proofs of Lemma 7.4 and Theorem 7.3 could quite easily be modified to provide an alternative conclusion to Vatsal's proof of Theorem 1.1 in the case $\ell \nmid N$, substituting his Eisenstein series (mentioned above) for G_k.

I am grateful to N. Bruin for raising the question of whether things work the same for $X_1(N)$-optimal curves, to J. Manoharmayum for the observation mentioned in §2, and to M. Watkins for various examples and observations on $X_1(N)$-optimal curves, and for making known to me Vatsal's preprint. I thank also a referee for extensive comments on an earlier version of this paper.

2. The case of prime conductor

The linear equivalence class of the divisor $(0)-(\infty)$ on $X_0(N)$ is a rational point on the abelian variety $J_0(N)$. According to the Manin-Drinfeld theorem it is a point of finite order. The exact order n, for general N, has been determined by Ligozat [Li]. In the case that N is prime, it is the numerator of $\frac{N-1}{12}$, as originally proved by Ogg.

Proposition 2.1. *Theorem 1.2 is true when N is prime.*

Proof. We may assume that ℓ is odd. Let $\mathcal{I}$ be the Eisenstein ideal of $\mathbb{T}$, generated by $T_p - (1+p)$ (for primes $p \neq N$) and by $W_N + 1 = -(T_N - 1)$. Let E be the optimal curve. Recall that its optimality is equivalent to the injectivity of the map $\hat{\pi} : E \to J_0(N)$ dual to $\pi : J_0(N) \to E$. The image of $E[\ell]$ under the injective map $\hat{\pi} : E \to J_0(N)$ is killed by $\mathcal{I}$, since $a_p \equiv 1 + p \pmod{\ell}$ for all primes $p \neq N$, and $w_N = -1$ in all cases (listed below). By 9.7 of [Mz1], $\ell \mid n$, the order of $[(0) - (\infty)]$ in $J_0(N)$.

Corollary 16.4 of [Mz1] states now that $J_0(N)[\ell, \mathcal{I}] \simeq (\mathbb{Z}/\ell\mathbb{Z}) \oplus \mu_\ell$, The two factors $\mathbb{Z}/\ell\mathbb{Z}$ and μ_ℓ are the cuspidal subgroup and the Shimura subgroup respectively. Since $\hat{\pi}(E[\ell])$ is 2-dimensional over $\mathbb{F}_\ell$, it must coincide with $J_0(N)[\ell, \mathcal{I}] \simeq (\mathbb{Z}/\ell\mathbb{Z}) \oplus \mu_\ell$. The $\mathbb{Z}/\ell\mathbb{Z}$ factor shows the existence of a rational point of order ℓ on the optimal curve E. □

I am grateful to J. Manoharmayum for pointing out the utility of Mazur's Corollary 16.4.

The only elliptic curves over $\mathbb{Q}$, of prime conductor and possessing a rational point of odd prime order ℓ are $11A1$, $11A3$ ($\ell = 5$), $19A1$, $19A3$ ($\ell = 3$) and $37B1$, $37B3$ ($\ell = 3$) [Mi], [Se], so one could prove Proposition 2.1 by just checking cases. In all cases $\ell = n$. Incidentally, the minimal discriminants of $11A1$, $19A1$ and $37B1$ are -11^5, -19^3 and 37^3 respectively, so in each case $E[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z}) \oplus \mu_\ell$ also follows from Proposition 4.2 below.

3. A certain cuspidal divisor

Suppose that N is square-free. In this section we generalise parts of §4 of [Og] (there $N = pq$). The construction also owes something to §3.2 of [BS], in the general case $G > 1$ (see below). Both [Og] and [BS] cite [Ne].

The cusps of $X_0(N)$ are all defined over $\mathbb{Q}$, and they are in one-to-one correspondence with the positive divisors of N, as follows. The divisor d corresponds to a point P_d which, as an orbit for the action of $\Gamma_0(N)$ on $\mathbb{P}^1(\mathbb{Q})$, contains all $\frac{a}{d}$ with $(a, d) = 1$. The orbit P_1 contains 0 and P_N contains ∞.

Lemma 3.1. *Recall that N is square-free. Let d be a positive divisor of N and p a prime number. Let T_p be the Hecke operator, acting on divisors on $X_0(N)$ via a*

Hecke correspondence. For $\delta \mid N$, let W_δ be the Atkin-Lehner involution, acting on $X_0(N)$.

(1) *If $p \nmid N$ then $T_p((P_d)) = (p+1)(P_d)$.*
(2) *If $p \mid N$ and $p \nmid d$ then*
$T_p((P_d)) = (P_d) + (p-1)(P_{pd})$ *and*
$T_p((P_{pd})) = p\,(P_{pd})$.
(3) *$W_\delta(P_d) = P_{d'}$, where $d' = d\delta/(d,\delta)^2$.*

These operators can be given modular interpretations which extend to the cusps via generalised elliptic curves. However, the lemma can be proved most easily using explicit formulas for the operators on the level of the completed upper half plane. For example, when $p \mid N$, $T_p((z)) = \sum_{j=0}^{p-1} \left(\frac{z+j}{p}\right)$. The details are omitted.

Given $E/\mathbb{Q}$ of level N, let f be the associated newform for $\Gamma_0(N)$, and for each positive $d \mid N$ let $w_d = \pm 1$ be such that $W_d f = w_d f$. Let G be the product of those primes such that $w_p = 1$. Note that, for any $\delta \mid (N/G)$, $w_{\delta G} = w_\delta$, since the W_d are multiplicative in d. Now define a divisor supported on the cusps of $X_0(N)$:

$$Q := \sum_{\delta \mid (N/G)} w_\delta (P_{\delta G}) = \left(\sum_{\delta \mid (N/G)} w_\delta W_\delta \right) (P_G). \tag{1}$$

By multiplicativity, the degree of this divisor is $\prod_{p \mid (N/G)} (1 + w_p)$ (where p always denotes a prime number), so as long as at least one w_p is equal to -1 we have a divisor of degree zero. Suppose from now on that this condition does hold.

Let $\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1-q^n)$ be Dedekind's eta function, and $\Delta = \eta^{24}$. Also, for $d \mid N$ let $\eta_d(z) = \eta(dz)$ and $\Delta_d(z) = \Delta(dz) = \eta_d(z)^{24}$. Define

$$r := \prod_{p \mid G} (p^2 - 1) \prod_{p \mid (N/G)} (p-1), \quad h := (r, 24),$$

and

$$F = \left(\prod_{g \mid G} \prod_{d \mid (N/G)} \eta_{dg}^{w_d \, \mu(g) g} \right)^{24/h},$$

where μ is the Möbius function.

Proposition 3.2. *Suppose that $w_p = -1$ for at least one prime $p \mid N$.*

(1) *F is a function on $X_0(N)(\mathbb{C})$, except for possibly when $w_p = -1$ for only one p, in which case F^2 is a function on $X_0(N)(\mathbb{C})$.*

(2) $\mathrm{div}(F^2) = (-1)^t w_N(2n)Q$, *where* $n := r/h$ *and* t *is the number of prime divisors of* N.

(3) (a) *For no* $m > 1$ *is* $F^{1/m}$ *a function on* $X_0(N)(\mathbb{C})$.

(b) *For no odd* $m > 1$ *is* $F^{2/m}$ *a function on* $X_0(N)(\mathbb{C})$.

Proof. (1) According to Proposition 3.2.1 of [Li] we need to check the following four conditions:

(a) $\sum_{g|G}\sum_{d|(N/G)}((24/h)w_d\mu(g)g)(N/(dg)) \equiv 0 \pmod{24}$;

(b) $\sum_{g|G}\sum_{d|(N/G)}((24/h)w_d\mu(g)g)(dg) \equiv 0 \pmod{24}$;

(c) $\sum_{g|G}\sum_{d|(N/G)}((24/h)w_d\mu(g)g) \equiv 0 \pmod{24}$;

(d) $\prod_{g|G}\prod_{d|(N/G)}(N/(dg))^{(24/h)w_d\mu(g)g} \in \mathbb{Q}^2$, except for possibly when $w_p = -1$ for only one p, in which case of course $\prod_{g|G}\prod_{d|(N/G)}(N/(dg))^{(48/h)w_d\mu(g)g} \in \mathbb{Q}^2$.

The first three are rather easy to check. For the fourth, consider the exponent, in the rational number defined by the first double product, of each prime $q \mid N$. If $q \mid G$ then this exponent is zero, since it is a multiple of $\sum_{d|(N/G)} w_d$, which is zero because some $w_p = -1$. Likewise if $q \mid (N/G)$ then the exponent of q is zero as long as $w_p = -1$ for some prime p *different from* q.

The above conditions guarantee that F (or F^2) is a holomorphic function on $\mathfrak{H}^*$, invariant under $\Gamma_0(N)$, and may consequently be viewed as an algebraic function on the curve $X_0(N)(\mathbb{C})$. In fact, it follows from the q-expansion principle that it is a function defined over $\mathbb{Q}$ on the curve $X_0(N)/\mathbb{Q}$, but we shall not need this fact.

(2) Fix a positive divisor D of N and write $D = \delta G'$, where $G' = (D, G)$ and $\delta = (D, N/G)$. According to Proposition 3.2.8 of [Li], if $dg \mid N$ then Δ_{dg} has zeros only at cusps, and at the cusp P_D the order of the zero is $ND'^2/(dgD)$, where $D' = (dg, D)$. Precisely, I mean that if we choose some $r \in \mathbb{P}^1(\mathbb{Q})$, belonging to the orbit P_D for the action of $\Gamma_0(N)$ on $\mathbb{P}^1(\mathbb{Q})$, and choose $s \in \mathrm{SL}_2(\mathbb{Z})$ such that $s(\infty) = r$, then this is the order of $\Delta_{dg}|s$ at ∞, for the usual uniformising parameter $q = e^{2\pi i z}$. The correctness of this particular formula depends on our assumption that N is square-free.

It follows that the multiplicity of P_D in $\mathrm{div}(F^2)$ (where F^2 is considered as a function on $X_0(N)(\mathbb{C})$) is

$$\mathrm{ord}_{P_D}(F^2) = \frac{2}{h}\sum_{g|G}\sum_{d|(N/G)} w_d\,\mu(g)\frac{N(d,\delta)^2(g,G')^2}{dD}$$

$$= \frac{2N}{hD}\sum_{g|G'}\mu(g)g^2\sum_{h|(G/G')}\mu(h)\sum_{d|(N/G)} w_d\frac{(d,\delta)^2}{d}.$$

The middle sum is zero unless $G' = G$, so we suppose now that $G' = G$, so that $D = \delta G$. Then

$$\mathrm{ord}_{P_D}(F^2) = \left((-1)^s\prod_{p|G}(p^2-1)\right)\frac{2N}{hD}\sum_{d|(N/G)} w_d\frac{(d,\delta)^2}{d}$$

$$= \left((-1)^s\prod_{p|G}(p^2-1)\right)\frac{2N}{hD}\sum_{d|\delta} w_d d\sum_{e|(N/(G\delta))}\frac{w_e}{e},$$

where s is the number of prime divisors of G. Finally, substituting $(N/(G\delta e))$ for e, and recalling that $D = \delta G$, we find

$$\mathrm{ord}_{P_D}(F^2) = \frac{2}{h}(-1)^s w_{N/D}\prod_{p|G}(p^2-1)\sum_{d|\delta} w_d d\sum_{e|(N/(G\delta))} w_e e$$

$$= \frac{2}{h}(-1)^s w_{N/D}\prod_{p|G}(p^2-1)\sum_{d|(N/G)} w_d d$$

$$= \frac{2}{h}(-1)^t w_{N/D}\prod_{p|G}(p^2-1)\prod_{p|(N/G)}(p-1),$$

where t is the number of prime divisors of N, and the final equality comes from the definition of G.

Since P_D appears in the divisor Q with sign w_D, we conclude that $\mathrm{div}(F^2) = (-1)^t w_N(2n)Q$.

(3) We prove (a), the proof of (b) being very similar. If, for some $m > 1$, $F^{1/m}$ were a function on $X_0(N)(\mathbb{C})$ then its divisor would be $\pm\frac{n}{m}Q$ so it would have to be the case that $m \mid n$. But $n = r/h$ where $h = (r, 24)$, so if $m > 1$ and $m \mid n$ then $24/(hm) \notin \mathbb{Z}$. Now we simply imitate the proof of Theorem 4 of [Og]. Recalling the definitions of F and of η, we see that

(for some choice of m^{th}-root) $F^{1/m} = \prod_{n=1}^{\infty}(1-q^n)^{\beta(n)\alpha}$ where $q = e^{2\pi iz}$, $\alpha = 24/(hm) \in \mathbb{Q} - \mathbb{Z}$ and

$$\beta(n) = \sum_{g|(n,G)} \mu(g)g \sum_{d|(n,N/G)} w_d.$$

Thus $F^{1/m}$ is of the form

$$(1-q^{n_1})^{\alpha}(1-q^{n_2})^{\pm\alpha}(1-q^{n_3})^{\pm\alpha},$$

where $1 = n_1 < n_2 \leq n_3 \leq \dots$. Expanding F as a product of binomial series, the coefficient of q^m is

$$\pm\binom{\alpha}{m} + \sum \pm \binom{\pm\alpha}{m_1} \cdots \binom{\pm\alpha}{m_r},$$

where the summation is over $m = n_1m_1 + \cdots + n_rm_r$, with $r > 1$ and all $m_i \geq 1$. Since $n_1 < n_2$ we have $m > m_1 + \cdots m_r$, so if we choose a prime l dividing the denominator of α then the $\binom{\alpha}{m}$ term dominates l-adically, and the l-adic absolute value tends to ∞ as $m \to \infty$. This contradicts the boundedness of the denominators of the Fourier coefficients of a modular form, as in the proof of Theorem 4 of [Og].

□

Corollary 3.3. *Suppose that $w_p = -1$ for at least one prime $p \mid N$. The exact order of the rational point $[Q]$ in the Jacobian $J_0(N)$ is either n or $2n$, where $n = r/h = \text{Num}\left(\frac{1}{24}\prod_{p|G}(p^2-1)\prod_{p|(N/G)}(p-1)\right)$.*

4. The case of square-free conductor, some $w_p = -1$

Theorem 4.1. *Let $E/\mathbb{Q}$ be an optimal elliptic curve of square-free conductor N. Let f be the associated newform, and for $d \mid N$ let $w_d = \pm 1$ be such that $W_d f = w_d f$. Suppose that $w_p = -1$ for at least one prime $p \mid N$. Let $\ell \nmid N$ be an odd prime such that some E', isogenous over $\mathbb{Q}$ to E, has a rational point of order ℓ. If $\ell \mid n$ (with n as in Corollary 3.3) then E has a rational point of order ℓ.*

Proof. Since $w_p = -1$ for some $p \mid N$, we may construct $[Q] \in J_0(N)(\mathbb{Q})$, of finite order n or $2n$ by Corollary 3.3. Since $\ell \mid n$, there is some multiple R of $[Q]$ having exact order ℓ. Let $\mathcal{I}$ be the ideal of $\mathbb{T}$ generated by $T_p - (1+p)$ for $p \nmid N$ and $T_p + w_p$ for $p \mid N$, and let $\mathfrak{m}$ be the maximal ideal of $\mathbb{T}$ generated by $\mathcal{I}$ and ℓ. Then

$\mathfrak{m}$ kills the image in $J_0(N)[\ell]$, under the injection $\hat{\pi} : E \to J_0(N)$, of $E[\ell]$. This follows from the facts that $a_p \equiv 1 + p \pmod{\ell}$ for $p \nmid N$ (because E' has a rational point of order ℓ), and that for $p \mid N$, $T_p f = -W_p f$ for the newform f [AL]. We show now that $\mathfrak{m}$ kills R.

First consider any prime $p \nmid N$. If $d \mid N$ then, by Lemma 3.1(1), $T_p((P_d)) = (p+1)(P_d)$. It follows that $T_p - (p+1)$ kills the divisor Q, so certainly kills the multiple R of its class $[Q]$.

Now consider any prime $p \mid N$. If $w_p = -1$ then $p \mid (N/G)$, and Q is a linear combination of terms of the form $(P_d) - (P_{pd})$, for certain $d \mid N$ with $p \nmid d$ (see (1)). But by Lemma 3.1(2),

$$T_p((P_d) - (P_{pd})) = ((P_d) + (p-1)(P_d)) - p(P_d) = -w_p((P_d) - (P_{pd})),$$

so $T_p + w_p$ kills Q, and hence kills R. Finally, if $w_p = 1$ then p is a prime of non-split multiplicative reduction (for E and for E'), and consideration of a Tate model shows that the existence of the rational point of order ℓ on E' forces $\ell \mid (p+1)$. Now $p \mid G$ so the divisor Q is a linear combination of P_{pd} for certain $d \mid N$ with $p \nmid d$. By Lemma 3.1(2), $T_p((P_{pd})) = p(P_{pd}) \equiv -(P_{pd}) \pmod{\ell}$, so although $T_p + w_p$ does not necessarily kill $[Q]$, it does kill the multiple R of order ℓ.

Let $\mathcal{J}_0(N)/\mathbb{Z}_\ell$ and $\mathcal{E}/\mathbb{Z}_\ell$ be the Néron models of $J_0(N)/\mathbb{Q}_\ell$ and $E/\mathbb{Q}_\ell$ respectively.

We have both $R \in J_0(N)[\mathfrak{m}]$ and $\hat{\pi}(E[\ell]) \subset J_0(N)[\mathfrak{m}]$. Suppose, for the purpose of obtaining a contradiction, that $R \notin \hat{\pi}(E[\ell])$. R generates the constant group-scheme $(\mathbb{Z}/\ell\mathbb{Z})/\mathbb{Q}_\ell$. The finite flat ℓ-torsion group-scheme $\mathcal{G} := ((\mathbb{Z}/\ell\mathbb{Z}) \times \mathcal{E}[\ell])/\mathbb{Z}_\ell$ embeds in $\mathcal{J}_0(N)[\mathfrak{m}]$. To deduce this from $\ell - 1 > 1$ and the embedding of generic fibres is a straightforward consequence of Corollaire 3.3.6(i) of [Ra], since $\mathcal{J}_0(N)[\mathfrak{m}]$ is finite flat ($\ell \nmid N$).

The elliptic curve E has good, ordinary reduction at ℓ (in fact $a_\ell \equiv 1 \pmod{\ell}$), so $\dim_{\mathbb{F}_\ell}(\mathcal{G}(\overline{\mathbb{F}}_\ell)[\mathfrak{m}]) = 2$, hence $\dim_{\mathbb{F}_\ell}(\mathcal{J}_0(N)(\overline{\mathbb{F}}_\ell)[\mathfrak{m}]) \geq 2$. Any element of this group is represented by some divisor D of degree zero on $X_0(N)/\overline{\mathbb{F}}_\ell$ such that $\ell D = \mathrm{div}(f)$ for some function f on $X_0(N)/\overline{\mathbb{F}}_\ell$. The map $[D] \mapsto df/f$ gives a well-defined injection from $\mathcal{J}_0(N)(\overline{\mathbb{F}}_\ell)[\mathfrak{m}]$ to $H^0(X_0(N)/\overline{\mathbb{F}}_\ell, \Omega^1)[\mathfrak{m}]$, whose dimension is at most one, by the q-expansion principle. (This kind of argument was originally

used in 14.8 of [Mz1].) This contradiction shows that E has a rational point of order ℓ (identified with R on $\hat{\pi}(E)$). □

To investigate the condition $\ell \mid n$, we collect some results on elliptic curves of square-free conductor for which the minimal discriminant Δ is an ℓ^{th} power. Note that by the Corollary to Proposition 1 of [MO], if Δ is an ℓ^{th} power then necessarily $\ell \leq 7$.

Proposition 4.2. *Let $E'/\mathbb{Q}$ be an elliptic curve of square-free conductor N and minimal discriminant Δ. Suppose that ℓ is an odd prime and that Δ is an ℓ^{th} power. Then $E'[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z}) \oplus \mu_\ell$ as a module for* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Proof. We follow the proof of Proposition 3 of [MO]. Consideration of a Tate model shows that if $\ell \mid r_i$ (where $\Delta = \pm\prod_i p_i^{r_i}$) then $E'[\ell]$ is unramified at p_i (unless $p_i = \ell$). Therefore if ℓ divides all the r_i then $E'[\ell]$ is unramified at all $p \neq \ell$. The proposition then follows from Théorème B of [Fo]. □

Mestre and Oesterlé also show (Proposition 3 of [MO]) that if Δ is a square then $E'[2] \simeq (\mathbb{Z}/2\mathbb{Z}) \oplus \mu_2$.

Proposition 4.3. *Let $E'/\mathbb{Q}$ be an elliptic curve of square-free conductor N. It is not possible that $E'[7] \simeq (\mathbb{Z}/7\mathbb{Z}) \oplus \mu_7$ as a* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-module. (Hence it is not possible that Δ is a 7^{th} power.)*

This is proved during the proof of Proposition 3 of [MO]. They observe that if $F = E'/(\mathbb{Z}/7\mathbb{Z})$ and $F' = E'/\mu_7$ then there would exist a cyclic, rational isogeny of degree 49 between F and F', contradicting the non-existence of rational points on $Y_0(49)$ (which is proved in 5.1 of [Li]).

The condition $\ell \mid n$ in Theorem 4.1 is very weak. Let $\Delta = \prod p_i^{r_i}$ be the minimal discriminant of E'. The reduction of E' at p_i is multiplicative, split if $w_{p_i} = -1$, non-split if $w_{p_i} = 1$. Consideration of a Tate model shows that the existence of a rational point of order ℓ forces $\ell \mid (p_i + 1)$ (in the non-split case) and either $\ell \mid (p_i - 1)$ or $\ell \mid r_i$ (in the split case). Hence $\ell \mid n$ except possibly if $\ell = 3$, or if all $w_p = -1$ and Δ is an ℓ^{th} power. Proposition 4.2 shows that the latter forces $E'[\ell] \simeq (\mathbb{Z}/\ell\mathbb{Z}) \oplus \mu_\ell$, which by Proposition 4.3 is impossible when $\ell = 7$. If $\ell = 5$ but there exists a prime $p \mid N$ such that $w_p = 1$ then ℓ must divide n.

5. $X_1(N)$-optimal curves

Let $X_1(N)/\mathbb{Q}$ be the modular curve whose non-cuspidal points classify elliptic curves with points of order N, and let $J_1(N)$ be its Jacobian. There is a natural map $\theta : X_1(N) \to X_0(N)$, of degree $\phi(N)/2$ (for $N > 2$), and a pullback homomorphism $\theta^* : J_0(N) \to J_1(N)$, both defined over $\mathbb{Q}$. In any isogeny class of elliptic curves over $\mathbb{Q}$ of conductor N, one may construct an "$X_1(N)$-optimal" curve E_1. There is a morphism $\phi_1 : X_1(N) \to E_1$, of minimal degree for the isogeny class, a homomorphism $\pi_1 : J_1(N) \to E_1$ with connected kernel, and an injection $\hat{\pi_1} : E_1 \to J_1(N)$.

What we have seen for $X_0(N)$-optimal curves works just as well for $X_1(N)$-optimal curves. In particular, there is a version of Theorem 4.1 where E is replaced by the $X_1(N)$-optimal curve E_1 in the isogeny class. In the proof, the rational point R of order ℓ on $J_0(N)$ is simply pulled back to $J_1(N)$ via θ^*. There are two ways to show that θ^* does not kill Q. One can note that in Proposition 3.2, we can use exactly the same function F on the upper half plane, and the proof of Proposition 3.2 (3) goes through exactly the same. Alternatively, one can use the fact that the kernel of θ^* (the "Shimura subgroup") is of "multiplicative type" (see [LO]). When showing that this point on $J_1(N)$ lies in the image of E_1, we just have to include the diamond operators $\langle d \rangle$ (for $d \in (\mathbb{Z}/N\mathbb{Z})^\times$) in the generators of $\mathbb{T}$, and the $\langle d \rangle - 1$ in the generators of the maximal ideal $\mathfrak{m}$. Similarly, pulling back to $J_1(N)$ the point used by Vatsal, one obtains a proof of a version of Theorem 1.2 where E_1 is substituted for E.

Stevens proved that in every isogeny class of elliptic curves over $\mathbb{Q}$ there exists a unique curve $E_{\min}$ whose lattice of periods (for a Néron differential) is minimal for the isogeny class. According to Theorem 2.3(b) of [Ste], from it to every other curve in the isogeny class there is an étale isogeny. From this follows the existence of (non-trivial) rational ℓ-torsion on $E_{\min}$ (if it exists somewhere in the isogeny class). Stevens conjectured that this $E_{\min}$ and the $X_1(N)$-optimal curve E_1 are one and the same thing. Vatsal proves his Proposition 5.3 in order to apply it to the proof of his Theorem 1.11 on Stevens' conjecture. This theorem states that if $\ell \geq 7$ and $E/\mathbb{Q}$, ordinary at ℓ, is such that $E[\ell]$ is reducible, then Stevens' conjecture is true for the isogeny class of E.

Actually, it seems to be the case that for most isogeny classes of conductors less than any given large bound, the $X_0(N)$-optimal and $X_1(N)$-optimal curves are the same. However, there are examples where they differ. For example, in the isogeny class $11A$, the curve $11A3$ is $X_1(11)$. It does have a rational point of order 5. Stein and Watkins have made a precise conjecture, based on many numerical examples, about when E_1 is not $X_0(N)$-optimal. This is in §4 of [SW]. The example $11A$ is the only one where E and E_1 are related by a 5-isogeny. In all their other examples, it is either a 2-isogeny or a 3-isogeny, and most of them form subsets of parametrised families.

6. Divisibility of the modular degree

Let $E/\mathbb{Q}$ be an elliptic curve, optimal in its isogeny class. Recall that $\phi : X_0(N) \to E$ is a modular parametrisation of minimal degree. If E has a rational point of order ℓ, the preceding sections provide (under certain conditions) an explicit construction of such a point, using a cuspidal divisor on $J_0(N)$. This construction is used in the proof of Theorem 6.2 below. The motivation for Theorems 6.2 and 1.3 comes from the ℓ-part of the Bloch-Kato conjecture applied to the special value $L(\mathrm{Sym}^2 E, 2)$ of the symmetric square L-function attached to E. Note that, since $E[\ell]$ is reducible, the main theorem of [DFG] does not apply to our situation. The following Lemma is an easy consequence of Lemmas 3.1, 4.3, 4.4 and Theorem 5.1 of [Du2], combined with the formula (10) of [Fl] (which is reproduced as (3-1) of [Du2]). (Please note that in the case of non-split multiplicative reduction, E in Lemma 3.1 of [Du2] should be replaced by a quadratic twist with split multiplicative reduction.) The prime conductor curves listed in §2 above all have rank zero so can be ignored.

Lemma 6.1. *Let E be an optimal elliptic curve of square-free conductor N, with a rational point of prime order $\ell > 3$, with $\ell \nmid N$. Suppose that Δ is not an ℓ^{th} power, but that there exists a prime p of split multiplicative reduction such that $\ell \nmid (p-1)$ and $\ell^2 \nmid \mathrm{ord}_p(\Delta)$. Suppose also that for any prime q of bad reduction, $E[\ell^\infty](\mathbb{Q}_q)$ has order ℓ. Then the Bloch-Kato conjecture predicts that if $R := \mathrm{rank}(E(\mathbb{Q}))$ then $\ell^R \mid \deg(\phi)$.*

The point is, multiplication by the rational point of order ℓ induces a map from $H^1(\mathbb{Q}, E[\ell])$ to $H^1(\mathbb{Q}, \mathrm{Sym}^2 E[\ell])$. Under the above conditions, this allows us to use the descent map to construct, from $E(\mathbb{Q})$, a subgroup of order ℓ^r in a generalised Shafarevich-Tate group. (Note that the finiteness of the ℓ-part of the relevant Selmer group is proved in [LS].) The order of this group appears on one side of the Bloch-Kato formula, with $\deg(\phi)$ on the other, among various other factors that can be controlled.

If $\mathrm{rank}(E(\mathbb{Q})) > 0$ then $L(E,1) = 0$, by Kolyvagin's theorem, and according to the conjecture of Birch and Swinnerton-Dyer $\mathrm{rank}(E(\mathbb{Q})) > 0$ is equivalent to $L(E,1) = 0$. This, combined with the above lemma, motivates Theorems 6.2 and 1.3.

It seems appropriate to mention that Watkins has made some interesting numerical observations on powers of 2 dividing $\deg(\phi)$. In 4.2 of [Wa], he conjectures (for any elliptic curve $E/\mathbb{Q}$) that if $R := \mathrm{rank}(E(\mathbb{Q}))$ then $2^R \mid \deg(\phi)$.

Let E be an optimal curve of conductor N, with $\phi : X_0(N) \to E$ of minimal degree. The homology $H_1(X_0(N)(\mathbb{C}), \mathbb{Q})$ has an action of complex conjugation, compatible with $z \mapsto -\overline{z}$ on $\mathfrak{H}$. The image $\mathbf{e}$ of the imaginary axis $[0, i\infty]$ represents a class in the eigenspace $H_1(X_0(N)(\mathbb{C}), \mathbb{Q})^+$, and $\phi_*([\mathbf{e}]) \in H_1(E(\mathbb{C}), \mathbb{Q})^+$, which is one-dimensional. Either $\phi_*([\mathbf{e}]) = 0$ or there is a unique positive rational r such that $r^{-1}\phi_*(\mathbf{e})$ is a generator for $H_1(E(\mathbb{C}), \mathbb{Z})^+$. In the latter case the order of the rational point $\pi([(0) - (\infty)])$ on E is just the denominator of r. If $\phi_*([\mathbf{e}]) = 0$ then $\pi([(0) - (\infty)]) = O$.

Let $f = \sum_{n=1}^{\infty} a_n q^n$ be the newform attached to E. The L-function $L(E,s) = L_f(s)$ is defined, for $\Re(s) > 3/2$, by the Dirichlet series $L_f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, but has an analytic continuation to the whole of $\mathbb{C}$, by means of the formula

$$(2\pi)^{-s}\Gamma(s)L_f(s) = \int_0^{i\infty} (-iz)^s f(z)\frac{dz}{z}.$$

Hence

$$L_f(1) = -\int_0^{i\infty} f(z)\,(2\pi i)dz = -\int_{\mathbf{e}} c^{-1}\phi^*\omega$$

$$= -c^{-1}\int_{\phi_*(\mathbf{e})} \omega = \frac{r}{c}\,\Omega.$$

Here, c is Manin's constant, ω is a Néron differential on E (with the sign chosen to make c positive) and Ω is the real period of E. We have

$$\frac{r}{c} = L_f(1)/\Omega.$$

Notice that if $L_f(1)/\Omega \neq 0$ and ℓ is a prime (even or odd) dividing the denominator of this rational number, then according to the conjecture of Birch and Swinnerton-Dyer, E has a rational point of order ℓ. If $\ell^2 \nmid N$ then $\mathrm{ord}_\ell(c) = 0$, by Corollary 4.2 of [Mz2], and its refinement [AU]. In this case ℓ divides the denominator of r (i.e. the order of $\pi([(0) - (\infty)])$), hence some multiple of $\pi([(0) - (\infty)])$ provides the predicted rational point of order ℓ on E.

Theorem 6.2. *Let $E/\mathbb{Q}$ be an optimal curve of square-free conductor N, with a rational point of odd prime order $\ell \mid n$, where n is as in Corollary 3.3. Suppose that $\ell \nmid N$, $w_N = -1$ and that $w_p = -1$ for all primes $p \mid N$. If $L(E,1) = 0$ then $\ell \mid \deg(\phi)$.*

Proof. Since all $w_p = -1$, $Q = \sum_{d|N} w_d(P_d)$ (see (1)). Now $\sum_{d|N} w_d W_d((P_1) - (P_N)) = \sum_{d|N} w_d(P_d) - \sum_{d|N} w_d(P_{N/d}) = 2Q$, since $w_d w_{N/d} = w_N = -1$. Since $L_f(1) = 0$, $\int_{\mathbf{e}} f(z)\,dz = 0$. Recall that $\mathbf{e}$ goes from P_1 to P_N. Moreover, for any $d \mid N$,

$$0 = \int_{\mathbf{e}} w_d f(z)\,dz = \int_{W_d(\mathbf{e})} f(z)\,dz.$$

Multiplying by w_d and summing over $d \mid N$, we see that $\int_{\mathcal{P}} \omega = 0$, where $\mathcal{P}$, the image of $\sum_{d|N} w_d W_d(\mathbf{e})$, is a certain 1-cycle on $E(\mathbb{C})$ whose oriented boundary is the divisor $2\phi_* Q$. Hence $2\,\pi([Q]) = O$.

In the proof of Theorem 4.1 we saw that there is a rational point R on E, of order ℓ, such that $\hat{\pi}(R)$ is a multiple of $[Q]$ in $J_0(N)$. Hence $\pi \cdot \hat{\pi}(R) = O$ (recall that ℓ is odd), so ℓ divides the degree of the endomorphism $\pi \cdot \hat{\pi}$ of E, but this endomorphism is just multiplication by $\deg(\phi)$ (it is $\phi_*\phi^*$ on divisor classes), hence $\ell \mid \deg(\phi)$. □

The sign in the functional equation of $L(E,s)$ is $-w_N$, so the above theorem only covers (part of) the case that the vanishing at $s = 1$ is to even order. There are several illustrative examples in the table in §6.4 of [Du2]. Theorem 1.3 is more

widely applicable, in fact the set of examples in §6.4 of [Du2] to which it applies includes as a subset those to which Theorem 6.2 applies.

Proof. of Theorem 1.3. Let $R \in E(\mathbb{Q})$ be a point of order ℓ. Since $\ell \nmid p-1$, the extension of R to the Néron model $\mathcal{E}/\mathbb{Z}_p$ intersects the special fibre on a non-trivial element $c(R)$ of order ℓ in the group of components. (If not, it would have to intersect the special fibre in the identity, but then $R \in E(\mathbb{Q}_p)$ would have to be the image of a 1-unit via the Tate parametrisation $\mathbb{Q}_p^\times/q^{\mathbb{Z}} \simeq E(\mathbb{Q}_p)$, and there is no non-trivial ℓ-torsion in the 1-units of $\mathbb{Q}_p$.) This $c(R)$ maps to the group of connected components of the Néron model of $J_0(N)$, by its defining property. By Proposition 3.2 of [Ri], a multiple of $[P_1 - P_N]$ generates the prime-to-6 part of this latter group of components. (See [MR] for a detailed calculation in the case that N is square-free and $(6, N) = 1$.) Then, arguing as in the proof of Theorem 6.2, the vanishing of $L(E, 1)$ implies that $\pi([P_1 - P_N]) = O$. Hence the endomorphism $\pi \cdot \hat{\pi}$ of E kills $c(R)$ and R, so ℓ divides the degree of $\pi \cdot \hat{\pi}$, thus $\ell \mid \deg \phi$. □

Originally I had tried to prove Theorem 4.1 by taking a rational point of order ℓ on $J_0(N)$ and mapping it to E via $\pi : J_0(N) \to E$, rather than by using the dual $\hat{\pi} : E \to J_0(N)$. I encountered the obstacle that the rational point of order ℓ on $J_0(N)$ may be killed by π. For example, when $L(E, 1) = 0$, π kills the divisor class $[P_1 - P_N]$. But this fact turned out to be exactly what was needed to prove Theorems 6.2 and 1.3, thus supporting the case $L(\mathrm{Sym}^2 E, 2)$ of the Bloch-Kato conjecture, partially removing the dependence on numerical evidence in [Du2]. The goal of the last two sections is likewise to support the Bloch-Kato conjecture applied to some critical L-values, though it is now a different kind of L-function we are looking at. Theorem 7.3 below may be regarded as a higher weight analogue of Theorem 1.2.

7. Forms of higher weight

Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a normalised, new, cuspidal Hecke eigenform of weight $k \geq 2$ for $\Gamma_0(N)$. Recall that in the case that $k = 2$ and the a_n are rational, when f is associated to an isogeny class of elliptic curves over $\mathbb{Q}$, the existence of rational points of odd prime order ℓ on some curve in the isogeny class is equivalent to the congruences

$$a_p \equiv 1 + p \pmod{\ell} \text{ for all primes } p \nmid N.$$

The following proposition concerns the existence of analogous congruences for $N = 1$ and $k > 2$. From now on let $\Gamma = \mathrm{SL}_2(\mathbb{Z})$ and for any ring R let $M_k(\Gamma, R)$ be the R-module of modular forms of level one and weight k over R, in the sense of Katz [K] (see §1 of [E] for the definition and basic properties). Let $S_k(\Gamma, R)$ be the submodule of cusp forms.

Proposition 7.1. *Suppose that the prime $\ell > k$ divides the numerator of B_k, the k^{th} Bernoulli number. There exists a cuspidal Hecke eigenform $f \in S_k(\Gamma, O_K)$, where K is some finite extension of $\mathbb{Q}$, and a prime $\lambda \mid \ell$ of O_K, such that*

$$a_p \equiv 1 + p^{k-1} \pmod{\lambda} \quad \textit{for all primes } p,$$

where $f = \sum_{n=1}^{\infty} a_n q^n$.

Proof. Consider the Eisenstein series $G_k = -\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$ as an element of $M_k(\Gamma, \mathbb{Z}_\ell)$. Since $\mathrm{ord}_\ell(B_k/2k) > 0$, the base change $\overline{G_k}$ of G_k to $\mathbb{F}_\ell$ is a non-zero element of $S_k(\Gamma, \mathbb{F}_\ell)$. Since $\ell > 3$, the reduction map from $S_k(\Gamma, \mathbb{Z}_\ell)$ to $S_k(\Gamma, \mathbb{F}_\ell)$ is surjective, by Lemma 1.9 of [E]. Hence $\overline{G_k}$ may be regarded as an element of $S_k(\Gamma, \mathbb{Z}_\ell)/\ell S_k(\Gamma, \mathbb{Z}_\ell)$, moreover an eigenfunction for all the Hecke operators, with eigenvalue $1 + p^{k-1}$ for T_p. The proposition is then a consequence of Lemme 6.11 of [DS]. □

The known examples with $K = \mathbb{Q}$ are $k = 12$, $\ell = 691$, $k = 16$, $\ell = 3617$, $k = 18$, $\ell = 43867$, $k = 20$, $\ell = 283$ or 617, $k = 22$, $\ell = 131$ or 593, and $k = 26$, $\ell = 657931$. In all six cases the dimension of the space of cusp forms is one.

The following is a very special case of a theorem of Deligne [De], [Sc].

Proposition 7.2. *Let $f = \sum_{n=1}^{\infty} a_n q^n$ be as in Proposition 7.1. There exists a 2-dimensional K_λ-vector space V_λ supporting a linear action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, at all primes $p \nmid \ell$ unramified with*

$$\det(I - \mathrm{Frob}_p^{-1} T | V_\lambda) = 1 - a_p T + p^{k-1} T^2.$$

There is always at least one $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable O_λ-lattice (and all its scalar multiples) in V_λ, but there may be distinct stable lattices which are not scalar multiples of each other. These are analogous to (twists of) ℓ-adic Tate modules of different elliptic curves that are ℓ-isogenous to each other. Choosing some $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable

O_λ-lattice T_λ inside V_λ, let $A_\lambda = V_\lambda/T_\lambda$ and $A[\lambda] = A_\lambda[\lambda] \simeq T_\lambda/\lambda T_\lambda$. Then $A[\lambda]$ is analogous to $E'[\ell](-1)$ for an elliptic curve $E'/\mathbb{Q}$. The congruence in Proposition 7.1 forces the composition factors of $A[\lambda]$ to be $\mathbb{F}_\lambda$ and $\mathbb{F}_\lambda(1-k)$. Necessarily there is *some* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable O_λ-lattice T_λ inside V_λ such that $A[\lambda]$ has $\mathbb{F}_\lambda(1-k)$ as a submodule, but to give an analogue of Theorem 1.2 we must specify a choice of T_λ without reference to composition factors (in Theorem 1.2 we took the Tate module of the *optimal* elliptic curve in the isogeny class), then prove that it does have $\mathbb{F}_\lambda(1-k)$ as a submodule.

Theorem 7.3. *If T_λ is chosen to be the $\mathfrak{M}_{f,\lambda}$ constructed in 1.6.2 of* [DFG] *(using the cohomology of modular curves with coefficients in non-trivial local systems) then $A[\lambda]$ does have $\mathbb{F}_\lambda(1-k)$ as a submodule.*

Before proving this we need a few preliminaries. Diamond, Flach and Guo, in 1.4.2 of [DFG], construct "premotivic structures" $M(N,\psi), M(N,\psi)_c$ and $M(N,\psi)_!$ for the space of modular forms of level N and character ψ. We take $N=1$ and trivial ψ, and call these M, M_c and $M_!$. (There is a map from M_c to M with image $M_!$.) Each has Betti, de Rham, and (for each prime ℓ) ℓ-adic realisations, denoted $M_B, M_{\mathrm{dR}}, M_\ell$, etc. The Betti and de Rham realisations are $\mathbb{Q}$-vector spaces and the ℓ-adic realisations are $\mathbb{Q}_\ell$-vector spaces. There are various additional structures and comparison maps, discussed in detail in [DFG]. For example, M_ℓ supports a continuous representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. There are also S-integral premotivic structures $\mathfrak{M}, \mathfrak{M}_c$ and $\mathfrak{M}_!$, where S is the set of primes dividing $k!$. These have realisations $\mathfrak{M}_B$ (a $\mathbb{Z}$-lattice in M_B), $\mathfrak{M}_{\mathrm{dR}}$ (a $\mathbb{Z}[1/S]$-lattice in M_{dR}) and $\mathfrak{M}_\ell$ (a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-stable $\mathbb{Z}_\ell$-lattice in M_ℓ) for all primes ℓ, etc. For $\ell \notin S$ there is also a crystalline realisation $\mathfrak{M}_{\ell-\mathrm{crys}}$.

Let $\mathbb{T}'$ be the ring generated over $\mathbb{Z}$ by all the Hecke operators T_n acting on $M_k(\Gamma,\mathbb{C})$. There are compatible actions of $\mathbb{T}'$ on all of the above, by Proposition 1.3 of [DFG]. Let $\mathcal{I}$ be the ideal of $\mathbb{T}'$ generated by $T_p - (1+p^{k-1})$ for all primes p, and let $\mathfrak{m}$ be the maximal ideal generated by $\mathcal{I}$ and ℓ.

For $\ell \notin S$, $\mathfrak{M}_{\ell-\mathrm{crys}}$ is a filtered $\mathbb{Z}_\ell$ module with graded pieces of degrees 0 and $k-1$. There is a Hecke-equivariant isomorphism $\mathrm{Fil}^{k-1}\mathfrak{M}_{\ell-\mathrm{crys}} \simeq M_k(\Gamma,\mathbb{Z}_\ell)$. It has an injective Frobenius endomorphism ϕ, and is strongly divisible in the sense that $\mathfrak{M}_{\ell-\mathrm{crys}} = \phi\mathfrak{M}_{\ell-\mathrm{crys}} + \phi_{k-1}(\mathrm{Fil}^{k-1}\mathfrak{M}_{\ell-\mathrm{crys}})$, where $\ell^{k-1}\phi_{k-1} : \mathrm{Fil}^{k-1}\mathfrak{M}_{\ell-\mathrm{crys}} \to$

$\mathfrak{M}_{\ell-\mathrm{crys}}$ is the restriction of ϕ. (See the end of 1.4.2 of [DFG].) Similar statements apply to $\mathfrak{M}_c$ and $\mathfrak{M}_!$, with $S_k(\Gamma,\mathbb{Z}_\ell)$ replacing $M_k(\Gamma,\mathbb{Z}_\ell)$. Viewing $\mathfrak{M}_\ell, \mathfrak{M}_{c,\ell}$ and $\mathfrak{M}_{!,\ell}$ as $\mathbb{Z}_\ell$-modules with $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$-action, they may be identified with, respectively, $\mathbb{V}(\mathfrak{M}_{\ell-\mathrm{crys}}), \mathbb{V}(\mathfrak{M}_{c,\ell-\mathrm{crys}})$ and $\mathbb{V}(\mathfrak{M}_{!,\ell-\mathrm{crys}})$, where $\mathbb{V}$ is the covariant version of Fontaine and Lafaille's functor used in [DFG].

Lemma 7.4. *Suppose that the prime $\ell > k$ divides the numerator of B_k, the k^{th} Bernoulli number. The $\mathbb{F}_\ell[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module $(\mathfrak{M}_{!,\ell}/\ell\mathfrak{M}_{!,\ell})[\mathfrak{m}]$ has a unique subquotient isomorphic to $\mathbb{F}_\ell(1-k)$, and it is a submodule.*

Proof. This is based on the proof of Proposition 4.6 of [FJ]. The rank-one $\mathbb{Z}_\ell$-submodule $\mathcal{E}$ of $M_k(\Gamma,\mathbb{Z}_\ell)$ generated by the Eisenstein series G_k is the kernel of $\mathcal{I}$ on $\mathfrak{M}_{\ell-\mathrm{crys}}$, so is stable under ϕ_{k-1}, since ϕ commutes with the Hecke operators. Since ϕ is injective and $\mathfrak{M}_{\ell-\mathrm{crys}}$ is strongly divisible, we must have $\phi_{k-1}(\mathcal{E}) = \mathcal{E}$, so $\mathcal{E}$ is a strongly divisible filtered ϕ-module. The functor $\mathbb{V}$ takes $\mathcal{E}$ to a rank-one $\mathbb{Z}_\ell$-submodule E of $\mathfrak{M}_\ell$, stable under $\mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell)$. In fact, since $\mathbb{V}$ respects Hecke operators, $E = \mathfrak{M}_\ell[\mathcal{I}]$ and so is stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In fact, $E \simeq \mathbb{Z}_\ell(1-k)$ as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module, since $M_{!,\ell}[\mathcal{I}] = 0$, and by 1.2.0 of [Sc] the cokernel of the inclusion of $M_{!,\ell}$ in M_ℓ is $\mathbb{Q}_\ell(1-k)$.

Let $M_k = M_k(\Gamma,\mathbb{Z}_\ell)$ and $S_k = S_k(\Gamma,\mathbb{Z}_\ell)$. The image of $\mathcal{E}$ in $M_k/\ell M_k$ actually lies in $S_k/\ell S_k$, as noted in the proof of Proposition 7.1. This gives a ϕ_{k-1}-stable, one-dimensional $\mathbb{F}_\ell$-subspace $\overline{\mathcal{E}}$ of the finite-length filtered $\mathbb{Z}_\ell$-module $\mathfrak{M}_{!,\ell-\mathrm{crys}}/\ell\mathfrak{M}_{!,\ell-\mathrm{crys}}$, lying inside Fil^{k-1}. Since $\mathcal{E}$ is killed by $\mathcal{I}$, $\overline{\mathcal{E}} \subset (\mathfrak{M}_{!,\ell-\mathrm{crys}}/\ell\mathfrak{M}_{!,\ell-\mathrm{crys}})[\mathfrak{m}]$.

We may apply a finite-length version of the functor $\mathbb{V}$ (see 1.1.2 of [DFG]) to get a one-dimensional subspace W of $(\mathfrak{M}_{!,\ell}/\ell\mathfrak{M}_{!,\ell})[\mathfrak{m}]$. Inside $(\mathfrak{M}_\ell/\ell\mathfrak{M}_\ell)[\mathfrak{m}]$, W is just the reduction of E, so is isomorphic to $\mathbb{F}_\ell(1-k)$ as a module for $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

By the q-expansion principle, $\dim_{\mathbb{F}_\ell}(S_k(\Gamma,\mathbb{F}_\ell)[\mathfrak{m}]) = 1$, hence

$$\mathrm{Fil}^{k-1}(((\mathfrak{M}_{!,\ell-\mathrm{crys}}/\ell\mathfrak{M}_{!,\ell-\mathrm{crys}})[\mathfrak{m}])/\overline{\mathcal{E}}) = 0.$$

But

$$\mathbb{V}(((\mathfrak{M}_{!,\ell-\mathrm{crys}}/\ell\mathfrak{M}_{!,\ell-\mathrm{crys}})[\mathfrak{m}])/\overline{\mathcal{E}}) = ((\mathfrak{M}_{!,\ell}/\ell\mathfrak{M}_{!,\ell})[\mathfrak{m}])/W,$$

and the filtered module $\mathbb{F}_\ell\{1-k\}$ such that $\mathbb{V}(\mathbb{F}_\ell\{1-k\}) = \mathbb{F}_\ell(1-k)$ has $\mathrm{Fil}^{k-1}\mathbb{F}_\ell\{1-k\} = \mathbb{F}_\ell\{1-k\}$, so $(\mathfrak{M}_{!,\ell}/\ell\mathfrak{M}_{!,\ell})[\mathfrak{m}]$ cannot have any more composition factors isomorphic to $\mathbb{F}_\ell(1-k)$. □

Proof of Theorem 7.3. By construction, T_λ is a submodule of $\mathfrak{M}_{!,\ell} \otimes O_{K,\lambda}$, hence $A[\lambda]$ is a submodule of $((\mathfrak{M}_{!,\ell}/\ell\mathfrak{M}_{!,\ell}) \otimes \mathbb{F}_\lambda)[\mathfrak{m}]$, in which, as above, $\mathbb{F}_\lambda(1-k)$ has multiplicity one and appears as a submodule. It remains to observe that the subquotients of $A[\lambda]$ are $\mathbb{F}_\lambda$ and $\mathbb{F}_\lambda(1-k)$, so the latter must be a submodule. □

8. The Bloch-Kato formula

Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a normalised, cuspidal Hecke eigenform for Γ, of weight $k = 12, 16, 18, 20, 22$ or 26. In W. Stein's table "Rational parts of the special values of the L-functions of level 1" [St] one finds the rational numbers $L_f(j)(j-1)!/(2\pi)^j\Omega^\pm$ for the critical integers $1 \leq j \leq k-1$, where $\pm = (-1)^{j-1}$ and $\Omega^\pm$, which depends only on the parity of j, is a canonical period. In each case, there is a factor of ℓ in the denominator of $L_f(1)/(2\pi)\Omega^+$, where ℓ is as in Proposition 7.1. At least in these cases where $K = \mathbb{Q}$, it is possible to prove the presence of the factor of ℓ in the denominator without relying on numerical data. This is omitted, to avoid a digression on period ratios and modular symbols. We now proceed to explain the factor of ℓ using Theorem 7.3 combined with the Bloch-Kato conjecture on special values of L-functions.

Attached to f are a premotivic structure M_f and an S-integral premotivic structure $\mathfrak{M}_f$. The comparison isomorphism between $M_{f,B} \otimes \mathbb{C}$ and $M_{f,\mathrm{dR}} \otimes \mathbb{C}$ induces an isomorphism of 1-dimensional $\mathbb{R}$-vector spaces, from $M^\pm_{f,B} \otimes \mathbb{R}$ (eigenspace for $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$) to $(M_{f,\mathrm{dR}}/\mathrm{Fil}^{k-1}M_{f,\mathrm{dR}}) \otimes \mathbb{R}$. Let $\tilde{\Omega}^\pm$ be the determinant of this isomorphism, with respect to a $\mathbb{Z}$-basis for $\mathfrak{M}^\pm_{f,B}$ and some choice of $\mathbb{Z}[1/S]$-basis for $\mathfrak{M}_{f,\mathrm{dR}}/\mathrm{Fil}^{k-1}\mathfrak{M}_{f,\mathrm{dR}}$. A different choice only affects $\tilde{\Omega}^\pm$ by multiplying by an element of $\mathbb{Z}[1/S]^\times$. The periods $\Omega^\pm$ and $\tilde{\Omega}^\pm$ differ at worst by multiplication by an element of $\mathbb{Z}[1/S]^\times$ (c.f. Lemma 4.1 of [DSW]). For each prime l let $A_l = M_{f,l}/\mathfrak{M}_{f,l}$.

According to the Bloch-Kato conjecture [BK]

$$L_f(j)/(2\pi)^j\tilde{\Omega}^\pm = \frac{\prod_p c_p(j)\#Ш(j)}{\#H^0(\mathbb{Q}, A(j))\#H^0(\mathbb{Q}, A(k-j))}.$$

Here $Ш(j)$ is a generalised Shafarevich-Tate group, the $c_p(j)$ are certain rational Tamagawa factors and A is $\oplus_l A_l$. It follows from Lemmas 4.3 and 4.6 of [DSW] that each $c_p(j)$ is in $p^{\mathbb{Z}}$, and is 1 unless $p < k$.

We set $j = 1$. The ℓ-part of $\#H^0(\mathbb{Q}, A(1))$ is trivial, since the composition factors of $A[\ell](1)$ are $\mathbb{F}_\ell(1)$ and $\mathbb{F}_\ell(2-k)$, neither of which is trivial. So when we look at Stein's data and see that, in all the cases listed above, $L_f(1)/(2\pi)\Omega^+$ has a factor of ℓ in the denominator, the only way the Bloch-Kato conjecture can be true is if the ℓ-part of $\#H^0(\mathbb{Q}, A(k-1))$ is non-trivial. This necessitates $\mathbb{F}_\ell(1-k)$ as a submodule of $A[\ell]$, which is confirmed by Theorem 7.3. In [Du1] I looked only at ratios of L-values. This is not enough to derive the existence of the submodule $\mathbb{F}_\ell(1-k)$ from the Bloch-Kato conjecture, despite the suggestion in §6 of [Du1].

References

[AL] A. O. L. Atkin, J. Lehner, Hecke operators on $\Gamma_0(m)$, *Math. Ann.* **185** (1970), 135–160.

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

[BS] S. Baba, R. Sreekantan, An analogue of circular units for products of elliptic curves, *Proc. Edinb. Math. Soc. (2)* **47** (2004), 35–51.

[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.

[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.

[Ca] H. Carayol, Sur les représentations ℓ-adiques associées aux formes modulaires de Hilbert, *Ann. Sci. École Norm. Sup. (4)* **19** (1986), 409–468.

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

[De] P. Deligne, Formes modulaires et représentations ℓ-adiques. Sém. Bourbaki, éxp. 355, Lect. Notes Math. **179,** 139–172, Springer-Verlag, 1969.

[DS] P. Deligne, J.-P. Serre, Formes modulaires de poids 1, *Ann. Sci. Ec. Norm. Sup.* **7** (1974), 507–530.

[DFG] F. Diamond, M. Flach, L. Guo, The Tamagawa number conjecture of adjoint motives of modular forms, *Ann. Sci. École Norm. Sup. (4)* **37** (2004), 663–727.

[Du1] N. Dummigan, Period ratios of modular forms, *Math. Ann.* **318** (2000), 621–636.

[Du2] N. Dummigan, Symmetric squares of elliptic curves: rational points and Selmer groups, *Experiment. Math.* **11** (2002), 457–464.

[DSW] N. Dummigan, W. Stein, M. Watkins, Constructing elements in Shafarevich-Tate groups of modular motives, in *Number Theory and Algebraic Geometry,* M. Reid, A. Skorobogatov, eds., London Math. Soc. Lecture Note Series 303, 91–118, Cambridge University Press, 2003.

[E] B. Edixhoven, Serre's Conjecture, *in* Modular Forms and Fermat's Last Theorem, (G. Cornell, J. H. Silverman, G. Stevens, eds.), 209–242, Springer-Verlag, New York, 1997.

[Fa] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983), 349–366.

[FJ] G. Faltings, B. Jordan, Crystalline cohomology and $\mathrm{GL}(2,\mathbb{Q})$, *Israel J. Math.* **90** (1995), 1–66.

[Fl] 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.

[Fo] J.-M. Fontaine, Il n'y a pas de variété abélienne sur $\mathbb{Z}$, *Invent. Math.* **81** (1985), 515–538.

[K] N. M. Katz, p-adic properties of modular schemes and modular forms, in *Modular Functions of One Variable III,* Lect. Notes Math. **350,** 69–190, Springer-Verlag, 1973.

[La] R. P. Langlands, Modular forms and ℓ-adic representations, in *Modular Functions of One Variable II,* Lect. Notes Math. **349,** 361–500, Springer-Verlag, 1973.

[LS] A. Langer, S. Saito, Torsion zero-cycles on the self-product of a modular elliptic curve, *Duke Math. J.* **85** (1996), 315–357.

[Li] G. Ligozat, Courbes modulaires de genre 1, Bull. Soc. Math. France, Mém. 43, supplement to *Bull. Soc. Math. France* **103** (1975), 1–80.

[LO] S. Ling, J. Oesterlé, The Shimura subgroup of $J_0(N)$, Courbes modulaires et courbes de Shimura (Orsay, 1987/1988), *Astérisque* **196–197** (1991), 6, 171–203, (1992).

[Mz1] B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. IHES* **47** (1977), 33–186.

[Mz2] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978), 129–162.

[MR] B. Mazur, M. Rapoport, Appendix to B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. IHES* **47** (1977), 33–186.

[MO] J.-F. Mestre, J. Oesterlé, Courbes de Weil semi-stables de discriminant une puissance m-ième, J. reine angew. Math. **400** (1989), 173–184.

[Mi] I. Miyawaki, Elliptic curves of prime power conductor with $\mathbb{Q}$-rational points of finite order, *Osaka J. Math.* **10** (1973), 309–323.

[Ne] M. Newman, Construction and applications of a class of modular functions I, II, *Proc. London Math. Soc.* **7** (1957), 334–350 and **9** (1959), 373–387.

[Og] A. P. Ogg, Hyperelliptic modular curves, *Bull. Soc. Math. France* **102** (1974), 449–462.

[Ra] M. Raynaud, Schémas en groupes de type $(p,\dots,p)$, *Bull. Soc. Math. France* **102** (1974), 241–280.

[Ri] K. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Invent. Math.* **100** (1990), 431–476.

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

[Sc] A. J. Scholl, Motives for modular forms, *Invent. Math.* **100** (1990), 419–430.

[Se] B. Setzer, Elliptic curves of prime conductor, J. London Math. Soc. (2) **10** (1975), 367–378.

[St] W. Stein, The Modular Forms Database: Tables, http://modular.ucsd.edu/Tables/tables.html

[SW] W. Stein, M. Watkins, A database of elliptic curves–first report, *Algorithmic Number Theory (Sydney 2002),* 267–275, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002.

[Ste] G. Stevens, Stickelberger elements and modular parametrisations of elliptic curves, *Invent. Math.* **98** (1989), 75–106.

[T] S.-L. Tang, Congruences between modular forms, cyclic isogenies of modular elliptic curves and integrality of p-adic L-functions, *Trans. Amer. Math. Soc.* **349** (1997), no. 2, 837–856.

[V] V. Vatsal, Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves, *J. Inst. Math. Jussieu* **4** (2005), 281–316.

[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