POWERS OF 2 IN MODULAR DEGREES OF MODULAR ABELIAN VARIETIES

NEIL DUMMIGAN AND SRILAKSHMI KRISHNAMOORTHY

ABSTRACT. An analogue, for modular abelian varieties A, of a conjecture of Watkins on elliptic curves over $\mathbb{Q}$, would say that 2^R divides the modular degree, where R is the rank of the Mordell-Weil group $A(\mathbb{Q})$. We exhibit some numerical evidence for this. We examine various sources of factors of 2 in the modular degree, and the extent to which they are independent. Assuming that a certain 2-adic Hecke ring is a local complete intersection, and is isomorphic to a Galois deformation ring (a 2-adic "$\mathcal{R} \simeq T$" theorem), we show how the analogue of Watkins's conjecture follows, under certain conditions on A, extending and correcting earlier work on the elliptic curve case.

1. INTRODUCTION

Let $f = \sum_{n=1}^{\infty} a_n q^n$ be a normalised newform of weight 2, for the congruence subgroup $\Gamma_0(N)$. Let O_f and K_f be the ring and the field generated, over $\mathbb{Z}$ and over $\mathbb{Q}$ respectively, by the Hecke eigenvalues a_n. Then $K = K_f$ is a number field of some degree $d = [K : \mathbb{Q}]$, and O_f is an order of finite index in the ring of integers O_K of K. We shall think of K as an abstract number field inside $\overline{\mathbb{Q}}$, with the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ producing Galois conjugates $f_1, \ldots, f_d$ of f, with $f = f_1$, but if we fix an embedding of $\overline{\mathbb{Q}}$ into $\mathbb{C}$ then these all become forms with coefficients in $\mathbb{C}$ (in fact in $\mathbb{R}$).

Let $J_0(N)/\mathbb{Q}$ be the Jacobian of the modular curve $X_0(N)/\mathbb{Q}$. The Hecke correspondences T_p (for primes $p \nmid N$) and U_p (for primes $p \mid N$) of $X_0(N)$ act as endomorphisms, defined over $\mathbb{Q}$, of $J_0(N)$, let's say by Albanese functoriality. (See §3 of [Ri1] for a discussion of Picard and Albanese functoriality.) Let $\mathbb{T} = \mathbb{T}_{\mathbb{Z}}$ be the ring of endomorphisms of $J_0(N)$ generated in this way. (Note that $\mathbb{T}$ may also be realised as a ring of linear operators generated by Hecke operators on the space $S_2(\Gamma_0(N))$ of cusp forms of weight 2 for $\Gamma_0(N)$.) Let $I_f = I_{f,\mathbb{Z}} = I_{\mathbb{Z}}$ be the kernel of the homomorphism $\theta_f : \mathbb{T}_{\mathbb{Z}} \to O_f$ determined by $T_p \mapsto a_p, U_p \mapsto a_p$, so $O_f \simeq \mathbb{T}_{\mathbb{Z}}/I_f$. (Note that I_f depends only on the Galois conjugacy class of f, in fact $S_2(\Gamma_0(N))[I_f]$ is spanned by $f_1, \ldots, f_d$.) Then $A = A_f := J_0(N)/I_f J_0(N)$ is a connected abelian variety of dimension $d = [K : \mathbb{Q}]$, defined over $\mathbb{Q}$, the modular quotient associated to f (or equally to any of the f_i–the cotangent space to $A_f(\mathbb{C})$ is spanned by these conjugates). Let $\pi_f : J_0(N) \to A$ be the projection morphism. Then there is a dual morphism $\pi_f^\vee : A^\vee \to J_0(N)^\vee$, but as a jacobian, $J_0(N)$ is naturally isomorphic to its dual abelian variety, via the theta polarisation, so we may view $\pi_f^\vee : A^\vee \to J_0(N)$. The action of $\mathbb{T}$ on $J_0(N)$ restricts to an action of $\mathbb{T}/I_f \simeq O_f$ on $A^\vee$, indeed $A^\vee$ is the connected component of the identity in the kernel of I_f on $J_0(N)$. (Strictly speaking it is I_f^* that kills $A^\vee$, where * is the Rosati

Date: June 5th, 2012.

involution associated to the theta polarisation of $J_0(N)$. But $T_p^* = T_p$ for $p \nmid N$ and $U_p^* = W_N U_p W_N$ for $p \mid N$, where W_N is the Atkin-Lehner involution, which restricts to the eigenvalue $w_N(f) = \pm 1$ on $A^\vee$.) The homomorphism $\pi_f \pi_f^\vee : A^\vee \to A$ is known to be an isogeny of square degree. (It is the polarisation of $A^\vee$ defined by the pullback of the theta divisor.) The square root of this degree is called the *modular degree* of A_f. In the case that $K_f = \mathbb{Q}$ and A is an elliptic curve, so $A^\vee \simeq A$, $\pi_f \pi_f^\vee : A \to A$ is multiplication by the degree of the morphism ("modular parametrisation") $\phi : X_0(N) \to A$, obtained by using a rational point to embed $X_0(N)$ in $J_0(N)$, then composing with $\pi_f : J_0(N) \to A$. In fact, on divisor classes, $\pi_f^\vee$ is ϕ^* and π_f is ϕ_*. In general, the modular degree is 1 if and only if $J_0(N)$ is isomorphic (rather than just isogenous) to the direct sum of A and another abelian variety.

M. Watkins conjectured [Wa], in the case that A is an elliptic curve, that 2^R (or even the order of the 2-Selmer group) divides the modular degree, where R is the rank of the group $A(\mathbb{Q})$ of rational points. It is natural to simply extend this conjecture to modular abelian varieties of any dimension. Since $A(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a K-vector space, R is necessarily a multiple of d. According to the Birch-Swinnerton-Dyer conjecture, R should be the order of vanishing at $s = 1$ of the L-function $L(A, s)$, which is the same as $\prod_{i=1}^d L(f_i, s)$. If the sign in the functional equation of $L(f, s)$ (namely $\epsilon = -\prod_{p|N} w_p(f)$, where $w_p(f)$ is the eigenvalue of the Atkin-Lehner involution W_p) is -1, then $L(A, 1) = 0$, so we would expect $R \geq d$ and 2^d dividing the modular degree, m. This is amply borne out in numerical examples in the tables of Stein [Ste]. All the examples with $N \leq 200$ and $\epsilon = -1$ are as follows.

N	d	m	N	d	m
67	2	2^2	133	2	2^4
73	2	2^2	133	2	$2^4 \cdot 3$
85	2	2^3	137	4	2^4
93	2	2^4	139	3	2^3
97	3	2^3	145	2	$2^3 \cdot 7$
103	2	2^2	147	2	2^4
107	2	2^2	149	3	2^3
109	3	2^3	151	3	2^3
113	3	2^3	157	5	2^5
115	2	2^4	161	2	2^4
127	3	2^3	163	5	$2^5 \cdot 3$

There are more spectacular examples further along, such as **443D**, with $d = 12$ and $m = 2^{13} \cdot 3 \cdot 7$, **457B**, with $d = 15$ and $m = 2^{15} \cdot 31$, and **487E**, with $d = 17$ and $m = 2^{17}$. Without the condition that $\epsilon = -1$, it is often the case that $2^d \nmid m$. For example, for **173A**, $d = 4, \epsilon = -1$ and $m = 2^4$, while for **173B**, $d = 10, \epsilon = 1$ but still $m = 2^4$. Similarly for **191A,B**, with $d = 2, 14$, $m = 2^2$, **281A,B** with $d = 7, 16$, $m = 2^7$, and **367A,B** with $d = 11, 19$, $m = 2^{11}$. There are several similar pairs of conductor ≤ 500.

Though it is tempting to view the above as good evidence for the direct analogue of Watkins's conjecture, we need to be more circumspect. For each prime $p \mid N$ let W_p (sometimes known as W_{p^α}, where $p^\alpha \mid\mid N$) be the Atkin-Lehner involution, which acts on $S_2(\Gamma_0(N))$, with f an eigenvector. It also acts on $X_0(N)$ as an

involution defined over $\mathbb{Q}$, and as an endomorphism defined over $\mathbb{Q}$ on $J_0(N)$. (The same endomorphism by either Picard or Albanese functoriality.) Let W be the group of order 2^s generated by the W_p (where s is the number of primes dividing N), and let $W' = W'(f)$ be the subgroup (of index 1 or 2) acting as $+1$ on f. We shall see in Section 2 that if $A_f(\mathbb{Q})[2] = \{O\}$ then $(\#W')^d \mid m$. This then is an alternative source of powers of 2 in the modular degree. It is easiest to understand in the case $d = 1$ that A_f is an elliptic curve, where the modular parametrisation $\phi : X_0(N) \to A$ factors through the quotient morphism $X_0(N) \to X_0(N)/W'$, which has degree $\#W'$. Note that if $A_f(\mathbb{Q})[2] \neq \{O\}$ then it is possible for an element of W' to induce translation by a rational 2-torsion point, so for ϕ to factor only through the quotient of $X_0(N)$ by some smaller subgroup of W', contributing some smaller power of 2 to $\deg \phi$. But we are always guaranteed that $(\#W'/\#A_f(\mathbb{Q})[2])^d \mid m$. We must now admit that, with the exception of **145B**, for which $\#W' = 2$ and $\#A_f(\mathbb{Q})[2] = 2^2$, every single instance of $2^d \mid m$ mentioned above can be accounted for by this. So to support the analogue of Watkins's conjecture we must try harder. In the case that N is prime, the contribution of Atkin-Lehner involutions is minimal. In this case, and when A_f is an elliptic curve, Watkins has produced numerous examples for which $R = 4$ and $2^4 \mid m$, supporting his conjecture.

If N is prime and $w_N = -1$ then W' is trivial so does not account for any power of 2 in m. Since $\epsilon = -w_N = 1$, $L(f, s)$ vanishes to even order at $s = 1$, so if $L(f, 1) = 0$ then it vanishes to order at least 2. Vanishing of $L(f, 1)$ implies vanishing of all the $L(f_i, 1)$, similarly all to order at least 2, so $\mathrm{ord}_{s=1} L(A, s) \geq 2d$, and we expect that $2^{2d} \mid m$. The following table gives all the examples with $d > 1$ and $N < 3650$ (found using Magma), and our expectation is fully borne out, supporting the higher-dimensional analogue of Watkins's conjecture quite convincingly if one compares the $d = 2$ examples with the $d = 3, 4$ examples.

N	d	m
1061	2	$2^4 \cdot 151$
1567	3	$2^9 \cdot 7 \cdot 41$
1693	3	$2^6 \cdot 1301$
1913	2	$2^4 \cdot 5^2 \cdot 61$
2029	2	$2^4 \cdot 5 \cdot 269$
2081	2	$2^4 \cdot 1319$
2293	2	$2^4 \cdot 479$
2333	4	$2^8 \cdot 83341$
2381	2	$2^4 \cdot 971$
2593	4	$2^8 \cdot 67 \cdot 2213$

N	d	m
2609	2	$2^4 \cdot 19 \cdot 61$
2843	3	$2^6 \cdot 3^3 \cdot 7 \cdot 587$
2861	2	$2^4 \cdot 11 \cdot 61$
2963	2	$2^4 \cdot 31 \cdot 61$
3019	2	$2^4 \cdot 3259$
3089	2	$2^4 \cdot 5 \cdot 131$
3217	3	$2^6 \cdot 7 \cdot 43 \cdot 71$
3463	2	$2^6 \cdot 199$
3583	2	$2^7 \cdot 17 \cdot 29$

We shall assume the following conditions on a modular abelian variety A (i.e. the quotient of $J_0(N)$ attached to a newform f):

(1) N is even and square-free;
(2) $A[2](\mathbb{Q}) = \{O\}$;
(3) $A(\mathbb{R})$ is connected;
(4) $\#\Phi_{A,p}$ (the group of components of the special fibre of the Néron model) is odd for each prime $p \mid N$;
(5) $2 \nmid \mathrm{disc}(O_f)$.

We explore the consequences of the assumption that a certain map between a 2-adic deformation ring $\mathcal{R}_{\mathcal{D}'}$ and a completed Hecke ring $\mathbb{T}_{\mathfrak{m}}$ is an isomorphism, and that

these rings are local complete intersections. The modular degree is linked to $\mathbb{T}_{\mathfrak{m}}$, and we bound from below the power of 2 dividing it by bounding from below the power of 2 dividing the order of the reduced cotangent space to $\mathcal{R}_{\mathcal{D}'}$. As in [Du] (in the elliptic curve case) we produce elements using Galois cohomology classes coming from rational points, to show that 2^{R-d} would divide the modular degree. In addition, as well as treating the case of modular abelian varieties of any dimension, we show that an (in general) even larger power of 2 would divide the modular degree. There are two ways to do this. One uses independent elements constructed from newforms g with the same residual mod 2 Galois representation as f, but different Atkin-Lehner eigenvalues. See Corollary 9.5. The other (using certain quotients of the original deformation and Hecke rings) shows that the contribution $(\#W')^d$ of the Atkin-Lehner involutions is independent of the contribution 2^{R-d} of rational points, by working with the quotient curve $X_0(N)/W'$. Since (under the condition (1)) $\#W' \geq 2$, this shows that the assumptions about deformation rings and Hecke rings imply that $2^R \mid m$, in accord with the analogue of Watkins's conjecture. See Corollary 12.3.

Acknowledgments. We are grateful to F. Diamond, J. Manoharmayum, W. Stein and M. Watkins for helpful communications. We are especially indebted to an anonymous referee for correcting an important error in an earlier version (and in [Du]), which had 2^R in place of 2^{R-d}, and for suggesting that we should determine whether or not a certain example of $\mathbb{T}_{\mathfrak{m}}$ is a local complete intersection.

2. The contribution of Atkin-Lehner involutions

Proposition 2.1. *With W' as above,*

$$\left(\frac{\#W'}{\#A_f(\mathbb{Q})[2]}\right)^d \Big| m,$$

where m is the modular degree and $d = [K : \mathbb{Q}]$ is the dimension of A_f.

Proof. Let P_0 be a fixed rational point on $X_0(N)$ (for example the cusp ∞). If $w \in W'$ then w acts trivially on A_f, i.e. if $\pi : J_0(N) \to A$ is the projection, and $[D] \in J_0(N)$, then $\pi([w(D)]) = \pi([D])$ for all divisors D of degree zero on $X_0(N)$. In particular, for any $P \in X_0(N)$, $\pi([w(P) - w(P_0)]) = \pi([(P) - (P_0)])$, so $\pi([w(P) - (P)]) = \pi([w(P_0) - (P_0)])$. Applying this to $P = w(P_0)$ shows that $\pi([w(P_0) - (P_0)]) \in A[2]$. Since $P_0 \in X_0(N)(\mathbb{Q})$ and w is defined over $\mathbb{Q}$, in fact $\pi([w(P_0) - (P_0)]) \in A(\mathbb{Q})[2]$. It is easy to see that the map $w \mapsto \pi([w(P_0) - (P_0)])$ is a homomorphism from W' to $A(\mathbb{Q})[2]$. Let W'' be its kernel. This has size at least $\frac{\#W'}{\#A_f(\mathbb{Q})[2]}$, so it suffices to prove that $(\#W'')^d \mid m$.

Let $X'' = X_0(N)/W''$, an algebraic curve over $\mathbb{Q}$, with $\theta : X_0(N) \to X''$ the quotient morphism. Let $J'' = J(X'')$ be its Jacobian. Let P_0'' be the image of P_0 on X''. We have embeddings $\iota : X_0(N) \hookrightarrow J_0(N)$ and $\iota'' : X'' \hookrightarrow J''$, given by $P \mapsto [(P) - (P_0)]$ and $P'' \mapsto [(P'') - (P_0'')]$ respectively. There is a commutative

diagram

$$\begin{array}{ccc} X_0(N) & \xrightarrow{\theta} & X'' \\ {\scriptstyle\iota}\downarrow & & {\scriptstyle\iota''}\downarrow \\ J_0(N) & \xrightarrow{\theta_*} & J''. \\ {\scriptstyle\pi}\downarrow & & \\ A & & \end{array}$$

For any $w \in W''$, $\pi([w(P_0)-(P_0)]) = O$, so $\pi([w(P)-w(P_0)]) = \pi([(P)-(P_0)])$ becomes $\pi\circ\iota\,(w(P)) = \pi\circ\iota\,(P)$, for all $P \in X_0(N)$. Hence $\pi\circ\iota$ factors through X'', and therefore, by the universal property of Jacobians, through $\iota''\circ\theta$. Since the image of ι generates $J_0(N)$, it follows that π factors through θ_*, say

$$J_0(N) \xrightarrow{\theta_*} J'' \xrightarrow{\pi''} A.$$

We have dual maps, composing to $\pi^\vee$:

$$A^\vee \xrightarrow{\pi''^\vee} J'' \xrightarrow{\theta^*} J_0(N).$$

Now

$$\pi\circ\pi^\vee = \pi''\circ\theta_*\circ\theta^*\circ\pi''^\vee = \pi''\circ[\deg(\theta)]\circ\pi''^\vee = [\#W'']\circ(\pi''\circ\pi''^\vee).$$

The order of the kernel of the multiplication map $[\#W'']$ on A is $(\#W'')^{2d}$, hence $(\#W'')^d \mid m$. □

3. Preliminaries on modular curves and p-adic uniformisation of abelian varieties

Suppose that $p \,||\, N$. Following Deligne and Rapoport [DR], we consider a certain model $\mathcal{X}/\mathbb{Z}_p$ for the modular curve $X_0(N)/\mathbb{Q}_p$. It is proper and flat, but not necessarily regular. Its special fibre $\tilde{\mathcal{X}}/\mathbb{F}_p$ has two irreducible components, isomorphic to $X_0(N/p)/\mathbb{F}_p$, crossing at supersingular points, which are ordinary double points, defined over $\mathbb{F}_{p^2}$. Let $\mathcal{J}_0(N)/\mathbb{Z}_p$ be the Néron model of $J_0(N)/\mathbb{Q}_p$, and let $\tilde{\mathcal{J}}_0(N)/\mathbb{F}_p$ be its special fibre, with connected component $\tilde{\mathcal{J}}_0(N)^0$ and group of components $\Phi = \tilde{\mathcal{J}}_0(N)/\tilde{\mathcal{J}}_0(N)^0$. As explained in §2 of [Ri1] (drawing on [Ra1, SGA7, MR, JL]), $\tilde{\mathcal{J}}_0(N)^0$ is an extension of the abelian variety $J_0(N/p)/\mathbb{F}_p \oplus J_0(N/p)/\mathbb{F}_p$ by a torus T_J, whose character group $X_J := \mathrm{Hom}_{\overline{\mathbb{F}}_p}(T_J/\overline{\mathbb{F}}_p, \mathbb{G}_m/\overline{\mathbb{F}}_p)$ is isomorphic (as a module for $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$) to $H_1(\mathcal{G},\mathbb{Z})$, where $\mathcal{G}$ is a graph with two vertices (one for each component of $\tilde{\mathcal{X}}/\mathbb{F}_p$) and an edge for each ordinary double point. The Atkin-Lehner involutions W_p and W_N extend to $\mathcal{X}$, and have a modular interpretation.

Lemma 3.1. *Let* Frob_p *be the generator* $x \mapsto x^p$ *of* $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$. *Then* W_p *acts as* $-\mathrm{Frob}_p$ *on* X_J.

Proof. It follows from the modular interpretation of W_p that it permutes the supersingular points of $\tilde{\mathcal{X}}/\mathbb{F}_p$ (i.e. the edges of $\mathcal{G}$) in the same way as Frob_p, but because it also swaps the components of $\tilde{\mathcal{X}}/\mathbb{F}_p$ (the vertices of $\mathcal{G}$), which Frob_p doesn't do, the action of W_p on $H_1(\mathcal{G},\mathbb{Z})$ is minus that of Frob_p. □

Lemma 3.2. *If $p \,||\, N$ then the connected component (of the identity) of the special fibre at p of the Néron model of A (or $A^\vee$) is a torus. In other words, A and $A^\vee$ have purely toric reduction.*

Proof. A is a quotient of, and $A^\vee$ a subvariety of, $J_0(N)$. Each is killed by the ideal $I_{\mathbb{Z}}$ associated to f. Since f is a newform (in particular, new at p), but the abelian variety quotient of $\tilde{J}_0(N)^0$ is $J_0(N/p)/\mathbb{F}_p \oplus J_0(N/p)/\mathbb{F}_p$, the lemma follows. □

Lemma 3.3. *Let $B/\mathbb{Q}_p$ be an abelian variety with purely toric reduction over $\mathbb{F}_p$. Let X_B and $X_{B^\vee}$ be the character groups of the connected components of the special fibres of the Néron models of B and its dual $B^\vee$. Then there is an exact sequence of groups, respecting the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$*:*

$$0 \longrightarrow X_{B^\vee} \xrightarrow{q} \mathrm{Hom}(X_B, \overline{\mathbb{Q}}_p^\times) \longrightarrow B(\overline{\mathbb{Q}}_p) \longrightarrow 0.$$

The group $\Phi_{B,p}$, of components of the special fibre at p of the Néron model of B, is isomorphic to $\mathrm{Hom}(X_B, \mathbb{Z})/v \circ q(X_{B^\vee})$*, where $v : \overline{\mathbb{Q}}_p^\times \to \mathbb{Q}$ is* ord_p*.*

This is a consequence of the theory summarised in [Ra2]. The identification with $X_{B^\vee}$ of the discrete subgroup of the torus by which we quotient out, is from [SGA7], IX, 14.1.

Lemma 3.4. *If ℓ is any prime number, and $B/\mathbb{Q}_p$ as in Lemma 3.3 above, then*

(1) *there is, for each $n \geq 1$, an exact sequence*

$$0 \to \mathrm{Hom}(X_B, \mu_{\ell^n}) \to B[\ell^n] \to X_{B^\vee}/\ell^n X_{B^\vee} \to 0$$

of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$*-modules;*

(2) *there is an exact sequence*

$$0 \to \mathrm{Hom}(X_B, T_\ell(\mu)) \to T_\ell(B) \to X_{B^\vee} \otimes \mathbb{Z}_\ell \to 0$$

of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$*-modules.*

Here, $T_\ell(\mu) := \varprojlim_n \mu_{\ell^n} = \mathbb{Z}_\ell(1)$ and $T_\ell(B) := \varprojlim_n B[\ell^n]$, and the lemma is just Lemmas 3.3.1 and 3.3.2 of [Ri2], easy consequences of the Snake Lemma.

4. λ-adic and residual representations

Recall that we have the order O_f in O_K. If we impose the condition $2 \nmid [O_K : O_f]$ then the natural map from $O_f/2O_f$ to $O_K/2O_K \simeq \oplus_{i=1}^t (O_{\lambda_i}/\lambda_i^{E_i})$ is an isomorphism, and similarly $O_f \otimes \mathbb{Z}_2 \simeq O_K \otimes \mathbb{Z}_2 \simeq \oplus_{i=1}^t O_{\lambda_i}$ is an isomorphism, where $2\,O_K = \prod_{i=1}^t \lambda_i^{E_i}$. Let $1 = \sum_{i=1}^t e_i$ in $O_f \otimes \mathbb{Z}_2$, where e_i is the projection onto the i^{th} factor. We also denote by λ_i the ideal $\lambda_i \cap O_f$ of O_f, and its image $\lambda_i O_{\lambda_i} \oplus \oplus_{j \neq i} O_{\lambda_j}$ in $O_f \otimes \mathbb{Z}_2$. Given a module for $O_f \otimes \mathbb{Z}_2$, tensoring over $O_f \otimes \mathbb{Z}_2$ with O_{λ_i} (via the projection to that factor) is equivalent to applying e_i.

With $A = A_f$, let $T_2(A) = \varprojlim_n A[2^n]$ and $V_2(A) = T_2(A) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$. For $1 \leq i \leq t$ let $T_{\lambda_i}(A) = e_i T_2(A)$, a free O_{λ_i}-module of rank 2 with O_{λ_i}-linear $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action, and $V_{\lambda_i}(A) = e_i V_2(A)$, a 2-dimensional K_{λ_i}-vector space with K_{λ_i}-linear $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action. Also let $V_i = T_{\lambda_i}(A)/\lambda_i T_{\lambda_i}(A)$, a 2-dimensional $\mathbb{F}_{\lambda_i}$-vector space with $\mathbb{F}_{\lambda_i}$-linear $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action. Let $\rho_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{O_{\lambda_i}}(T_{\lambda_i})$ be the representation by which $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on T_{λ_i}, and $\overline{\rho}_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{F}_{\lambda_i}}(V_i)$ its reduction modulo λ_i.

Lemma 4.1. *If $p \,||\, N$ then $\rho_i|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$ has the form $\begin{pmatrix} \chi(a_p)\omega & * \\ 0 & \chi(a_p) \end{pmatrix}$, where ω is the 2-adic cyclotomic character and $\chi(a_p)$ is the unramified character such that $\chi(a_p)(\mathrm{Frob}_p) = a_p = -w_p$.*

Proof. $X_{A^\vee}$ and X_A are free $\mathbb{Z}$-modules of rank d, with O_f-action, so $X_{A^\vee} \otimes \mathbb{Q}$ and $X_A \otimes \mathbb{Q}$ are 1-dimensional K-vector spaces. It follows that $e_i(X_{A^\vee} \otimes \mathbb{Z}_2)$ and $e_i\mathrm{Hom}(X_A, T_2(\mu))$ are free O_{λ_i}-modules of rank one. Now $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts on $T_2(\mu)$ by ω, and on $X_{A^\vee}$ and X_A by $\chi(a_p)$ (by Lemma 3.1). The lemma follows from Lemma 3.4 (2) (with $B = A$) by applying the projector e_i. □

Proposition 4.2. *Suppose $2 \nmid [O_K : O_f]$, and let V_i and $\overline{\rho}_i$ be as above, for some $1 \le i \le t$. If*

1. *N is even and square-free;*
2. *$A[2](\mathbb{Q}) = \{O\}$ and*
3. *$A(\mathbb{R})$ is connected,*

then $\overline{\rho}_i$ is absolutely irreducible.

Proof. Let $U_i = (e_i A[2])[\lambda_i]$. If U_i is irreducible then necessarily $U_i \simeq V_i$. Therefore it suffices to prove that U_i is absolutely irreducible.

It follows from the fact that $A(\mathbb{R})$ is connected (isomorphic to $(\mathbb{R}/\mathbb{Z})^d$ as a topological group) that $\#\, A[2](\mathbb{R}) = 2^d$. Now $H_1(A(\mathbb{R}), \mathbb{Q})$ is a K-vector space, necessarily 1-dimensional, from which it follows that $e_i H_1(A(\mathbb{R}), \mathbb{Q}_2)$ is a 1-dimensional K_{λ_i}-vector space. Then $e_i H_1(A(\mathbb{R}), \mathbb{Z}_2)$ is a free O_{λ_i}-module of rank 1, and $e_i A[2](\mathbb{R}) \simeq e_i(H_1(A(\mathbb{R}), \mathbb{Z})/2H_1(A(\mathbb{R}), \mathbb{Z})) \simeq e_i(H_1(A(\mathbb{R}), \mathbb{Z}_2)/2H_1(A(\mathbb{R}), \mathbb{Z}_2))$ is a free $(O_{\lambda_i}/2O_{\lambda_i})$-module of rank 1. Then $U_i(\mathbb{R})$, i.e. the $\mathbb{F}_{\lambda_i}$-subspace of invariants of complex conjugation in U_i, is 1-dimensional.

Now any $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant line in $U_i \otimes \overline{\mathbb{F}}_{\lambda_i}$ is necessarily made up of invariants under complex conjugation (since the only possible eigenvalues are 1 and $-1 = 1$ in $\overline{\mathbb{F}}_{\lambda_i}$). Hence such a line must be $U_i(\mathbb{R}) \otimes_{\mathbb{F}_{\lambda_i}} \overline{\mathbb{F}}_{\lambda_i}$, so $U_i(\mathbb{R})$ is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant line in U_i, assuming that such a line exists. Let χ be the character by which $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $U_i(\mathbb{R})$. If $p \mid N$ then by Lemma 4.1, $\chi|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$ is trivial. (Note that both ω and the $\chi(a_p)$ in that lemma become trivial modulo λ_i.) Also, if $p \nmid N$ then χ is unramified at p (using the fact that $2 \mid N$). The only character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ unramified at all p is the trivial character, so χ is trivial, and any non-zero element of $U_i(\mathbb{R})$ is a rational point of order 2 on A, contradicting (2). □

Proposition 4.3. *Suppose that $p \,||\, N$ and that $\#\Phi_{A,p}$ is odd. Then, for each i, there exists $\gamma \in I_p$ (the inertia group at p) such that the $*$ in the matrix of Lemma 4.1 is not divisible by λ_i.*

Proof. By the last part of Lemma 3.3, using the oddness of $\#\Phi_{A,p}$, $v \circ q$ induces an isomorphism $e_i(X_{A^\vee} \otimes ((1/2)\mathbb{Z}/\mathbb{Z})) \simeq e_i(\mathrm{Hom}(X_A, (1/2)\mathbb{Z}/\mathbb{Z}))$. The left-hand side (rather its image under q) represents the quotient of $e_i(A[2](\overline{\mathbb{Q}}_p))$ by $e_i\mathrm{Hom}(X_A, \mu_2)$. We need to show that I_p acts non-trivially on any representative of a non-zero element of this quotient, but this is true because it acts non-trivially on any element of $\mathrm{Hom}(X_A, \overline{\mathbb{Q}}_p^\times)$ that maps under v to a non-zero element of $\mathrm{Hom}(X_A, \mathbb{Q}/\mathbb{Z})$. □

5. Pairings

Recall that $2O_K = \prod_{i=1}^{t} \lambda_i^{E_i}$, and we are assuming that $2 \nmid [O_K : O_f]$. From now on we shall assume that all $E_i = 1$, i.e. that 2 is unramified in O_K, since this will be necessary anyway once we consider deformation rings and Hecke rings, and makes the exposition slightly simpler from this point onwards. With $2 \nmid [O_K : O_f]$, this is equivalent to $2 \nmid \mathrm{disc}(O_f)$. Let F_i be the degree of the prime divisor λ_i. Recall that $V_i := T_{\lambda_i}(A)/\lambda_i T_{\lambda_i}(A)$, but since 2 is unramified we also have now $V_i \simeq e_i(A[2])$. Let $V_i^* = \mathrm{Hom}_{\mathbb{F}_2}(V_i, \mathbb{F}_2)$, which is also naturally a 2-dimensional $\mathbb{F}_{\lambda_i}$-vector space. Let $W_i = \mathrm{Sym}^2 V_i$, i.e. the subspace of symmetric tensors in $V_i \otimes_{\mathbb{F}_{\lambda_i}} V_i$, and $W_i^* = \mathrm{Hom}_{\mathbb{F}_2}(W_i, \mathbb{F}_2)$. These are 3-dimensional $\mathbb{F}_{\lambda_i}$-vector spaces.

We have Weil pairings

$$A[2] \times A^\vee[2] \to \mu_2,$$
$$T_2(A) \otimes T_2(A^\vee) \to T_2(\mu).$$

With respect to these pairings, the Hecke operators T_p and U_p, which generate O_f, are self-adjoint. This follows from the discussion in §3 of [Ri1], and from Lemma 16.2(a) of [Mi]. Hence for $i \neq j$, $e_i(A[2])$ and $e_j(A^\vee[2])$ are orthogonal, and likewise $e_i(T_2(A))$ and $e_j(T_2(A^\vee))$ are orthogonal. We can then restrict to perfect pairings

$$e_i(A[2]) \times e_i(A^\vee[2]) \to \mu_2,$$
$$e_i(T_2(A)) \times e_i(T_2(A^\vee)) \to T_2(\mu).$$

Assuming irreducibility of $\overline{\rho}_i$, as in the conclusion of Proposition 4.2, the polarisation $A^\vee \to A$ from the introduction necessarily identifies $e_i(T_2(A^\vee))$ with $\lambda_i^r e_i(T_2(A))$ for some r, then re-scaling we get $e_i(T_2(A^\vee)) \simeq e_i(T_2(A))$, hence perfect pairings

$$V_i \times V_i \to \mu_2,$$
$$T_{\lambda_i}(A) \otimes T_{\lambda_i}(A) \to T_2(\mu).$$

In particular, we have an isomorphism $V \simeq V^*$, respecting the actions of $\mathbb{F}_\lambda$ and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. (We drop the subscripts i temporarily, imagining a fixed choice to have been made.)

Lemma 5.1. *Under the isomorphism $V \simeq V^*$ we have, for any $x \in V$ and $\alpha, \beta \in \mathbb{F}_\lambda$, $(\alpha x)(\beta x) = 0$, where $\alpha x \in V^*$ is applied to $\beta x \in V$.*

Proof. It suffices to show that, under the Weil pairing $[,] : T_\lambda(A) \times T_\lambda(A) \to \mathbb{Z}_2(1)$, we have, for any $\alpha, \beta \in O_\lambda$ and $x \in T_\lambda(A)$, $[\alpha x, \beta x] = 0$. The Weil pairing $[,]$ may be viewed as a $\mathbb{Z}_2$-linear map from $\wedge^2_{O_\lambda} T_\lambda(A)$ (a free O_λ-module of rank one) to $\mathbb{Z}_2(1)$. (The wedge is over O_λ because T_p and U_p are self-adjoint.) But there is a $\mathbb{Z}_2$-linear isomorphism $O_\lambda \simeq \mathrm{Hom}_{\mathbb{Z}_2}(O_\lambda, \mathbb{Z}_2)$, with $\gamma \mapsto (\beta \mapsto \mathrm{tr}_{O_\lambda/\mathbb{Z}_2}(\gamma\beta))$. Hence there is an O_λ-linear, skew-symmetric pairing $[,]' : T_\lambda(A) \times T_\lambda(A) \to O_\lambda(1)$ such that $[,] = \mathrm{tr}([,]')$. Since the O_λ submodule spanned by x is isotropic for $[,]'$, the lemma follows. □

Using the trace as in the above proof, we see that there is a natural isomorphism between $V^* := \mathrm{Hom}_{\mathbb{F}_2}(V, \mathbb{F}_2)$ and $\mathrm{Hom}_{\mathbb{F}_\lambda}(V, \mathbb{F}_\lambda)$. It follows, since the pairing is skew-symmetric, that $W := \mathrm{Sym}^2 V$, inside $V \otimes V \simeq V^* \otimes V$, may be identified with $\mathrm{ad}^0(V) = \{A \in \mathrm{Hom}_{\mathbb{F}_\lambda}(V, V) : \mathrm{tr}(A) = 0\}$. (This W is not to be confused with the group of Atkin-Lehner involutions!) Also, by composing with the trace, we may identify $W^* := \mathrm{Hom}_{\mathbb{F}_2}(W, \mathbb{F}_2)$ with the set of $\mathbb{F}_\lambda$-valued quadratic polynomial

functions on V, i.e. with the symmetric quotient of $V^* \otimes_{\mathbb{F}_\lambda} V^*$. The following is a direct consequence of Lemma 5.1.

Lemma 5.2. *For any $x \in V$ (which may be viewed as an element of V^* using the isomorphism $V \simeq V^*$), and $\alpha, \beta \in \mathbb{F}_\lambda$, we have $(\alpha x^2)(\beta x \otimes x) = 0$.*

6. A Selmer group

Let $G_\infty := \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and, for each prime number p, $G_p := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. All of these are considered as subgroups of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, though this depends on choices of embeddings of $\overline{\mathbb{Q}}$ in $\mathbb{C}$ and the $\overline{\mathbb{Q}}_p$. Let I_p be the inertia subgroup at p. We define a Selmer group $H^1_{\mathcal{D}'}(\mathbb{Q}, W) := \{c \in H^1(\mathbb{Q}, W) | \, \mathrm{res}_p(c) \in L_p \ \forall \text{ primes } p \leq \infty\}$, where the subspaces $L_p \subset H^1(G_p, W)$ are defined as follows.

(1) $L_\infty := H^1(G_\infty, W)$. Its annihilator in $H^1(G_\infty, W^*)$ with respect to the local Tate duality pairing is $L_\infty^\perp = \{0\}$.
(2) Given a prime $p \mid N$, choose a basis $\{x, y\}$ for V with respect to which G_p acts via a matrix as in Lemma 4.1. Let $W^0 := \langle x \otimes x \rangle$ and
$$L_p := \ker(H^1(G_p, W) \to H^1(G_p, W/W^0)).$$
(3) At all finite primes $p \nmid N$ let $L_p = H^1(G_p/I_p, W^{I_p})$ (i.e. its image under inflation), and note that $L_p^\perp = H^1(G_p/I_p, (W^*)^{I_p})$.

Lemma 6.1. *Suppose that $p \mid N$.*

(1) *$L_p \simeq H^1(G_p, W^0)$;*
(2) *$\# L_p = 2^{2F}$ if $p \neq 2$;*
(3) *$\# L_2 = 2^{3F}$.*

Proof. Let $\{x, y\}$ be a basis for V as in Lemma 4.1. Take the cohomology, for G_p, of the exact sequence $0 \to W^0 \to W \to W/W^0 \to 0$. The H^0-part is exact. If we assume $\# \Phi_{A,p}$ is odd, and use Proposition 4.3, then it looks like this:
$$0 \to \langle x \otimes x \rangle \to \langle x \otimes x, x \otimes y + y \otimes x \rangle \to \langle [x \otimes y + y \otimes x] \rangle \to 0,$$
but it is exact even without that assumption. So
$$L_p \simeq H^1(G_p, W^0) \simeq \mathrm{Hom}(G_p, (\mathbb{F}_2)^F) \simeq (\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2)^F.$$
(Note that $W^0 \simeq \mathbb{F}_2^F$ as abelian groups.) Now $\dim_{\mathbb{F}_2}(\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2) = \begin{cases} 2 & \text{if } p \neq 2; \\ 3 & \text{if } p = 2. \end{cases}$ □

We have defined a Selmer group $H^1_{\mathcal{D}'}(\mathbb{Q}, W)$. We may similarly define a dual Selmer group $H^1_{\mathcal{D}'^*}(\mathbb{Q}, W^*)$ using the dual local conditions $L_v^\perp$, for all places v of $\mathbb{Q}$.

Lemma 6.2. *Assume the conditions of Proposition 4.2 (and that $E = 1$). Assume also that for each $p \mid N$, $\# \Phi_{A,p}$ is odd. Then $\# H^1_{\mathcal{D}'}(\mathbb{Q}, W) \geq \# H^1_{\mathcal{D}'^*}(\mathbb{Q}, W^*) \frac{2^F}{\# H^0(\mathbb{Q}, W^*)}$.*

(There is also a Tate twist by 1 attached to W^*, but it doesn't show up, since the cyclotomic character modulo 2 is trivial.)

Proof. By Theorem 2.18 of [DDT] (based on Proposition 1.6 of [Wi]),
$$\frac{\# H^1_{\mathcal{D}'}(\mathbb{Q}, W)}{\# H^1_{\mathcal{D}'^*}(\mathbb{Q}, W^*)} = \frac{\# H^0(\mathbb{Q}, W)}{\# H^0(\mathbb{Q}, W^*)} \prod_{\text{places of } \mathbb{Q}} \frac{\# L_v}{\# H^0(G_v, W)}.$$

Now $\#H^0(\mathbb{Q},W) \geq 2^F$ since it contains the $\mathbb{F}_\lambda$-subspace spanned by $x\otimes y + y\otimes x$, where $\{x,y\}$ is any $\mathbb{F}_\lambda$-basis for V. To see this, note that any element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts via some matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, with $a,b,c,d \in \mathbb{F}_\lambda$. This sends $x\otimes y + y\otimes x$ to $2acx\otimes x + 2bdy\otimes y + (ad+bc)(x\otimes y + y\otimes x) = (ad-bc)(x\otimes y + y\otimes x)$. Now $ad-bc=1$, since $\det\rho$ is the 2-adic cyclotomic character, which is trivial mod 2.

In the product we shall show that the contributions from 2 and ∞ cancel out, and that the contributions from all other places are trivial.

(1) For $p\nmid N\infty$, $\#L_p = \#H^1(G_p/I_p, W^{I_p}) = \#H^0(G_p,W)$.
(2) For $p \mid N$ with $p\neq 2$, we have $\#L_p = 2^{2F}$ by Lemma 6.1, but also $\#H^0(G_p,W) = 2^{2F}$, since $H^0(G_p,W)$ is spanned over $\mathbb{F}_\lambda$ by $\{x\otimes x, x\otimes y + y\otimes x\}$. This uses Proposition 4.3.
(3) $\#L_2 = 2^{3F}$, by Lemma 6.1, and $\#H^0(G_2,W) = \#\langle x\otimes x, x\otimes y + y\otimes x\rangle = 2^{2F}$ (again using Proposition 4.3), so $\frac{\#L_2}{\#H^0(G_2,W)} = 2^F$.
(4) Let $G_\infty = \langle\sigma\rangle$. Choose a basis $\{x,y\}$ for V such that σ acts as $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. (That we may do so follows from the assumption that $A(\mathbb{R})$ is connected.) Then $\#H^0(G_\infty,W) = \#\langle x\otimes x + y\otimes y, x\otimes y + y\otimes x\rangle = 2^{2F}$. If $f\in Z^1(G_\infty,W)$ (the group of 1-cocycles) then $f(\sigma^2)=0$ so $f(\sigma)+f(\sigma)^\sigma = 0$, so $f(\sigma)\in H^0(G_\infty,W) = \langle x\otimes x + y\otimes y, x\otimes y + y\otimes x\rangle$. Modding out by the coboundaries $(\sigma-1)W = \langle x\otimes x + y\otimes y\rangle$, we find that $\#H^1(G_\infty,W) = 2^F$ and $\frac{\#L_\infty}{\#H^0(G_\infty,W)} = \frac{1}{2^F}$.

□

Lemma 6.3. *Let $i : W \hookrightarrow V\otimes V$ (i.e. $i : \mathrm{ad}^0(V) \hookrightarrow \mathrm{ad}(V)$) be the inclusion. Then the kernel of $i_* : H^1(\mathbb{Q},\mathrm{ad}^0(V)) \to H^1(\mathbb{Q},\mathrm{ad}(V))$ is a 1-dimensional $\mathbb{F}_\lambda$-vector space. Moreover, it is contained in $H^1_{\mathcal{D}'}(\mathbb{Q},W)$.*

Proof. Consider the short exact sequence

$$0 \longrightarrow \mathrm{ad}^0(V) \longrightarrow \mathrm{ad}(V) \xrightarrow{\mathrm{tr}} \mathbb{F}_\lambda \longrightarrow 0.$$

Note that the Galois action on the $\mathbb{F}_\lambda$ is trivial, because the trace is invariant under conjugation. It is easy to see from (4) in the proof of the previous lemma that $H^0(G_\infty,W) = H^0(G_\infty, V\otimes V)$, from which it follows that $H^0(\mathbb{Q},W) = H^0(\mathbb{Q},V\otimes V)$, giving us the first part of this lemma. Take any element $M\in\mathrm{ad}(V)$ of non-zero trace (equivalently a non-symmetric element of $V\otimes V$). Then $\ker(i_*)$ is generated, as an $\mathbb{F}_\lambda$-vector space, by a class represented by the cocycle $\sigma\mapsto\sigma(M)-M$. Given a $p\mid N$, and a basis $\{x,y\}$ of V as above, we may adjust M by an element of $\mathrm{ad}^0(V)$ (only changing the cocycle by a coboundary) to get M to be a scalar multiple of $y\otimes x$. Then one sees easily that, for $\sigma\in G_p$, $\sigma(M)-M\in\langle x\otimes x\rangle = W^0$, as required. □

7. An application of the squaring map

We retain from earlier the assumptions

(1) N is even and square-free;
(2) $A[2](\mathbb{Q}) = \{O\}$;
(3) $A(\mathbb{R})$ is connected;
(4) $\#\Phi_{A,p}$ is odd for each prime $p\mid N$;

(5) $2 \nmid \mathrm{disc}(O_f)$.

We choose an i with $1 \le i \le t$, with $\lambda = \lambda_i$ of degree F. As above, $V = V_i = e_i(A[2])$, $W = \mathrm{Sym}^2 V$. We defined a Selmer group $H^1_{\mathcal{D}'}(\mathbb{Q}, W)$ and a dual Selmer group $H^1_{\mathcal{D}'^*}(\mathbb{Q}, W^*)$, and we proved an inequality relating their orders.

Applying e_i to the descent map, we get $\psi : e_i(A(\mathbb{Q})/2A(\mathbb{Q})) \hookrightarrow H^1(\mathbb{Q}, e_i(A[2])) \simeq H^1(\mathbb{Q}, V^*)$ (using the isomorphism $V \simeq V^*$). Then we have the squaring map $s : V^* \to W^*$, which squares linear functions to produce quadratic functions, and is $\mathbb{F}_2$-linear because squaring is additive in characteristic 2. It is also, by definition of the Galois action on W^* induced by that on V^*, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant. There is an induced map $s_* : H^1(\mathbb{Q}, V^*) \to H^1(\mathbb{Q}, W^*)$.

Lemma 7.1. *The kernel of s_* has size $\frac{2^F}{\#H^0(\mathbb{Q}, W^*)}$.*

Proof. Since $\#H^0(\mathbb{Q}, V^*) = \#A[2](\mathbb{Q}) = 1$, it suffices to show that $\#H^0(\mathbb{Q}, W^*/V^*) = 2^F$, i.e. that $H^0(\mathbb{Q}, W^*/V^*)$ is the whole of W^*/V^* (i.e. $W^*/s(V^*)$), spanned over $\mathbb{F}_\lambda$ by the image of xy. But this is true, because under $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, xy goes to $(ad+bc)xy + acx^2 + bdy^2 \equiv (ad-bc)xy$ in W^*/V^*, and, as already noted, $ad - bc = 1$. □

Proposition 7.2. *If $P \in A(\mathbb{Q})$ represents an element of $e_i(A(\mathbb{Q})/2A(\mathbb{Q}))$ then $s_*\psi(P) \in H^1_{\mathcal{D}'^*}(\mathbb{Q}, W^*)$.*

Proof. We need to check that $\mathrm{res}_v(s_*\psi(P)) \in L_v^\perp$ for all places v of $\mathbb{Q}$.

(1) It is well-known that $\psi(P)$ is unramified at all primes $p \nmid N\infty$. The same is then true for $s_*\psi(P)$.

(2) Let $G_\infty = \langle\sigma\rangle$, acting by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with respect to a chosen $\mathbb{F}_\lambda$-basis $\{x, y\}$ of V^*, as in the proof of Lemma 6.2. If $f \in Z^1(G_\infty, V^*)$ is a cocycle then, again as in the proof of Lemma 6.2, $f(\sigma) \in (V^*)^{G_\infty} = \langle x + y\rangle$. But $x + y = x^\sigma - x$, so $H^1(G_\infty, V^*) = \{0\}$. Necessarily then $\mathrm{res}_\infty(\psi(P)) = 0$, so $\mathrm{res}_\infty(s_*\psi(P)) \in L_\infty^\perp = \{0\}$.

(3) Now take a prime $p \mid N$. Looking at Lemma 3.3, P is represented by some $w \in \mathrm{Hom}(X_A, \overline{\mathbb{Q}}_p^\times)$ (determined up to multiplication by any element of $q(X_{A^\vee})$). If we choose $u \in \mathrm{Hom}(X_A, \overline{\mathbb{Q}}_p^\times)$ with $u^2 = w$, then, for any $\sigma \in G_p$, $\psi(P)(\sigma)$ is represented by u^σ/u. Here the division is in the image, and the action of G_p is simultaneously on X_A and $\overline{\mathbb{Q}}_p^\times$. Recall that on the former the action is unramified, with Frob_p acting as $a_p = -w_p$. Anyway, $(u^\sigma/u)^2 = w^\sigma/w \in q(X_{A^\vee})$, since P is fixed by G_p. Applying the valuation map, $v(w) = v(w^\sigma) \in \mathrm{Hom}(X_A, \mathbb{Z})$, so $v(w^\sigma/w) = 0$ (if $w_p = -1$) or $2v(w)$ (if $w_p = 1$). In the former case $w^\sigma/w = 1$ is the only possibility, while in the latter case the alternative is that $v(w)$ represents an element of order 2 in $\Phi_{A,p}$ (see the last part of Lemma 3.3), contrary to our assumption that $\Phi_{A,p}$ has odd order. Hence $(u^\sigma/u)^2 = 1$, so $\psi(P)(\sigma) \in e_i\mathrm{Hom}(X_A, \mu_2) = \langle x\rangle$, and $s_*\psi(P)(\sigma) \in \langle x^2\rangle$. It follows from Lemma 5.2 that $\mathrm{res}_p(s_*\psi(P))$ kills $H^1(G_p, W^0)$ under the local Tate duality pairing, hence that $\mathrm{res}_p(s_*\psi(P)) \in L_p^\perp$.

□

Corollary 7.3. *Assume the conditions (1)-(5) listed at the beginning of this section.*

(1) $\#H^1_{\mathcal{D}'}(\mathbb{Q}, W) \geq 2^{F_i r}$, *where* $r = \dim_K(A(\mathbb{Q}) \otimes \mathbb{Q}) = \frac{1}{d}\operatorname{rank}_{\mathbb{Z}} A(\mathbb{Q})$.
(2) *In fact,* $\#H^1_{\mathcal{D}'}(\mathbb{Q}, W)$ *is at least the size of the* e_i *part of the Selmer group for multiplication by* 2 *on* $A/\mathbb{Q}$.

To get (1), simply combine Lemmas 6.2, 7.1 and Proposition 7.2, noting that $\#e_i(A(\mathbb{Q})/2A(\mathbb{Q})) = 2^{F_i r}$. To get (2), observe that the proof of Proposition 7.2 only depends on the element of $H^1(\mathbb{Q}, V^*)$ being everywhere locally the image of a rational point.

8. A deformation problem

Again, we retain the assumptions (1)-(5) of the previous section. We have chosen an i with $1 \leq i \leq t$, with $\lambda = \lambda_i$ of degree F. As above, $V = V_i = e_i(A[2])$, $W = \operatorname{Sym}^2 V \simeq \operatorname{ad}^0(V)$ as an $\mathbb{F}_\lambda[\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module. We have the representation $\overline{\rho}$ of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on V, a 2-dimensional $\mathbb{F}_\lambda$-vector space.

Let $\mathcal{C}$ be the category whose objects are complete noetherian local O_λ-algebras with residue field $\mathbb{F}_\lambda$, and whose morphisms are local O_λ-algebra homomorphisms. If we choose any basis for V then we have $\overline{\rho} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\mathbb{F}_\lambda)$. If $\mathcal{R} \in \mathcal{C}$, a lifting $\rho : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{R})$ is said to be of type $\mathcal{D}$ if and only if the following conditions hold:

(1) ρ is unramified outside N;
(2) For any prime $p \mid N$, $\rho|_{G_p} \sim \begin{pmatrix} \omega\chi^{-1} & * \\ 0 & \chi \end{pmatrix}$, where ω is the restriction of the 2-adic cyclotomic character, and χ is any unramified character (not fixed);
(3) $\det \rho = \omega$.

Proposition 8.1. *There is a universal coefficient ring* $\mathcal{R}_{\mathcal{D}}$ *and a universal deformation of* $\overline{\rho}$ *of type* $\mathcal{D}$*:*

$$\rho^{\text{univ}}_{\mathcal{D}} : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(\mathcal{R}_{\mathcal{D}})$$

(see §§8 and 10 of [Ma] *for precise definitions).*

Proof. The existence of a universal ring for deformations of $\overline{\rho}$ subject only to the condition (1) above follows from Proposition 2 in §20 of [Ma]. Note that $\overline{\rho}$ is absolutely irreducible, by Proposition 4.2. The determinant condition (3) is handled by §24 of [Ma]. For $p \neq 2$, that (2) is a deformation condition is part of the proposition in §29 of [Ma]. It may be proved in the same way even for $p = 2$, replacing the γ in Lemma 1 of §29 of [Ma] (a topological generator of the 2-part of the tame quotient of I_p) by an element as in Proposition 4.3. □

Let $\rho : \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \operatorname{GL}_2(O_\lambda)$ be the lifting of $\overline{\rho}$ arising from the action of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $T_\lambda(A)$ (with a chosen O_λ-basis lifting the chosen $\mathbb{F}_\lambda$-basis of V). This is obtained (up to strict equivalence) from $\rho_{\mathcal{D}}$ by composing with some homomorphism $\pi_{\mathcal{R}} : \mathcal{R}_{\mathcal{D}} \to O_\lambda$. Let $\mathcal{P}_{\mathcal{R}} := \ker(\pi_{\mathcal{R}})$.

Recall that A is associated to a particular $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbit of newforms for $\Gamma_0(N)$, represented by f. Forms in the same orbit have the same sequence (w_p) of eigenvalues for the Atkin-Lehner involutions. Fixing an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_2$, each newform for $\Gamma_0(N)$ may be considered to have coefficients in $\overline{\mathbb{Q}}_2$, and each $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbit may be subdivided into G_2-orbits, where $G_2 := \operatorname{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$. Now let g be any newform for $\Gamma_0(N)$ and, for some fixed ordering of the s primes $p \mid N$, consider

the vector $v(g) := ((w_p(g) - w_p(f))/2)_{p|N} \in \mathbb{F}_2^s$. It has a 1 where $w_p(g) \neq w_p(f)$, zeroes elsewhere. Now consider only those g such that all the Hecke eigenvalues of g lie in an unramified extension of $\mathbb{Q}_2$ and become congruent $\pmod 2$ to those of f, i.e. the same in $\overline{\mathbb{F}}_2$. (There will be at most one such g in each G_2-orbit.) Define a matrix B whose rows are the $v(g)$, for all such g. Let k be the rank of B. Note that $k \leq s$, the number of primes dividing N.

Proposition 8.2.

$$\#\mathrm{Hom}_{O_\lambda}(\mathcal{P}_\mathcal{R}/\mathcal{P}_\mathcal{R}^2, \mathbb{F}_\lambda) \geq 2^{F(r-1+k)}.$$

It is only because $\ell = 2$ that we can have congruences between newforms with different Atkin-Lehner eigenvalues.

Proof. Corollary 7.3 tells us that $\#H^1_{\mathcal{D}'}(\mathbb{Q}, W) \geq 2^{Fr}$. Given a cocycle c representing an element of $H^1_{\mathcal{D}'}(\mathbb{Q}, W) = H^1_{\mathcal{D}'}(\mathbb{Q}, \mathrm{ad}^0(V))$, in the standard way we may produce a representation $\rho_c : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\lambda[\epsilon])$ (where $\epsilon^2 = 0$), by putting $\rho_c(\sigma) = \overline{\rho}(\sigma)(I + c(\sigma)\epsilon)$, for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. This lifts $\overline{\rho}$, is unramified at $p \nmid N$ (since $\overline{\rho}$ and c are) and has the same determinant as $\overline{\rho}$ (since $c(\sigma)$ has trace 0). Thus the conditions (1) and (3) are satisfied. At $p \mid N$, choosing a basis $\{x, y\}$ for V as in the proof of Lemma 6.1, the image of c is contained in $W^0 = \langle x \otimes x \rangle$ which, under the isomorphism $W \simeq \mathrm{ad}^0(V)$, corresponds to $\begin{pmatrix} 0 & * \\ 0 & 0 \end{pmatrix}$, using Lemma 5.1. Hence the diagonal entries for $\rho_c(\sigma)$ are the same as those for $\overline{\rho}(\sigma)$, for any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, so the condition (2) is satisfied, in fact for each $p \mid N$ it is the *same* unramified character χ for both $\overline{\rho}$ and ρ_c. (Actually, $H^1_{\mathcal{D}'}(\mathbb{Q}, W)$ maps to the reduced cotangent space for a deformation problem $\mathcal{D}'$ with stronger local conditions, where the unramified characters for each $p \mid N$ are fixed.)

By the universal property, there is an O_λ-linear homomorphism $\theta_c : \mathcal{R}_\mathcal{D} \to \mathbb{F}_\lambda[\epsilon]$ inducing ρ_c. Looking at the coefficient of ϵ gives an element $\phi_c \in \mathrm{Hom}_{O_\lambda}(\mathcal{P}_\mathcal{R}/\mathcal{P}_\mathcal{R}^2, \mathbb{F}_\lambda)$. Let $i_* : H^1(\mathbb{Q}, \mathrm{ad}^0(V)) \to H^1(\mathbb{Q}, \mathrm{ad}(V))$ be the map induced by the inclusion $i : \mathrm{ad}^0(V) \hookrightarrow \mathrm{ad}(V)$. By a standard argument, the group homomorphism $i_*(H^1_{\mathcal{D}'}(\mathbb{Q}, W)) \to \mathrm{Hom}_{O_\lambda}(\mathcal{P}_\mathcal{R}/\mathcal{P}_\mathcal{R}^2, \mathbb{F}_\lambda)$ given by $i_*[c] \mapsto \phi_c$ is an injection. But, as pointed out by the referee, and proved in Lemma 6.3 above, i_* has a non-trivial kernel, which is even contained in $H^1_{\mathcal{D}'}(\mathbb{Q}, W)$. So we can deduce only that $\#\mathrm{Hom}_{O_\lambda}(\mathcal{P}_\mathcal{R}/\mathcal{P}_\mathcal{R}^2, \mathbb{F}_\lambda) \geq 2^{F(r-1)}$.

Now, as above, consider g such that all the Hecke eigenvalues of g lie in an unramified extension of $\mathbb{Q}_2$ and become congruent $\pmod 2$ to those of f. Then there is a representation $\rho_g : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(O_g)$ lifting $\overline{\rho}$, where O_g is the ring of integers in the finite extension of $\mathbb{Q}_2$ generated by the $a_p(g)$, which must in fact be the unique unramified extension with residue field $\mathbb{F}_\lambda$, in particular $O_g \simeq O_\lambda$. This ρ_g is a lifting of type $\mathcal{D}$, for the same reason that $\rho_f = \rho_\lambda$ is (see Lemma 4.1). Hence there is a corresponding local O_λ-algebra homomorphism $\theta_g : \mathcal{R}_\mathcal{D} \to O_g$. If $R \in \mathcal{P}_\mathcal{R}$ then $\theta_f(R) = \pi_\mathcal{R}(R) = 0$, so $\theta_g(R) \in \lambda O_g$. (This uses the assumption that the Hecke eigenvalues of g lie in an unramified extension of $\mathbb{Q}_2$, not just that they have the same images in $\overline{\mathbb{F}}_2$ as those of f.) We can define an element ϕ_g of $\mathrm{Hom}_{O_\lambda}(\mathcal{P}_\mathcal{R}/\mathcal{P}_\mathcal{R}^2, \mathbb{F}_\lambda)$ by $R \mapsto (\theta_g(R)/2) \pmod{\lambda O_g}$. (Recall that 2 is unramified in O_λ, so 2 is a uniformising element for λ.)

For each $p \mid N$, we have $\rho_g|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} \sim \begin{pmatrix} \omega\chi_{g,p}^{-1} & * \\ 0 & \chi_{g,p} \end{pmatrix}$, with $\chi_{g,p}$ an unramified character such that $\chi_{g,p}(\mathrm{Frob}_p) = -w_p(g)$. Let $\chi^{\mathrm{univ}}_{\mathcal{D},p}$ be the analogous character

for the universal representation, and define $R_p = w_p(f) + \chi^{\mathrm{univ}}_{\mathcal{D},p}(\mathrm{Frob}_p)$. Then $R_p \in \mathcal{P}_{\mathcal{R}}$ and $\phi_g(R_p) = (w_p(f) - w_p(g))/2$. If an $\mathbb{F}_\lambda$-linear combination of the vectors $(\phi_g(R_p))_{p|N}$ is non-zero, then so is the corresponding linear combination of the ϕ_g. For $[c] \in H^1_{\mathcal{D}'}(\mathbb{Q}, W)$, $(\phi_c(R_p))_{p|N}$ is the zero vector, since $\overline{\rho}|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$ and $\rho_c|_{\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)}$ have the same diagonal entries, as already noted. The $(\phi_g(R_p))_{p|N}$ are the rows of the matrix B. Therefore, to the $r-1$ we already had from $H^1_{\mathcal{D}'}(\mathbb{Q}, W)$, we can add a further k to the $\mathbb{F}_\lambda$-dimension of $\mathrm{Hom}_{O_\lambda}(\mathcal{P}_{\mathcal{R}}/\mathcal{P}^2_{\mathcal{R}}, \mathbb{F}_\lambda)$. □

Remark. In [Du], the first-named author (in the elliptic curve case) asserted that for odd $p \mid N$ the local subgroups L_p, defining a Selmer group $H^1_{\mathcal{D}}(\mathbb{Q}, W)$ that maps onto $\mathrm{Hom}_{O_\lambda}(\mathcal{P}_{\mathcal{R}}/\mathcal{P}^2_{\mathcal{R}}, \mathbb{F}_\lambda)$, are $H^1(G_p/I_p, W^{I_p})$, i.e. $\ker(H^1(G_p, \mathrm{ad}^0(V)) \to H^1(I_p, \mathrm{ad}^0(V)))$. In fact it should be $\ker(H^1(G_p, \mathrm{ad}^0(V)) \to H^1(I_p, \mathrm{ad}(V)))$. (See Proposition 3 in §26 of [Ma].) There would be no difference in odd residue characteristic, where the matrix n at the end of §29 of [Ma] can be replaced by $\begin{pmatrix} b/2 & * \\ -a & -b/2 \end{pmatrix} \in \mathrm{ad}^0(V)$, but here where $\ell = 2$ we cannot do this.

9. Hecke rings and the modular degree

Let $\mathbb{T} = \mathbb{T}_{\mathbb{Z}}$ be as in the introduction. Let $\overline{\psi}_f : \mathbb{T} \to \mathbb{F}_\lambda$ be the homomorphism determined by $T_p \mapsto a_p(f) \pmod{\lambda}, U_p \mapsto a_p(f) \pmod{\lambda}$, and let $\mathfrak{m}$ be the maximal ideal of $\mathbb{T}$ that is the kernel of $\overline{\psi}_f$. For g as in the previous section, the same $\mathfrak{m}$ is also the kernel of a similarly defined $\overline{\psi}_g$. We denote also by $\mathfrak{m}$ the ideal generated by the image of $\mathfrak{m}$ in $\mathbb{T} \otimes \mathbb{Z}_2$. The localisation or completion $\mathbb{T}_{\mathfrak{m}}$ is a direct summand of $\mathbb{T} \otimes \mathbb{Z}_2$. It is isomorphic to the subring of $\prod_g O_g$ generated by the $(a_p(g))_g$, where p runs over all primes. (Note that it follows from the oddness of the $\#\Phi_{A,p}$ that N is the minimal level for modular liftings of $\overline{\rho}$, c.f. Proposition 4.3, so no newforms of level strictly dividing N appear in this product.) Now the product is over G_2-orbits of g such that all $a_p(f)$ and $a_p(g)$ become the same in $\overline{\mathbb{F}}_2$, but without the earlier condition about the $a_p(g)$ lying in an unramified extension of $\mathbb{Q}_2$. Equivalently, g and f have isomorphic residual representations. Although O_g is no longer necessarily isomorphic to O_λ, it is an O_λ algebra, since the congruence forces it to have the same residue field $\mathbb{F}_\lambda$, and O_λ is the ring of integers in the unique unramified extension of $\mathbb{Q}_2$ with that residue field.

Lemma 9.1. *The localisation $T_2(J_0(N))_{\mathfrak{m}}$ of the 2-adic Tate module of $J_0(N)$ is free of rank 2 over $\mathbb{T}_{\mathfrak{m}}$.*

This follows from Proposition 2.4 of [Bz]. Note that because $\#\Phi_{A,2}$ is odd, the proof of Proposition 4.3 shows that $\overline{\rho}|_{G_2}$ is trés ramifié, hence by Proposition 8.2 of [Ed] that $\overline{\rho}$ is not finite at 2. Furthermore, $\overline{\rho}(\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2))$ is not contained in the scalar matrices, by Proposition 4.3.

The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $T_2(J_0(N))_{\mathfrak{m}}$ gives a representation $\rho_{\mathbb{T}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{T}_{\mathfrak{m}})$, lifting $\overline{\rho}$. We can obtain from it each representation ρ_g by composing with $\psi_g : \mathbb{T}_{\mathfrak{m}} \to O_g$ such that $T_p \mapsto a_p(g), U_p \mapsto a_p(g)$. Given also how $\mathbb{T}_{\mathfrak{m}}$ is a subring of $\prod_g O_g$, we may deduce from the fact that each ρ_g is of type $\mathcal{D}$ that so is $\rho_{\mathbb{T}}$. Hence $\rho_{\mathbb{T}}$ arises from $\rho^{\mathrm{univ}}_{\mathcal{D}}$ via an O_λ-algebra homomorphism $\theta : \mathcal{R}_{\mathcal{D}} \to \mathbb{T}_{\mathfrak{m}}$.

Hypothesis 9.2. *θ is an isomorphism and $\mathcal{R}_{\mathcal{D}} \simeq \mathbb{T}_{\mathfrak{m}}$ is a local complete intersection.*

Let $\mathcal{P}_{\mathbb{T}}$ be the kernel of $\psi_f : \mathbb{T}_{\mathfrak{m}} \to O_\lambda$. Let $I = \mathrm{Ann}_{\mathbb{T}_{\mathfrak{m}}}(\mathcal{P}_{\mathbb{T}})$ and $\eta = \psi_f(I)$. As in §4.4. of [DDT], η is non-zero, and $O_\lambda/\eta \simeq \mathbb{T}_{\mathfrak{m}}/(\mathcal{P}_{\mathbb{T}} + I)$.

Lemma 9.3. *Let I_f be the ideal of $\mathbb{T}$ described in the introduction, so $\mathbb{T}/I_f \simeq O_f$. Suppose that $2 \nmid [O_K : O_f]$. Viewing $\mathbb{T}_{\mathfrak{m}}$ as a subring of $\mathbb{T} \otimes \mathbb{Z}_2$, $\mathcal{P}_{\mathbb{T}} \subseteq I_f \otimes \mathbb{Z}_2$.*

Proof. Among the G_2-orbits into which the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbit of f breaks up, only that of f is involved in the product $\prod_g O_g$ into which $\mathbb{T}_{\mathfrak{m}}$ embeds. If this were not the case then $O_f \otimes \mathbb{Z}_2$, mapped to $\sum_{i=1}^t O_{\lambda_i}$, would land in a subring defined by a condition that the entries in two specific positions are the same in the residue field (like all the entries in $\mathbb{T}_{\mathfrak{m}} \subseteq \prod_g O_g$), contrary to $2 \nmid [O_K : O_f]$. Hence any element of $\mathcal{P}_{\mathbb{T}}$ is not only in the kernel of the homomorphism $\psi_f : \mathbb{T}_{\mathfrak{m}} \to O_\lambda$, but also in the kernel of the extended $\theta_f : \mathbb{T} \otimes \mathbb{Z}_2 \to O_K \otimes \mathbb{Z}_2$, which is $I_f \otimes \mathbb{Z}_2$. □

Theorem 9.4. *Assume the conditions (1)-(5) from the introduction (repeated at the beginning of Section 7). Let $r = \dim_K(A(\mathbb{Q}) \otimes \mathbb{Q})$ and $k_i = k$ as in Proposition 8.2. Then, assuming Hypothesis 9.2, $2^{2F(r-1+k_i)}$ divides the order of $e_i(\ker(\pi \circ \pi^\vee))$.*

If $r = 0$ then $r - 1$ should be replaced by 0.

Proof. By Theorem 5.3 of [DDT], Hypothesis 9.2 is equivalent to $\#(\mathcal{P}_{\mathcal{R}}/\mathcal{P}_{\mathcal{R}}^2) = \#(O_\lambda/\eta)$. Then by Proposition 8.2, $2^{F(r-1+k_i)}$ divides $\#(O_\lambda/\eta)$, so λ^{r-1+k_i} divides η. Recall that 2 is a uniformiser for λ, so equivalently 2^{r-1+k_i} divides η, and $\eta = (2^S)$ for some $S \geq r - 1 + k_i$.

Let I_f be the ideal of $\mathbb{T}$ defined in the introduction, and let $S' \geq S$ be such that $2^{S'-S}$ kills any 2-torsion in the quotient by $\pi^\vee(A^\vee)$ of the kernel of I_f on $J_0(N)$. Since $O_\lambda/\eta \simeq \mathbb{T}_{\mathfrak{m}}/(\mathcal{P}_{\mathbb{T}} + I)$, we may write $2^S = p + i$, with $p \in \mathcal{P}_{\mathbb{T}}$, $i \in I$ and $2 \nmid i$ in $\mathbb{T}_{\mathfrak{m}}$. As vectors, $i = (2^S, 0, \ldots, 0)$ and $p = (0, 2^S, \ldots, 2^S)$.

By Lemma 9.1, $T_2(J_0(N))_{\mathfrak{m}}$ projects to a subgroup G of $J_0(N)[2^{S'}]$ isomorphic to $(\mathbb{T}_{\mathfrak{m}}/2^{S'})^2$. (It may help to think of $\mathbb{T}_{\mathfrak{m}}$ just as a free $\mathbb{Z}_2$-module.) Let $\{g_1, g_2\}$ be a $(\mathbb{T}_{\mathfrak{m}}/2^{S'})$-basis for G. Since I annihilates $\mathcal{P}_{\mathbb{T}}$, $\mathcal{P}_{\mathbb{T}}$ kills $i(G)$, so $\mathbb{T}_{\mathfrak{m}}$ acts on $i(G)$ through $\mathbb{T}_{\mathfrak{m}}/\mathcal{P}_{\mathbb{T}} \simeq O_\lambda$. It follows from the fact that $2 \nmid i$ in $\mathbb{T}_{\mathfrak{m}}$ that ig_1 and ig_2 are linearly independent over $O_\lambda/2^{S'}$, so $i(G)$ is free of rank 2 over $O_\lambda/2^{S'}$. Extending $\theta_f : \mathbb{T} \to O_K$ to $\theta_f : \mathbb{T} \otimes \mathbb{Z}_2 \to O_K \otimes \mathbb{Z}_2$, since $e_i \circ \theta_f : \mathbb{T} \to O_\lambda$ factors through $\psi_f : \mathbb{T}_{\mathfrak{m}} \to O_\lambda$, if $t \in I_f$ then the image of t in $\mathbb{T}_{\mathfrak{m}}$ is in $\mathcal{P}_{\mathbb{T}}$, so kills $i(G)$. Hence $i(2^{S'-S}G)$, which is isomorphic to $(O_\lambda/2^S)^2 \simeq (O_\lambda/\eta)^2$, lies in $\pi^\vee(A^\vee)$. Moreover, if $P \in i(2^{S'-S}G)$, say $P = i(Q)$, then, recalling that $2^S = p + i$, $P = i(Q) = 2^S Q - pQ = -pQ$. Since, by Lemma 9.3 $p \in \mathcal{P}_{\mathbb{T}} \subseteq \mathbb{T}_{\mathfrak{m}}$ may be 2-adically approximated by some $t \in I_f$ that acts the same way on Q, we see that $P \in I_f J_0(N)$, so $P \in \ker \pi$. Hence $i(2^{S'-S}G)$, viewed as a subgroup of $A^\vee$ via the injection $\pi^\vee : A^\vee \to J_0(N)$, is inside $\ker(\pi \circ \pi^\vee)$. As already noted, $e_i \circ \theta_f : \mathbb{T} \to O_\lambda$ factors through $\psi_f : \mathbb{T}_{\mathfrak{m}} \to O_\lambda$, so in fact $i(2^{S'-S}G)$ is inside the image of $e_i(\ker(\pi \circ \pi^\vee))$. Since $i(2^{S'-S}G)$ has order $2^{2S} \geq 2^{2F(r+k_i)}$, the proposition follows. □

Putting together the different contributions for $1 \leq i \leq t$, we get the following.

Corollary 9.5. *Assume the conditions (1)-(5) from the introduction (repeated at the beginning of Section 7), and also Hypothesis 9.2. Then the modular degree of A is divisible by $2^{R-d+\sum F_i k_i}$, where $R = \mathrm{rank}(A(\mathbb{Q}))$ and k_i is as in Proposition 8.2.*

If $R = 0$ then $R - d$ should be replaced by 0. As in Corollary 7.3(2), the factor 2^R may be replaced by the order of the 2-Selmer group for A. Note that $2^{R-d+\sum F_i k_i} \leq 2^{R-d+ds} = 2^{d(r-1+s)}$, where s is the number of prime factors of N.

By Corollary 5.20 and Theorem 5.27 of [DDT], $\#(\mathcal{P}_{\mathbb{T}}/\mathcal{P}_{\mathbb{T}}^2) = \#(O_\lambda/\eta)$ is equivalent to $\mathbb{T}_{\mathfrak{m}}$ being a local complete intersection. In Proposition 8.2 we may replace $\mathcal{P}_{\mathcal{R}}/\mathcal{P}_{\mathcal{R}}^2$ by $\mathcal{P}_{\mathbb{T}}/\mathcal{P}_{\mathbb{T}}^2$ if we delete the $r-1$. In the proof we simply replace the element $R_p = w_p(f) + \chi_{\mathcal{D},p}^{\mathrm{univ}}(\mathrm{Frob}_p)$ of $\mathcal{P}_{\mathcal{R}}$ by the element $w_p(f) + U_p$ of $\mathcal{P}_{\mathbb{T}}$. Then, repeating the proof of Theorem 9.4, we obtain the following.

Proposition 9.6. *Assume the conditions (1)–(5) of the introduction (except we don't need to assume that $\#\Phi_{A,p}$ is odd for odd p). If $\mathbb{T}_{\mathfrak{m}}$ is a local complete intersection, then the modular degree of A is divisible by $2^{\sum F_i k_i}$.*

The reason that we cannot dispense with conditions (2) and (3) is that Proposition 2.4 of [Bz] relies on the irreducibility of $\overline{\rho}$, which we get from Proposition 4.2.

10. Examples

The conditions (1)–(5) are chosen to make life easy. In this section we show that they are not so strong as to make it impossible to find examples. We have repeatedly used Sturm's bound [Stu]: if newforms f and g of weight κ for $\Gamma_0(N)$ have Hecke eigenvalues $a_n(f) \equiv b_n(f) \pmod{\lambda}$ for all $n \leq \frac{\kappa N}{12} \prod_{p|N} \left(1 + \frac{1}{p}\right)$, then $a_n(f) \equiv b_n(f) \pmod{\lambda}$ for all n. The data in Stein's table "q-expansions of eigenforms on $\Gamma_0(N)$" [Ste] goes far enough to confirm that apparent congruences really hold.

10.1. **Elliptic curves.** For $d = 1$, the optimal elliptic curves with $N \leq 250$ satisfying conditions (1)–(5) (of which condition (5) is automatic), and of rank $R = 0$, are 26a1, 26b1, 38a1, 38b1, 106a1, 106d1, 110a1, 110b1, 110c1, 118c1, 118d1, 170c1, 170d1, 170e1, 174a1, 174b1, 174c1, 174e1, 182b1, 182c1, 182d1, 182e1, 186a1, 186b1, 186c1, 202a1, 222a1, 222b1, 222d1, 222e1, 246a1, 246b1, 246f1, 246g1 (as listed in [Cr1]). Note that if the conditions hold for an elliptic curve then they hold for any isogenous elliptic curve, since the irreducibility of $\overline{\rho}$ rules out rational 2-isogenies. Recall that $E(\mathbb{R})$ is connected if and only if $\Delta < 0$, and that, for $p \,||\, N$, $\#\Phi_{E,p}$ is the exponent of p in Δ. For 26a1: $y^2 + xy + y = x^3 - 5x - 8$ (for which $\#E(\mathbb{Q})_{\mathrm{tors}} = 3$ and $\Delta = -2^3 13^3$) and 26b1: $y^2 + xy + y = x^3 - x^2 - 3x + 3$ (for which $\#E(\mathbb{Q})_{\mathrm{tors}} = 7$ and $\Delta = -2^7 13$), we have $(w_2, w_{13}) = (1, -1)$ and $(-1, 1)$, respectively. For either 26a1 or 26b1, $B = [1, 1]$ so $k = 1$. There are no other newforms of level 26, and the Hecke eigenvalues for 26a1 and 26b1 are congruent mod 2 but not mod 4. It follows that $\mathbb{T}_{\mathfrak{m}} \simeq \mathbb{Z}_2[[X]]/(X(X-2))$, where in $\prod_g O_g$, X is $(0, 2)$. This is a local complete intersection. Also $\#W' = 2$. Both Proposition 9.6 and Proposition 2.1 give $2 \mid m$. In fact the modular degrees are both 2. The conductor 38 examples are similar (with modular degrees 6 and 2).

The optimal elliptic curves with $N \leq 1000$ satisfying conditions (1)–(5), and of rank $R = 1$, are 214a1, 214b1, 262a1, 302a1, 302c1, 362a1, 362b1, 430b1, 430c1, 430d1, 542b1, 618c1, 618e1, 618f1, 622a1, 670a1, 670c1, 670d1, 706b1, 794c1, 814a1, 814b1, 886e1, 890d1, 890f1, 890g1, 974e1. We consider a few of these in more detail.

The elliptic curve 214b1: $A : y^2 + xy + y = x^3 + x$ has $R = 1$, $A(\mathbb{Q})_{\mathrm{tors}} = \{O\}$, $N = 214 = 2 \cdot 107$, and minimal discriminant $\Delta = -2 \cdot 107$. Since $\Delta < 0$, $A(\mathbb{R})$ is connected, and $\#\Phi_{A,2} = \#\Phi_{A,107} = 1$, the exponents in Δ. We have

$w_2 = w_{107} = 1$, so $\#W' = 2^2$, and Proposition 2.1 gives $2^2 \mid m$, the modular degree. In fact, $m = 2^2 \cdot 3$.

The elliptic curve 214a1, $y^2 + xy = x^3 - 12x + 16$, has the same residual mod 2 Galois representation as 214b1, and has $w_2 = w_{107} = -1$, contributing a row $[1, 1]$ to the matrix B. There are also two 2-dimensional modular abelian varieties of conductor 214 with the same residual mod 2 representation, which would have contributed rows $[0, 1]$ and $[1, 0]$, but they don't count, since 2 is ramified in the coefficient field $\mathbb{Q}(\sqrt{3})$. Hence $k = 1$, and Proposition 9.6 predicts only $2 \mid m$. The example 262b1 is similar. Since $R - d = 0$, Corollary 9.5 does not improve on this.

The elliptic curve 430b1 has $(w_2, w_5, w_{43}) = (1, -1, -1)$, so $\#W' = 2^2$, and Proposition 2.1 gives $2^2 \mid m$. Its Hecke eigenvalues are congruent mod 2 to those of 430c1 and 430d1, which have $(w_2, w_5, w_{43}) = (-1, 1, -1)$ and $(-1, -1, 1)$ respectively, contributing rows $[1, 1, 0]$ and $[1, 0, 1]$ to the matrix B. In fact this is the whole of B, so $k = 2$. (There are two 2-dimensional modular abelian varieties of conductor 430 with the same residual mod 2 representation, but 2 is ramified in their coefficient fields.) Proposition 9.6 also predicts that $2^2 \mid m$, and in fact $m = 2^3 \cdot 5$. (The curves 430c1 and 430d1 also have $2^3 \mid m$, and could just as well have been used as the example.) Again, $R = 1$ and Corollary 9.5 does not predict anything stronger.

10.2. **An elliptic curve of rank 2.** In all the examples so far, $r = 0$ or 1, so Corollary 9.5 adds nothing to Proposition 9.6. The same is true of the examples in the next subsection with $d > 1$. So it seems worthwhile to produce an example of an elliptic curve with $r = 2$ satisfying the conditions (1)–(5). Such an elliptic curve is 2038a1, $y^2 + xy = x^3 - 10x + 36$, for which $\Delta = -2^9 \cdot 1019$. Using Stein's tables, the other newforms of this conductor have coefficient fields of degrees, $2, 14, 20, 22$ and 25. Factoring the minimal polynomials of generating elements modulo a high power of 2 shows that in each field, 2 has no unramified prime factors of degree 1, and consequently $k = 0$, and Corollary 9.5 suggests $2^{r-1} = 2 \mid m$. On the other hand, $(w_2, w_{1089}) = (-1, 1)$, so $\#W' = 2$, and Corollary 12.3 below suggests $2^2 \mid m$. In fact, $m = 720 = 2^4 \cdot 3^2 \cdot 5$.

10.3. **Higher dimensional modular abelian varieties.** There is no shortage of modular abelian varieties of dimension $d \geq 2$ satisfying conditions (1)–(5). Listed by (N, d), those with $N \leq 400$ are $(74, 2), (74, 2), (86, 2), (86, 2), (122, 2), (134, 3), (134, 3), (206, 2), (206, 2), (218, 2), (266, 2), (266, 2), (266, 2), (278, 3), (290, 2), (290, 2), (314, 6), (326, 5), (334, 2), (334, 2), (334, 2), (358, 2), (358, 2), (358, 2), (374, 3), (374, 3), (382, 3), (382, 3), (386, 2), (386, 2)$. These were found using the computer packages SAGE and Magma. Further along, the example $(554, 8)$ is noteworthy.

For the two examples with $N = 74$ and $d = 2$, we have $(w_2, w_{37}) = (1, -1)$ and $(-1, 1)$. The coefficient fields are $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{13})$, in both of which 2 is inert, and the Hecke eigenvalues become equal in $\mathbb{F}_4$. We have $B = [1, 1]$ so $k = 1$. It is easy to see that $\mathbb{T}_{\mathfrak{m}}$ is a local complete intersection, because the Hecke eigenvalues are congruent mod 2 but not mod 4, and there are no other newforms of conductor N, so $\mathbb{T}_{\mathfrak{m}} \simeq W(\mathbb{F}_4)[[X]]/(X(X-2))$, where $W(\mathbb{F}_4)$ is the ring of integers in the unramified extension of $\mathbb{Q}_2$ of degree 2. Also $\#W' = 2$. Corollary 9.5 (or Proposition 9.6) and Proposition 2.1 both give $2^2 \mid m$. The modular degrees are in fact $12 = 2^2 \cdot 3$ and $20 = 2^2 \cdot 5$. The examples of conductor 86 are similar (except the modular degrees are 4 and 8).

There is a 2-dimensional abelian variety with $N = 334 = 2 \cdot 167$ and $(w_2, w_{167}) = (1, 1)$. Notations differ, but let's call it 334B. There is another 2-dimensional abelian variety (let's say 334D) with $N = 334 = 2 \cdot 167$, but $(w_2, w_{167}) = (-1, -1)$. They are the modular abelian varieties with smallest conductor such that $d \geq 2$ and $\epsilon = -1$. Both have coefficient field $\mathbb{Q}(\sqrt{5})$, in which 2 is inert. Their Hecke eigenvalues are congruent in $\mathbb{F}_4$, and in fact for either we have $B = [1, 1]$ so $k = 1$. Clearly N is even and square-free. Using SAGE we checked that $A[2](\mathbb{Q}) = \{O\}$ and $A(\mathbb{R})$ is connected, and that $\#\Phi_{A,p}$ is odd for each prime $p \mid N$. (For 334B we have $\#\Phi_{A,2} = 5$ and $\#\Phi_{A,167} = 1$, while for 334D we have $\#\Phi_{A,2} = 99$ and $\#\Phi_{A,167} = 1$.) Finally, using Stein's table, O_f is the full ring of integers in $\mathbb{Q}(\sqrt{5})$, so all the conditions (1)–(5) of the introduction are satisfied. Hence Proposition 9.6 predicts that $2^2 \mid m$. Using Stein's tables or Magma, one finds that for 334B $m = 2^4 \cdot 5$, while for 334D $m = 2^4 \cdot 3^2 \cdot 11$. The sign $\epsilon = -1$, and using Magma ("leading coefficient" command for the L-series of a modular abelian variety) one checks that the order of vanishing of $L(A, s)$ at $s = 1$ is precisely d. It then follows from the theorem of Gross-Zagier [GZ] that $r \geq 1$. (In fact, as noted in the penultimate paragraph of [G], Kolyvagin's method then shows that $r = 1$.) So as in §10.1 (and also in the examples below), Corollary 9.5 does not predict anything stronger than Proposition 9.6.

There are three 3-dimensional modular abelian varieties with $N = 422 = 2 \cdot 211$, and $(w_2, w_{211}) = (1, 1), (-1, -1)$ and $(1, -1)$. Call them 422C, 422E and 422D respectively. For the first two of these $\epsilon = -1$, and Magma gives $\mathrm{ord}_{s=1} L(A, s) = d$, so again $r = 1$. Taking discriminants of the polynomials in Stein's tables, we find that for all three $2 \nmid \mathrm{disc}(O_f)$. In fact 422C and 422E satisfy all the conditions (1)–(5). In each case 2 is inert in K_f, and the three sequences of Hecke eigenvalues all become the same in $\mathbb{F}_8$. This is easy to check from Stein's table, since the minimal polynomials for a_3 given there are all congruent to $x^3 + x^2 + 1$ mod 2, so one just reads each sequence (of polynomials of degree ≤ 2 in x) modulo 2, and they are all the same sequence. There is also a newform for $\Gamma_0(422)$ with coefficient field of degree 6, whose Hecke eigenvalues become the same in $\mathbb{F}_8$, modulo a divisor of 2 of degree 3. For this newform, $(w_2, w_{211}) = (-1, 1)$. Hence, relative to 422C, $B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $k = 2$. Since $Fk = 6$, Proposition 9.6 shows that if $\mathbb{T}_{\mathfrak{m}}$ is a local complete intersection (which we actually confirm in the next subsection) then $2^6 \mid m$ (for 422C and 422E). In fact, for 422C, 422D and 422E we have $m = 2^6 \cdot 3 \cdot 7^2$, $m = 2^6 \cdot 23 \cdot 29$ and $m = 2^6 \cdot 223$, respectively. For 422E, Proposition 2.1 only gives $2^3 \mid m$, while for 422C it gives $2^6 \mid m$.

There are four modular abelian varieties with $N = 478 = 2 \cdot 239$, of dimensions $4, 4, 5, 6$. For the two 4-dimensional varieties, $(w_2, w_{239}) = (1, 1)$ and $(-1, -1)$, so $\epsilon = -1$, and as above one finds that $r = 1$. In both cases the conditions (1)–(5) of the introduction are satisfied. For the 5 and 6-dimensional varieties we have $(w_2, w_{239}) = (-1, 1)$ and $(1, -1)$, respectively. In all four cases O_K has a prime of norm 2^4, and in $\mathbb{F}_{16}$ all four sequences of Hecke eigenvalues appear to become the same. Accepting this, $k = 2$, and $Fk = 8$, so Proposition 9.6 implies that if $\mathbb{T}_{\mathfrak{m}}$ is a local complete intersection then $2^8 \mid m$ (for the 4-dimensional varieties), and in fact their modular degrees are $2^8 \cdot 13$ and $2^8 \cdot 11 \cdot 829$.

11. Examination of Hypothesis 9.2

11.1. **Local complete intersections.** The examples of conductors 26, 38, 74 and 86 were too easy. We take two more challenging examples from §§10.1 and 10.3, and show that in each, $\mathbb{T}_{\mathfrak{m}}$ is a local complete intersection, thus lending weight to the idea that it might always, or at least often, be so.

N = 214, d = 1.

The Hecke ring $\mathbb{T}_{\mathfrak{m}}$ is isomorphic to the subring of $\mathbb{Z}_2^2 \times (\mathbb{Z}_2(\sqrt{3}))^2$ generated by $v_p := (a_p(g_1), a_p(g_2), a_p(g_3), a_p(g_4))$, where p runs over the prime numbers, and g_1, g_2, g_3 and g_4 are the normalised newforms associated to the elliptic curves 214b1, 214a1, and two 2-dimensional abelian varieties with coefficient field $\mathbb{Q}(\sqrt{3})$, respectively. As a $\mathbb{Z}_2$-module it is generated by the vectors $v_n := (a_n(g_1), a_n(g_2), a_n(g_3), a_n(g_4))$ for $1 \leq n \leq 54 = \frac{N}{6}\prod_{p|N}\left(1+\frac{1}{p}\right)$, by Theorem 5.1 of [LS], part of Agashe and Stein's appendix. Each v_n may be viewed as an element of $\mathbb{Z}_2^6$ by expressing $a_n(g_3)$ as a $\mathbb{Z}_2$-linear combination of 1 and $\alpha := \sqrt{3}-1$, and $a_n(g_4)$ as a $\mathbb{Z}_2$-linear combination of 1 and $\beta := \sqrt{3}+1$. Using Stein's tables [Ste] to get $v_1, \ldots, v_{54}$, and using the computer package PARI to compute Hermite normal form, one finds that $\mathbb{T}_{\mathfrak{m}}$ is the $\mathbb{Z}_2$-submodule of $\mathbb{Z}_2^2 \times (\mathbb{Z}_2(\sqrt{3}))^2$ generated by the rows of the matrix

$$\begin{pmatrix} 4 & 0 & 0 & 0 \\ 2 & 2 & 0 & 0 \\ 0 & 0 & 2\alpha & 0 \\ 2 & 0 & 2 & 0 \\ 0 & 0 & \alpha & \beta \\ 1 & 1 & 1 & 1 \end{pmatrix}.$$

The top row shows that, with respect to projection to the first entry, $\eta = (4)$. Considering ways to take linear combinations of the rows to get a 0 in the first entry, one finds that $\mathcal{P}_{\mathbb{T}}$ is the $\mathbb{Z}_2$ submodule spanned by the rows of

$$\begin{pmatrix} 0 & 0 & \alpha & \beta \\ 0 & 0 & 2\alpha & 0 \\ 0 & 0 & 2 & 2 \\ 0 & 2 & 0 & 2 \\ 0 & 2 & -2 & 0 \\ 0 & 4 & 0 & 0 \end{pmatrix}.$$

Then multiplying pairs of these elements together one finds that $\mathcal{P}_{\mathbb{T}}^2$ is spanned by the rows of

$$\begin{pmatrix} 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \\ 0 & 0 & 2\alpha & 0 \\ 0 & 0 & 0 & 2\beta \\ 0 & 0 & 4-4\alpha & 0 \\ 0 & 0 & 2-2\alpha & 2+2\beta \end{pmatrix}.$$

By deleting the 0 in the first position, we may view $\mathcal{P}_{\mathbb{T}}$ and $\mathcal{P}_{\mathbb{T}}^2$ as submodules of $\mathbb{Z}_2^5$, and using Hermite normal form we find that they are of index 2^5 and 2^7, respectively. Hence $\#(\mathcal{P}_{\mathbb{T}}/\mathcal{P}_{\mathbb{T}}^2) = 4$. Since $\#(\mathcal{P}_{\mathbb{T}}/\mathcal{P}_{\mathbb{T}}^2) = \#(\mathbb{Z}_2/\eta)$, $\mathbb{T}_{\mathfrak{m}}$ is a local complete intersection.

N = 422, d = 3.

The Hecke ring $\mathbb{T}_{\mathfrak{m}}$ is isomorphic to the subring of $W(\mathbb{F}_8)^4$ generated by $v_p := (a_p(g_1), a_p(g_2), a_p(g_3), a_p(g_4))$, where p runs over the prime numbers, and g_1, g_2, g_3 and g_4 are the normalised newforms associated to the 3-dimensional abelian varieties 422E, 422C, 422D, and a certain 6-dimensional abelian variety, respectively. Here $W(\mathbb{F}_8)$ is the ring of integers in the unramified extension of $\mathbb{Q}_2$ of degree 3, and each coefficient ring is embedded in $W(\mathbb{F}_8)$ using a divisor of (2) of degree 3. As a $W(\mathbb{F}_8)$-module, $\mathbb{T}_{\mathfrak{m}}$ is generated by the vectors $v_n := (a_n(g_1), a_n(g_2), a_n(g_3), a_n(g_4))$ for $1 \leq n \leq 106 = \frac{N}{6}\prod_{p|N}\left(1+\frac{1}{p}\right)$, again by Agashe and Stein's appendix to [LS].

We have $W(\mathbb{F}_8) = \mathbb{Z}_2(\alpha)$ with $\alpha^3+\alpha^2+1=0$. The coefficient fields of g_1, g_2, g_3 and g_4 are obtained from $\mathbb{Q}$ by adjoining roots of polynomials $x^3+5x^2+6x+1, x^3+x^2-8x-3, x^3+x^2-6x-5$ and $x^6-4x^5-4x^4+28x^3-15x^2-33x+28$ respectively. There are roots of these polynomials in $W(\mathbb{F}_8)$ congruent modulo 2^5 to $20+31\alpha+30\alpha^2$, $28+21\alpha$, $14+9\alpha+30\alpha^2$ and $14+11\alpha+8\alpha^2$ respectively. Plugging in these expressions for x in Stein's tables, we get vectors v_n', approximating the v_n modulo 2^5, which (using all $n \geq 1$) generate a $W(\mathbb{F}_8)$-submodule M_2 of $M := W(\mathbb{F}_8)^4$ such that $M_2 + 2^5M = M_1 + 2^5M$, where $M_1 := \mathbb{T}_{\mathfrak{m}}$. By Lemma 2.1 of [LS], if $2^4M \subseteq M_2$ then $M_1 = M_2$.

Let

$$u_1 := v_1' + v_2' = (1,1,1,1) + (1,-1,-1,1) = (2,0,0,2),$$
$$u_2 := v_{211}' - v_2' = (1,-1,1,-1) - (1,-1,-1,1) = (0,0,2,-2) \text{ and}$$
$$u_3 := v_1' - v_{211}' = (1,1,1,1) - (1,-1,1,-1) = (0,2,0,2).$$

Also let

$$u_4 := v_6' - v_7' = (30\alpha^2+31\alpha+20, 11\alpha+4, 2\alpha^2+23\alpha+18, 8\alpha^2+11\alpha+14)$$
$$-(12\alpha^2+31\alpha+14, 11\alpha+2, 2\alpha^2+23\alpha+18, 30\alpha^2+7\alpha+6) = (18\alpha^2+6, 2, 0, -22\alpha^2+4\alpha+8).$$

Then $u_4 - u_3 = (18\alpha^2+6, 0, 0, -22\alpha^2+4\alpha+6)$, so

$$u_4 - u_3 - (9\alpha^2+3)u_1 = (0,0,0,-40\alpha^2+4\alpha) \text{ and}$$
$$u_4 - u_3 - (-11\alpha^2+2\alpha+3)u_1 = (40\alpha^2-4\alpha, 0, 0, 0),$$

so M_2 contains $(0,0,0,4)$ and $(4,0,0,0)$. It also contains $u_1+u_2 = (2,0,2,0)$ and $u_1-u_3 = (2,-2,0,0)$. We now see easily that M_2 contains $(4,0,0,0), (0,4,0,0), (0,0,4,0)$ and $(0,0,0,4)$, so that in fact $2^2M \subseteq M_2$, and indeed $M_1 = M_2$, i.e. $\mathbb{T}_{\mathfrak{m}} = M_2$.

The element $(4,0,0,0)$ of $\mathbb{T}_{\mathfrak{m}}$ shows that if η is defined with respect to projection to the first coordinate then $\eta \mid (4)$. Since (2) is inert in the coefficient ring for g_1, and in particular is the unique divisor of (2), η is the 2-part of what in [ARS](Definition 4.10) is called the congruence ideal (with A the abelian variety 422C). Hence the 2-part of their "congruence exponent" is 2^s, where $\eta = (2^s)$. Now we already know that the 2-part of the modular degree is 2^6, and using again the uniqueness of the divisor of (2), the 2-part of $\ker(\pi \circ \pi^\vee)$ must have structure $W(\mathbb{F}_8)/(2^2)$, so that the 2-part of the "modular exponent" in [ARS] is 2^2. By their Theorem 3.7, that the modular exponent divides the congruence exponent, we see that also $(4) \mid \eta$, so in fact $\eta = (4)$.

Since $-u_1u_2 = (0,0,0,4), u_2^2 + u_2u_3 = (0,0,4,0)$ and $u_3^2 + u_2u_3 = (0,4,0,0)$ all belong to $\mathcal{P}_{\mathbb{T}}^2$, while necessarily $\#(W(\mathbb{F}_8)/\eta) \mid \#(\mathcal{P}_{\mathbb{T}}/\mathcal{P}_{\mathbb{T}}^2)$, the Fitting ideal of $\mathcal{P}_{\mathbb{T}}/\mathcal{P}_{\mathbb{T}}^2$ must be either (2^2) or (2^3). If it was the latter then $\mathcal{P}_{\mathbb{T}}$ would contain $(0,2,0,0)$,$(0,0,2,0)$ and $(0,0,0,2)$, which subtracted from u_1 shows that $(2,0,0,0) \in$

$\mathbb{T}_{\mathfrak{m}}$, contrary to $\eta = (4)$. Hence $\#(W(\mathbb{F}_8)/\eta) = \#(\mathcal{P}_{\mathbb{T}}/\mathcal{P}_{\mathbb{T}}^2) = (2^3)^2$, so $\mathbb{T}_{\mathfrak{m}}$ is a local complete intersection.

11.2. **Modularity of lifts.** Having examined the hypothesis that $\mathbb{T}_{\mathfrak{m}}$ is a local complete intersection, we now look into what it would take for the isomorphism in Hypothesis 9.2 to fail.

If O is the ring of integers in a finite extension of $\mathbb{Q}_2$ containing K_λ, and if $\theta : \mathcal{R}_{\mathcal{D}} \to O$ is a local O_λ-algebra homomorphism, then $\theta \circ \rho_{\mathcal{D}}^{\mathrm{univ}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(O)$ is ordinary when restricted to $\mathrm{Gal}(\overline{\mathbb{Q}}_2/\mathbb{Q}_2)$, since it satisfies condition (2) of §8 at $p = 2$. By §4 of [P], since $\theta \circ \rho_{\mathcal{D}}^{\mathrm{univ}}|_{G_2}$ is ordinary, it is semi-stable. It is then a direct consequence of Theorem 4.1 of [KW] that, if the image of $\overline{\rho}$ in $\mathrm{GL}_2(\mathbb{F})$ is non-solvable, then $\theta \circ \rho_{\mathcal{D}}^{\mathrm{univ}}$ is modular. In particular, any such $\theta : \mathcal{R}_{\mathcal{D}} \to O$ must factor through $\mathbb{T}_{\mathfrak{m}}$, and if $\mathcal{R}_{\mathcal{D}} \not\simeq \mathbb{T}_{\mathfrak{m}}$ then this is not due to any failure of lifts of $\overline{\rho}$ to $\mathrm{GL}_2(O)$ to be modular. When $d = 1$, the image of $\overline{\rho}$ is always solvable, since $\mathrm{GL}_2(\mathbb{F}_2)$ is solvable. In general, given the absolute irreducibility implied by Proposition 4.2, in our examples the only way for the image of $\overline{\rho}$ to be solvable is for its image in $\mathrm{PGL}_2(\mathbb{F}_\lambda)$ to be dihedral, by Lemma 6.1 of [KW]. This is equivalent to $\overline{\rho}$ being isomorphic, over $\overline{\mathbb{F}}_2$, to the representation induced from some character of a subgroup of index 2. This would imply that there is a quadratic field F, ramified at most at primes dividing N, such that $\overline{a_p(f)} = 0$ in $\mathbb{F}_\lambda$ whenever p is inert in F. It is easy to check using Stein's tables that this is not the case in the examples in this section with $d > 1$, so the image of $\overline{\rho}$ is indeed non-solvable. In fact, if we assume that $\mathcal{R}_{\mathcal{D}}$ is finitely generated as an O_λ-module then it is easy to show that, given the above, any non-zero element of the kernel of θ must be nilpotent. (Note that the nilradical is the intersection of all prime ideals.)

12. A different approach

We continue to impose the conditions (1)–(5) from the introduction. Corollary 9.5 shows that, if each $k_i \geq 1$, then Hypothesis 9.2 implies that $2^R \mid m$, in accord with the analogue of Watkins's conjecture. It seems difficult to prove that each $k_i \geq 1$, so we outline a different approach.

Recall from §2 the subgroup W' of Atkin-Lehner involutions fixing f. Thanks to the condition (2), $W'' = W'$, and by Proposition 2.1, $(\#W')^d \mid m$. The proof shows that $m = m'(\#W')^d$, where m' is defined as follows. Let $X' = X/W'$, and J' the Jacobian of X'. The maps $\pi : J_0(N) \to A$ and $\pi^\vee : A^\vee \to J_0(N)$ factor through $\pi' : J' \to A$ and $\pi'^\vee : A^\vee \to J'$. We define m' to be the square root of the degree of the isogeny $\pi' \circ \pi'^\vee : A^\vee \to A$.

As already hinted, we may define a deformation problem $\mathcal{D}'$ in the same way as $\mathcal{D}$ except that for $p \mid N$ we fix the character χ. Let $\mathcal{R}_{\mathcal{D}'}$ be the universal deformation ring (a certain quotient of $\mathcal{R}_{\mathcal{D}}$), and let $\mathbb{T}''$ be the quotient of $\mathbb{T}_{\mathfrak{m}}$ obtained by viewing it as a subring of $\prod_g O_g$ then projecting to the product over just those g such that $w_p(g) = w_p(f)$ for all $p \mid N$. There is an O_λ-algebra homomorphism $\theta : \mathcal{R}_{\mathcal{D}'} \to \mathbb{T}''$.

Hypothesis 12.1. *θ' is an isomorphism and $\mathcal{R}_{\mathcal{D}'} \simeq \mathbb{T}''$ is a local complete intersection.*

Theorem 12.2. *Assume the conditions (1)-(5) from the introduction. Let $r = \dim_K(A(\mathbb{Q}) \otimes \mathbb{Q})$. Then, assuming Hypothesis 12.1, $2^{2F(r-1)}$ divides the order of $e_i(\ker(\pi' \circ \pi'^\vee))$.*

Corollary 12.3. *Assume the conditions (1)-(5) from the introduction, and also Hypothesis 12.1. Then the modular degree of A is divisible by $2^{R-d}(\#W')^d$, where $R = \mathrm{rank}(A(\mathbb{Q}))$. In particular (since the condition (1) implies that N is divisible by at least two primes, so $\#W' \geq 2$), 2^R divides the modular degree, in accord with the analogue of Watkins's conjecture.*

Note that $2^{R-d}(\#W')^d = 2^{d(r-1+s-1)}$ or $2^{d(r-1+s)}$, and compare with the comment following Corollary 9.5. If $r = 0$ then $r-1$ should be replaced by 0.

The steps in the proof of Theorem 12.2 are described below. The elements of W' commute with the T_p (for $p \nmid N$) and the W_p (for $p \mid N$), but not with the U_p, so we define $\tilde{\mathbb{T}}'$ to be the ring of endomorphisms of J' generated by the T_p (for $p \nmid N$) and W_p (for $p \mid N$). Let $\tilde{\mathbb{T}}$ be the ring of endomorphisms of $J_0(N)$ generated by T_p (for $p \nmid N$) and W_p (for $p \mid N$). Fixing i and $\lambda = \lambda_i$, let $\tilde{\mathfrak{m}}'$ and $\tilde{\mathfrak{m}}$ be the kernels of the homomorphisms from $\tilde{\mathbb{T}}'$ and $\tilde{\mathbb{T}}$ (respectively) to $\mathbb{F}_\lambda$ given by $T_p \mapsto \overline{a_p(f)}$ and $W_p \mapsto w_p(f)$. Recall that $\mathbb{T}_{\mathfrak{m}}$ can be described as the subring of $\prod_g O_g$ generated by the $(a_p(g))$, where g runs over certain G_2-orbits of newforms for $\Gamma_0(N)$. Likewise $\tilde{\mathbb{T}}_{\tilde{\mathfrak{m}}}$ may be identified with the subring of $\prod_g O_g$ generated by the $(a_p(g))$ (for $p \nmid N$) and $(w_p(g))$ (for $p \mid N$). But each $w_p(g) = -a_p(g)$, so these are the same subrings, and we have a natural isomorphism $\mathbb{T}_{\mathfrak{m}} \simeq \tilde{\mathbb{T}}_{\tilde{\mathfrak{m}}}$, taking $\mathfrak{m}$ to $\tilde{\mathfrak{m}}$. Let $\theta : X \to X'$ be the quotient morphism.

Lemma 12.4. *$\theta^* : J'[\tilde{\mathfrak{m}}'] \to J_0(N)[\tilde{\mathfrak{m}}]$ is injective.*

We shall give a full proof of this after describing how it is used.

Lemma 12.5. *There is an equality of $\mathbb{T}_{\mathfrak{m}}$-modules*

$$T_2(J_0(N))_{\mathfrak{m}} = T_2(J_0(N))_{\tilde{\mathfrak{m}}},$$

inside $T_2(J_0(N)$, where the right-hand side is a $\mathbb{T}_{\mathfrak{m}}$-module via the isomorphism $\mathbb{T}_{\mathfrak{m}} \simeq \tilde{\mathbb{T}}_{\tilde{\mathfrak{m}}}$.

We sketch the proof. The actions of all the T_p, U_p and W_p on $H_1(X_0(N), \mathbb{Q})$ commute with the action of complex conjugation, as remarked in §2.4 of [Cr2], which uses the earlier §2.1.3. Hence each $H_1(X_0(N), \mathbb{Q})^{\pm}$ is a $\mathbb{T}_{\mathbb{Q}}$-module and a $\tilde{\mathbb{T}}_{\mathbb{Q}}$-module. The space $S_2(\Gamma_0(N))$ is dual as a $\mathbb{T}_{\mathbb{C}}$-module (respectively as a $\tilde{\mathbb{T}}_{\mathbb{C}}$-module) to each $H_1(X_0(N), \mathbb{Q})^{\pm} \otimes \mathbb{C}$, but also to $\mathbb{T}_{\mathbb{C}}$ (via $(T, f) \mapsto a_1(Tf)$) (respectively to $\tilde{\mathbb{T}}_{\mathbb{C}}$, by Theorem 5 of [AL]). It follows that each $H_1(X_0(N), \mathbb{Q})^{\pm}$ is free of rank one as a $\mathbb{T}_{\mathbb{Q}}$-module and as a $\tilde{\mathbb{T}}_{\mathbb{Q}}$-module (c.f. Lemma 1.37 of [DDT] for the former). Since $T_2(J_0(N)) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2 \simeq H^1(X_0(N), \mathbb{Q}_2)$, we get that $T_2(J_0(N)) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$ is free of rank two as a $\mathbb{T}_{\mathbb{Q}_2}$-module and as a $\tilde{\mathbb{T}}_{\mathbb{Q}_2}$-module. Both $T_2(J_0(N))_{\mathfrak{m}} \otimes \mathbb{Q}_2$ and $T_2(J_0(N))_{\tilde{\mathfrak{m}}} \otimes \mathbb{Q}_2$ may be obtained from $T_2(J_0(N)) \otimes_{\mathbb{Z}_2} \mathbb{Q}_2$ by applying appropriate elements in the subalgebra (of both $\mathbb{T}_{\mathbb{Q}_2}$ and $\tilde{\mathbb{T}}_{\mathbb{Q}_2}$) generated by the T_p for $p \nmid N$, to isolate the part corresponding to newforms "belonging to" $\mathfrak{m}$ (equivalently to $\tilde{\mathfrak{m}}$, i.e. the g above). Hence $T_2(J_0(N))_{\mathfrak{m}} \otimes \mathbb{Q}_2 = T_2(J_0(N))_{\tilde{\mathfrak{m}}} \otimes \mathbb{Q}_2$, and we obtain $T_2(J_0(N))_{\mathfrak{m}} = T_2(J_0(N))_{\tilde{\mathfrak{m}}}$ by intersecting with $T_2(J_0(N))$, since both are direct summands of $T_2(J_0(N)$ as $\mathbb{Z}_2$-modules.

Lemma 12.6. (1) $\dim_{\mathbb{F}_\lambda} J'[\tilde{\mathfrak{m}}'] = 2$.
(2) *$T_2(J')_{\tilde{\mathfrak{m}}'}$ is free of rank 2 over $\tilde{\mathbb{T}}'_{\tilde{\mathfrak{m}}'}$.*

Lemma 12.5 implies that $J_0(N)[\tilde{\mathfrak{m}}] \simeq J_0(N)[\mathfrak{m}]$, which has $\mathbb{F}_\lambda$-dimension 2 by Proposition 2.4 of [Bz]. Then by Lemma 12.4, $\dim_{\mathbb{F}_\lambda} J'[\tilde{\mathfrak{m}}'] \leq 2$, but it must be equal

to 2 since it supports the irreducible 2-dimensional representation $\overline{\rho}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The second part of Lemma 12.6 follows from the first.

Deduction of Theorem 12.2.

To get $T_2(J') \otimes \mathbb{Q}_2$ from $T_2(J_0(N)) \otimes \mathbb{Q}_2$, one takes W'-invariants. (This does not apply integrally, since W' is a 2-group.) It follows that $\tilde{\mathbb{T}}'_{\tilde{\mathfrak{m}}'}$ is the quotient of $\tilde{\mathbb{T}}_{\tilde{\mathfrak{m}}} \simeq \mathbb{T}_{\mathfrak{m}}$ obtained by restricting the product of O_g to g fixed by W'. This includes all g such that $w_p(g) = w_p(f)$ for all primes $p \mid N$, and if $W' \neq W$ possibly some extra g such that $w_p(g) = +1$ for all primes $p \mid N$. Thus we see that the $\mathbb{T}''$ appearing in Hypothesis 12.1 is a quotient of $\tilde{\mathbb{T}}'_{\tilde{\mathfrak{m}}'}$. If we define congruence ideals η' and η'' in O_λ, for $\tilde{\mathbb{T}}'_{\tilde{\mathfrak{m}}'}$ and $\mathbb{T}''$ respectively, then $\eta' \subseteq \eta''$. Thus it follows from Hypothesis 12.1 and the first half of the proof of Proposition 8.2 that $\eta' = (2^S)$ for some $S \geq r-1$. Now one can prove Theorem 12.2 in the same manner as Theorem 9.4.

Proof of Lemma 12.4.

Consider $\theta^* : J' \to J_0(N)$. We define a map $F : \ker \theta^* \to (W')^\wedge$ (the character group of W') as follows. Given a divisor class $[D'] \in \ker \theta^*$, $\theta^*(D') = \mathrm{div}(g)$ for some function g on $X_0(N)$. If $w \in W'$ then wg is a multiple of g, since $\mathrm{div}(g)$, as a pullback from X', is invariant under W'. Thus we may define $F([D'])(w) = wg/g = \pm 1$. If $[D'] \in \ker F$ then $wg = g \ \forall w \in W'$ so g is the pullback of a function on X', whose divisor is D', showing that $[D'] = [0]$. Hence F is injective.

Now suppose that $[D'] \in J'[\tilde{\mathfrak{m}}']$ is a non-zero element of $\ker \theta^*$, say $\theta^*(D') = \mathrm{div}(g)$. Since $\overline{\rho}$ is irreducible it has non-zero character, so we may choose a prime $p \nmid N$ such that $\mathrm{tr}(\overline{\rho}(\mathrm{Frob}_p^{-1})) \neq 0$, so $a_p \not\equiv 0 \pmod{\lambda}$. Hence $[T_p D'] \neq [0]$ in J', since T_p acts as multiplication by a_p on the $\mathbb{F}_\lambda$-vector space $J'[\tilde{\mathfrak{m}}']$, but $[T_p D']$ is also in $\ker \theta^*$, in fact $\theta^*(T_p D') = \mathrm{div}(T_p g)$. (The Hecke correspondence acts on functions, as on divisors, by pullback and push-forward under degeneracy maps.) If $w \in W'$ then $w(T_p g) = T_p(wg) = T_p(\pm g) = (\pm 1)^{p+1} T_p g = T_p g$, since T_p has degree $(p+1)$, which is even. This shows that $F([T_p D'])$ is trivial, contrary to the injectivity of F. Hence θ^* must be injective on $J'[\tilde{\mathfrak{m}}']$.

□

References

[ARS] A. Agashe, K. Ribet, W. Stein, The Modular Degree, Congruence Primes and Multiplicity One, 2009, *to appear in* Number Theory, Analysis and Geometry: In Memory of Serge Lang, (D. Goldfeld, ed.), Springer. http://www.williamstein.org/papers/

[AL] A.O.L. Atkin, J. Lehner, Hecke operators on $\Gamma_0(N)$, *Math. Ann.* **185** (1970), 134–160.

[Bz] K. Buzzard, On level-lowering for mod 2 representations, *Math. Res. Lett.* **7** (2000), 95–110.

[Cr1] J. Cremona, *Elliptic curve data.* http://homepages.warwick.ac.uk/staff/J.E.Cremona/.

[Cr2] J. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1997 (second edition), online version, http://homepages.warwick.ac.uk/staff/J.E.Cremona/book/fulltext/index.html.

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

[DR] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972),* 143–316. Lect. Notes in Math., **349**. Springer, Berlin, 1973.

[Du] N. Dummigan, On a conjecture of Watkins, *J. Th. Nombres Bordeaux* **18** (2006), 345–355.

[Ed] B. Edixhoven, The weight in Serre's conjectures on modular forms, *Invent. Math.* **109** (1992), 563–594.

[G] B. H. Gross, Kolyvagin's work on modular elliptic curves, *in* L-functions and Arithmetic, (J. Coates, M. J. Taylor, eds.), 235–256, Cambridge University Press, 1991.
[GZ] B. H. Gross, D. B. Zagier, Heegner points and derivatives of L-series, *Invent. Math.* **84** (1986), 225–320.
[JL] B. Jordan, R. Livné, Local diophantine properties of Shimura curves, *Math. Ann.* **270**, 235–248 (1985).
[KW] C. Khare, J.-P. Wintenberger, Serre's Modularity Conjecture, I, *Invent. Math.* **178** (2009), 485–504.
[LS] J.-C. Lario, R. Schoof, Some computations with Hecke rings and deformation rings. With an appendix by A. Agashe and W. Stein. *Experiment. Math.* **11** (2002), 303–311.
[Ma] B. Mazur, An introduction to the deformation theory of Galois representations, *in* Modular Forms and Fermat's Last Theorem, (G. Cornell, J. H. Silverman, G. Stevens, eds.), 243–311, Springer-Verlag, New York, 1997.
[MR] B. Mazur, M. Rapoport, Appendix to B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. IHES* **47** (1977), 33–186.
[Mi] J. S. Milne, Abelian Varieties. In *Arithmetic Geometry (Storrs, Conn., 1984),* G. Cornell, J. Silverman, eds., 103–150. Springer, New York, 1986.
[P] B. Perrin-Riou, Représentations p-adiques ordinaires, *Astérisque* **223** (1994), 185–207.
[Ra1] M. Raynaud, Spécialisation du foncteur de Picard, *Publ. Math. IHES* **38** (1970), 27–76.
[Ra2] M. Raynaud, Variétés abéliennes et géométrie rigide. In *Actes du Congrès International des Mathématiciens (Nice, 1970),* Tome 1, 473–477. Gauthier-Villars, Paris, 1971.
[Ri1] K. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Invent. Math.* **100** (1990), 431–476.
[Ri2] K. Ribet, Galois action on division points of abelian varieties with real multiplications, *Amer. J. Math.,* **98** (1976), 751–804.
[SGA7] *Groupes de monodromie en géométrie algébrique. I.* Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I). Dirigé par A. Grothendieck, avec la collaboration de M. Raynaud et D. S. Rim, Lect. Notes in Math., **288**. Springer, Berlin, 1972.
[Ste] W. Stein, The Modular Forms Database: Tables, http://www.williamstein.org/Tables/tables.html
[Stu] J. Sturm, On the congruence of modular forms, *in* Number Theory (New York 1984–85), 275–280, Lect. Notes in Math., **1240**. Springer, Berlin, 1987.
[TW] R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. Math.* **141** (1995), 553–572.
[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, School of Mathematics and Statistics, Hicks Building, Hounsfield Road, Sheffield, S3 7RH, U.K.

Institute of Mathematical Sciences, IV Cross Road, CIT Campus, Taramani, Chennai 600 113, Tamil Nadu, India.

E-mail address: n.p.dummigan@shef.ac.uk
E-mail address: lakshmi@imsc.res.in