ISRAEL JOURNAL OF MATHEMATICS **169** (2009), 417–444
DOI: 10.1007/s11856-009-0017-x

ELLIPTIC CURVES OF ODD MODULAR DEGREE

BY

Frank Calegari* and Matthew Emerton**

Northwestern University, Department of Mathematics
2033 Sheridan Rd. Evanston, IL 60208 United States
e-mail: fcale@math.northwestern.edu, emerton@math.northwestern.edu

ABSTRACT

The modular degree m_E of an elliptic curve $E/\mathbf{Q}$ is the minimal degree of any surjective morphism $X_0(N) \to E$, where N is the conductor of E. We give a necessary set of criteria for m_E to be odd. In the case when N is prime our results imply a conjecture of Mark Watkins. As a technical tool, we prove a certain multiplicity one result at the prime $p = 2$, which may be of independent interest.

1. Introduction

Let E be an elliptic curve over $\mathbf{Q}$ of conductor N. Since E is modular [3], there exists a surjective map $\pi : X_0(N) \to E$ defined over $\mathbf{Q}$. There is a unique such map of minimal degree (up to composing with automorphisms of E), and its degree m_E is known as the **modular degree** of E. This degree has been much studied, both in relation to congruences between modular forms [38] and to the Selmer group of the symmetric square of E [14], [15], [35]. Since this Selmer

* Supported in part by the American Institute of Mathematics.
** Supported in part by NSF grant DMS-0401545.
Receved August 11, 2006 and in revised form June 28, 2007

group can be considered as an elliptic analogue of the class group, one might expect in analogy with genus theory to find that m_E satisfies certain divisibility properties, especially, perhaps, by the prime 2. More precisely, we remind the reader that the class number of an imaginary quadratic extension K of $\mathbf{Q}$ is odd if and only if the absolute discriminant D_K of K is equal either to 4 or to an odd prime (and similarly for the strict class number of a real quadratic extension). In this paper we consider the analogous question of the parity of m_E. In particular we establish a conjecture of Watkins (see Theorem 1.7 below) to the effect that if E has no rational 2-torsion points, then m_E is odd only if the conductor N of E is a prime congruent to 3 mod 8. In fact we prove the following more precise theorem:

1.1 Theorem: *If $E/\mathbf{Q}$ is an elliptic curve of odd modular degree, then:*

1. *The conductor N of E is divisible by no more than two odd primes,*
2. *E is of even analytic rank, and*
3. *One of the following holds:*
   (a) *E has a rational point of order 2 (equivalently, admits a rational 2-isogeny);*
   (b) *E has prime conductor and supersingular reduction at 2, and $\mathbf{Q}(E[2])$ is totally complex (equivalently, $E(\mathbf{R})$ is connected);*
   (c) *E has complex multiplication, and $N = 27, 32, 49,$ or 243.*

1.2 Example: The following examples of elliptic curves with odd modular degree should serve to illustrate conditions (3a), (3b) and (3c). The curve $X_0(15)$ has modular degree one and a rational two torsion point, and thus satisfies condition (3a). Another example is given by the curve

$$y^2 + xy = x^3 - x^2 - 58x - 105$$

($2537E$ in Cremona's tables) of conductor $43 \cdot 59$ with modular degree 445 and torsion subgroup $\mathbf{Z}/4\mathbf{Z}$. The curves $X_0(11)$ and $X_0(19)$ both have modular degree one and satisfy condition (3b). An example of larger conductor is given by

$$y^2 + y = x^3 + x^2 - 4x - 10$$

of conductor 24859 and modular degree 3979. Finally, there are exactly four curves of odd modular degree with complex multiplication, namely $X_0(27)$,

$X_0(32)$, $X_0(49)$ (all of modular degree one) and

$$y^2 + y = x^3 + 2$$

of modular degree 9, conductor 243 and j-invariant 0.

1.3 Remark: Each of the conditions appearing in Theorem 1.1 is invariant under isogeny, other than the condition that $E(\mathbf{R})$ be connected, which is, however, invariant under isogenies of odd degree. Since the modular parameterization of E factors through the optimal member of the isogeny class of E (that is, the member of its isogeny class having minimal modular degree; in older terminology, a strong Weil curve), it is therefore no loss of generality in the proof of Theorem 1.1 to assume that E is optimal.

1.4 Remark: Cremona and Watkins have computed the modular degree of every optimal elliptic curve of conductor $\leq 25{,}000$ [8]. These computations suggest that there may be even stronger limitations on the conductor of a curve of odd modular degree than those imposed by Theorem 1.1. Indeed, in the range of Watkins' computations, every curve of odd modular degree has conductor divisible by at most two primes, and the conductor always has one of the following forms: $2p$, $4p$, or pq, where p and q are odd primes[1].

1.5 Remark: The statement of the Theorem regarding the analytic rank of E is consistent with the conjecture of Birch and Swinnerton-Dyer and with the rank conjecture of Watkins [35, Conj. 4.1] that $2^r | m_E$, where $r = \operatorname{rank}(E(\mathbf{Q}))$.

1.6 Remark: In [32] the parity of m_E was determined for a very particular explicit class of elliptic curves, namely, the Neumann–Setzer curves, which are the curves of prime conductor > 17 which have a rational 2-torsion point. (See also the remark following Theorem 5.1 below.)

The following result, conjectured by Watkins ([32, Conj. 4.3], [35, Conj. 4.2]), is a simple consequence of Theorem 1.1 (see Lemma 3.3):

[1] Since this paper was circulated as a preprint, Soroosh Yazdani, in his UC Berkeley thesis *Modular abelian variety of odd modular degree,* has established further limitations on the possible shape of the conductor of an elliptic curve of odd modular degree. For example, he has shown that if the conductor is divisible by more than one prime, and is not divisible by 4, then it is of the form $2p$ or pq where p and q are odd primes satisfying certain congruence conditions modulo 16. In each of these cases he has also shown that E has rank 0.

1.7 Theorem: *Let $E/\mathbf{Q}$ be an elliptic curve of prime conductor N, and suppose that E is neither a Neumann–Setzer curve, nor $X_0(17)$ (equivalently, E does not have a rational 2-torsion point). If m_E is odd, then $N \equiv 3 \bmod 8$.*

One technique for proving that an elliptic curve E has even modular degree is to show that the map π factors through $X_0(N)/w$ for some non-trivial Atkin–Lehner involution w. We use this approach in Section 2 to prove Theorem 2.1, which in turn implies parts (1) and (2) of Theorem 1.1, and shows that (3a) holds if N is divisible by at least two primes. It remains to prove (3) in the case when N is a prime power. The most difficult case to handle is when N is actually prime, and in this case we deduce Theorem 1.1 from the following result, proved in Section 3.

1.8 Theorem: *Let N be prime, let $\mathbf{T}$ denote the Hecke algebra over $\mathbf{Z}$ acting on weight two cuspforms on $\Gamma_0(N)$, and let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ such that $\mathbf{T}/\mathfrak{m} = \mathbf{F}_2$, and such that the associated semi-simple Galois representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_2)$ is irreducible. If the completion $\mathbf{T}_{\mathfrak{m}} = \mathbf{Z}_2$, then*

1. *$\mathfrak{m}$ is supersingular at 2 (i.e. $T_2 \in \mathfrak{m}$), or equivalently, $\overline{\rho}|_{D_2}$ is absolutely irreducible.*
2. *$\overline{\rho}$ is totally complex.*

The relevance of this result to Theorem 1.1 is that, since N is prime in the context of Theorem 1.8, a result of Ribet [38] shows (assuming, as we may, that E is optimal) that the modular degree of E is even if and only if 2 is a congruence prime for the newform of level N attached to E.

1.9 Remark: The equivalence between the supersingularity of $\mathfrak{m}$ and the absolute irreducibility of $\overline{\rho}|_{D_2}$ can be deduced (in the standard way) as follows: if $V_{/\mathbf{Z}_2}$ denotes a finite group scheme subquotient of $J[\mathfrak{m}]_{/\mathbf{Z}_2}$ (where $J := J_0(N)$) whose generic fibre (regarded as a Galois module) is isomorphic to $\overline{\rho}|_{D_2}$, then both conditions are equivalent to V being local-local. For the first condition, this follows from the Eichler-Shimura relation and a calculation with Dieudonné modules; see [23, p. 113]. For the second, note that if V is not local-local, then it admits either a multiplicative or an étale subgroup scheme, either of which gives rise to an étale subgroup scheme of the generic fibre $V_{/\mathbf{Q}_2}$. Thus $\overline{\rho}|_{D_2}$ admits an unramified subrepresentation, and hence is not absolutely irreducible.

Conversely, if $\overline{\rho}|_{D_2}$ is absolutely reducible, then, extending scalars to $\mathbf{F}_4$ if necessary, it contains a one-dimensional subrepresentation, which (by local class field theory at 2) must be an unramified character. The Zariski closure in V (or in $\mathbf{F}_4 \otimes_{\mathbf{F}_2} V$) of this subrepresentation gives rise to a rank one subgroup scheme (or subvector space scheme) which is either étale or multiplicative. Thus V is not local-local. Of course, suitably modified forms of these arguments apply to any maximal ideal in $\mathbf{T}$ of residue characteristic prime to N (a not necessarily prime level); see, for example, [13, Thms. 2.5, 2.6].

The proof of Theorem 1.8 is motivated by the following considerations: If p is an odd prime and $\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow \mathrm{GL}_2(\mathbf{F}_p)$ is a surjective modular representation, then theorems of Wiles and Taylor–Wiles [37, 34] show that the universal minimal deformation ring $R_\emptyset$ attached to $\overline{\rho}$ is isomorphic to the universal minimal modular deformation ring $\mathbf{T}_\emptyset$ ($= \mathbf{T}_\mathfrak{m}$, since N is prime). Since $\mathbf{T}_\emptyset$ is a finite $W(\mathbf{F}_p) = \mathbf{Z}_p$ algebra with residue field $\mathbf{F}_p$, it is exactly equal to $\mathbf{Z}_p$ if and only if it is an étale $\mathbf{Z}_p$-algebra. On the other hand, since $R_\emptyset \cong \mathbf{T}_\emptyset$, this is equivalent to $R_\emptyset$ being étale over $\mathbf{Z}_p$, which is in turn equivalent to the reduced Zariski cotangent space of $R_\emptyset$ being trivial. Since by construction $R_\emptyset$ represents the minimal deformation functor, its reduced Zariski cotangent space considered as a set has cardinality equal to the number of minimal deformations

$$\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow \mathrm{GL}_2(\mathbf{F}_p[x]/(x^2))$$

of $\overline{\rho}$. Thus to prove that $\mathbf{T}_\mathfrak{m} \neq \mathbf{Z}_p$ it suffices to show that there exists a non-trivial minimal deformation of $\overline{\rho}$ to $\mathrm{GL}_2(\mathbf{F}_p[x]/(x^2))$.

In spirit, the proof of Theorem 1.8 follows this strategy; in other words, we determine whether or not $\mathbf{T}_\mathfrak{m} = \mathbf{Z}_2$ by a calculation on tangent spaces. A significant problem arises, however, since we are working in the case $p = 2$, whilst the method of Wiles and Taylor–Wiles applies only to $p > 2$. This is not a mere technical obstruction; many phenomena can occur when $p = 2$ that do not occur for odd p. To name two: the possible failure of $\mathbf{T}_\mathfrak{m}$ to be Gorenstein and the consequent failure of multiplicity one [21], and the fact that $\overline{\rho}$ can arise from a totally real extension of $\mathbf{Q}$. Calculations in the second case suggest that the Taylor–Wiles strategy for proving $R = \mathbf{T}$ in the minimal case will not work without some significant new idea, since the numerical coincidences that occur for odd p whilst balancing the Selmer and dual Selmer groups in the Greenberg–Wiles product formula (see, for example, the remarks of de Shalit [9], top of p. 442) do not occur in the case $p = 2$. Mark Dickinson [11] has proved an $R = \mathbf{T}$ theorem for $p = 2$; however, his result requires many non-trivial hypotheses, and indeed does not apply to any of the representations considered in Theorem 1.8, since the Taylor–Wiles auxiliary prime arguments fail when $p = 2$ and the image of $\overline{\rho}$ is dihedral. (The main application of [11] to date, has been to representations with image $\mathrm{SL}_2(\mathbf{F}_4) \simeq A_5$.) The recent preprint [20] establishes modularity lifting results at the prime $p = 2$ in some generality; nevertheless, these results do not apply to the situation we consider. Indeed, at least as stated the results of [20] require that $\overline{\rho}$ has non-solvable image, and in any case, they do not give the precise $R = \mathbf{T}$ statements that would be needed for applications to Theorem 1.8.

Thus, instead of appealing to any general modularity results, we show that $\mathbf{T}_{\mathfrak{m}}$ is bigger than $\mathbf{Z}_2$ by explicitly constructing (in certain situations) non-trivial deformations of $\overline{\rho}_{\mathfrak{m}}$ to $\mathbf{F}_2[x]/(x^2)$ that are demonstrably modular (and hence contribute to the reduced cotangent space of $\mathbf{T}_{\mathfrak{m}}$). The most difficult point is to show that these deformations are modular of the correct (minimal) level. We prove this via a level-lowering result for modular forms with values in Artinian $\mathbf{Z}_2$-algebras (Theorem 3.14 below). This level lowering result may be of independent interest; for example, it provides evidence that an $R = \mathbf{T}$ theorem should hold for those $\overline{\rho}$ of characteristic two to which it applies.

The proof of (3) when N is a prime power (but is not actually prime) is given in Section 4. In Section 5 we make some concluding remarks.

Let us close this introduction by pointing out that recently Dummigan [12] has provided a heuristic explanation for Watkins' rank conjecture that also relies on a hypothetical $R = \mathbf{T}$ theorem for the residual Galois representation $\overline{\rho}$ arising from the 2-torsion on an elliptic curve E: he uses the symmetric square map from $\overline{\rho}$ to $\mathrm{Sym}^2\overline{\rho}$ to lift elements from the 2-Selmer group of E to the tangent space to the deformation ring of $\overline{\rho}$. He also shows that the resulting tangent space elements can never be "trapped" (in the words of [37, p. 450]) by the Taylor–Wiles method of introducing auxiliary primes. Thus, although the experimental work of Watkins on the parity of modular degrees, together with the results of this paper and of [12], suggests the validity of an $R = \mathbf{T}$ theorem for (at least certain) residual Galois representations arising from the 2-torsion on elliptic curves, the proof of such a theorem seems out of the reach of current techniques.

2. N composite with at least two distinct prime factors

In this section we prove the following theorem.

2.1 Theorem: *If E is an elliptic curve of odd modular degree, then the conductor N of E is divisible by at most two odd primes, and E is of even analytic rank. Furthermore, if N is divisible by at least two primes, then E contains a rational 2-torsion point.*

We begin with a preliminary lemma. Let E be an elliptic curve over a field k; let O denote the origin of E. Let A denote the group of automorphisms of E as a curve over k (i.e. k-rational automorphisms of E that do not necessarily fix O), and suppose that W is a finite elementary abelian 2-subgroup of A.

2.2 Lemma: *The order of W divides twice the order of $E[2](k)$.*

Proof. Let A_0 denote the subgroup of A consisting of automorphisms of E as an elliptic curve over k (i.e. k-rational automorphisms of E that do fix O). The action of $E(k)$ on E via translation realizes $E(k)$ as a normal subgroup of A which has trivial intersection with A_0, and which together with A_0 generates A. Thus A sits in the split short exact sequence of groups

$$0 \to E(k) \to A \to A_0 \to 1. \tag{1}$$

(This is of course well-known. The surjection $A \to A_0$ may also be regarded as the map $A = \mathrm{Aut}(E) \to \mathrm{Aut}(\mathrm{Pic}^0(E))$ induced by the functoriality of the formation of Picard varieties — the target being the group of automorphisms of $\mathrm{Pic}^0(E)$ as a group variety — once we identify E and $\mathrm{Pic}^0(E)$ as group varieties in the usual way.)

The short exact sequence (1) induces a short exact sequence

$$0 \to W \cap E(k) \to W \to W_0 \to 1,$$

where W_0 denotes the projection of W onto A_0. The known structure of A_0 shows that W_0 is either trivial or of order 2. Since $W \cap E(k) \subset E[2](k)$, the lemma follows. ∎

Proof of Theorem 2.1. The discussion of Remark 1.3 shows that it suffices to prove the theorem under the additional assumption that E is an optimal quotient of $X_0(N)$.

Let W denote the group of automorphisms of $X_0(N)$ generated by the Atkin–Lehner involutions; W is an elementary abelian 2-group of rank equal to the number of primes dividing N. Since E is an optimal quotient of $X_0(N)$, the action of W on $X_0(N)$ descends to an action on E. If $w \in W$ were to act trivially on E, then the quotient map $X_0(N) \to E$ would factor through $X_0(N)/w$, contradicting our assumption that E is of odd modular degree. Thus Lemma 2.2 shows that W has order at most 8, and hence that N is divisible by at most 3 primes. Furthermore, if N is divisible by more than one prime, then it shows that $E[2](\mathbf{Q})$ is non-trivial.

Suppose now that N is odd, so that $X_0(N)$ and E both have good reduction at 2. We may then apply the argument of the preceding paragraph over $\mathbf{F}_2$, and so conclude from Lemma 2.2 that W has order at most 4. Hence N is divisible by at most two primes.

Recall that the sign of the functional equation of f is $-w_N$. If E is of odd analytic rank, and if f_E denotes the normalized newform of level N attached to E, then $w_N f_E = f_E$, and so the automorphism of E induced by w_N has trivial image in A_0. Thus w_N acts on E via translation by an element $P \in E(\mathbf{Q})$. Since w_N interchanges the cusps 0 and ∞ on $X_0(N)$, we see that $P = \pi(0) - \pi(\infty)$ (where $\pi : X_0(N) \to E$ is a modular parameterization of E, chosen so that $\pi(\infty) = O$).

The assumption that E has odd analytic rank also implies that $L(f_E, 1) = 0$. Since this L-value can be computed (up to a non-zero factor) by integrating f_E from 0 to ∞ in the upper half-plane, we conclude that $P = O$, and thus that w_N acts trivially on E. Hence π factors through the quotient $X_0(N)/w_N$ of $X_0(N)$, and so must be of even modular degree, a contradiction. ∎

3. N prime

3.1. Reductions.

3.1 Lemma: *Theorem 1.8 implies part (3) of theorem 1.1 for N prime.*

Proof. Suppose that E is an elliptic curve of conductor N, assumed to be optimal in its isogeny class. Let f_E be the associated Hecke eigenform of level $\Gamma_0(N)$ and weight 2. From a theorem of Ribet [38], $2|m_E$ if and only if f_E satisfies a congruence mod 2 with another cuspidal eigenform of level N. The set of cuspidal eigenforms (in characteristic zero) congruent to f is indexed by

$\mathrm{Hom}(\mathbf{T}_{\mathfrak{m}} \otimes \mathbf{Q}_2, \overline{\mathbf{Q}}_2)$. Thus f_E satisfies no non-trivial congruences if and only if $\mathbf{T}_{\mathfrak{m}} \otimes \mathbf{Q}_2 = \mathbf{Q}_2$, or equivalently if and only if $\mathbf{T}_{\mathfrak{m}} = \mathbf{Z}_2$. ∎

The following theorem of Grothendieck on Abelian varieties with semistable reduction [18, Exposé IX, Prop. 3.5] will be useful.

3.2 Theorem (Grothendieck): *Let A be an Abelian variety over $\mathbf{Q}$ with semistable reduction at ℓ. Let $I_\ell \subset \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ denote a choice of inertia group at ℓ. Then the action of I_ℓ on the p^n-division points of A for $p \neq \ell$ is rank two unipotent; i.e., as an endomorphism, for $\sigma \in I_\ell$,*

$$(\sigma - 1)^2 A[p^n] = 0.$$

In particular, I_ℓ acts through its maximal pro-p quotient, which is procyclic.

Shimura proved that a modular form f of weight 2 and level $\Gamma_0(N)$ gives rise to a modular Abelian variety A_f in such a way that the p-adic representations ρ_f attached to f arise from the torsion points of A_f. For prime N, these varieties are semistable at N, and so we may apply the theorem above to deduce that for $p = 2$, such representations ρ restricted to I_N factor through a pro-cyclic 2-group. For representations $\overline{\rho}$ with image inside $\mathrm{GL}_2(\mathbf{F}_2) \simeq S_3$, this means, in particular, that the order of inertia at N is either 1 or 2.

Let us now consider a Galois representation $\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \rightarrow \mathrm{GL}_2(\mathbf{F}_2)$, arising from a cuspidal Hecke eigenform of level $\Gamma_0(N)$, whose image is not contained in a Borel subgroup. (This is equivalent to $\overline{\rho}$ being irreducible, and also to the image of $\overline{\rho}$ having order divisible by 3.) Let L be the fixed field of the kernel of $\overline{\rho}$; the extension $L/\mathbf{Q}$ is unramified outside 2 and N. If $L/\mathbf{Q}$ is unramified at N, then $\overline{\rho}$ has Serre conductor 1, contradicting a theorem of Tate [33]. Thus by the discussion above we see that inertia at N factors through a group of order 2, that $L/\mathbf{Q}$ is an S_3-extension, and (hence) $\overline{\rho}$ is absolutely irreducible. Let $K/\mathbf{Q}$ be a cubic subfield of L, and let F be the quadratic extension inside L. Since $\overline{\rho}$ is finite flat at 2, it follows from Fontaine's discriminant bounds [16] that the power of 2 dividing the discriminant of $F/\mathbf{Q}$ is at most 4. Thus $F/\mathbf{Q}$ must be $\mathbf{Q}(\sqrt{\pm N})$ (as it is ramified at N). The extension L/F is unramified at the prime above N, since as explained above, $\overline{\rho}|_{I_N}$ has order dividing two. Moreover, the extension L/K is ramified at 2 if and only if $\overline{\rho}$ is supersingular, as follows from Remark 1.9.

3.3 Lemma: *If $\overline{\rho}$ is supersingular at two and L is not totally real, then $N \equiv 3 \bmod 8$. In particular, Theorem 1.1 implies Theorem 1.7.*

Proof. By class field theory the quadratic field $F/\mathbf{Q}$ admits a degree three extension ramified precisely at 2 only if 2 is unramified and inert in F. This occurs if and only if $N \equiv 3 \bmod 8$ and $F = \mathbf{Q}(\sqrt{-N})$, or $N \equiv 5 \bmod 8$ and $F = \mathbf{Q}(\sqrt{N})$. Moreover if $F = \mathbf{Q}(\sqrt{N})$, then K and L are totally real. ∎

We shall prove Theorem 1.8 by showing in the following subsections that if $\overline{\rho}$ satisfies at least one of the following conditions:

1. $\overline{\rho}$ is totally real;
2. $\overline{\rho}$ is unramified at 2;
3. $\overline{\rho}$ is ordinary, complex, and ramified at 2;

then $\mathbf{T}_{\mathfrak{m}} \neq \mathbf{Z}_2$.

3.2. $\overline{\rho}$ is totally real.

The theory of modular deformations is not well-understood when $\overline{\rho}$ is totally real. Thus our arguments in this section are geometric. We use the following theorem, due to Merel [25, Prop. 5]. (This interpretation of Merel's result is due to Agashe [1, Cor. 3.2.9]).

3.4 Theorem: *Let N be prime. Then $J_0(N)(\mathbf{R})$ is connected.*

If we let g denote the dimension of $J := J_0(N)$ it follows that $J(\mathbf{R}) \simeq (\mathbf{R}/\mathbf{Z})^g$, $J(\mathbf{R})^{\mathrm{tors}} \simeq (\mathbf{Q}/\mathbf{Z})^g$ and $J[2](\mathbf{R}) = (\mathbf{Z}/2\mathbf{Z})^g$.

Let $J[2^\infty] = \varinjlim J[2^m]$. Then $J[2^\infty]$ is a 2-divisible group over $\mathbf{Q}$ admitting an action of $\mathbf{T}_2$.

Since $\mathbf{T}_2$ is finite and flat over the complete local ring $\mathbf{Z}_2$ there exists a decomposition

$$\mathbf{T}_2 = \prod \mathbf{T}_{\mathfrak{m}},$$

where the product is taken over the maximal ideals $\mathfrak{m}$ of $\mathbf{T}$ of residue characteristic two. If $g(\mathfrak{m})$ denotes the rank of $\mathbf{T}_{\mathfrak{m}}$ over $\mathbf{Z}_2$, then

$$\sum_{\mathfrak{m}} g(\mathfrak{m}) = \mathrm{rank}(\mathbf{T}_2/\mathbf{Z}_2) = g.$$

If $J[\mathfrak{m}^\infty] := J[2^\infty] \otimes_{\mathbf{T}_2} \mathbf{T}_{\mathfrak{m}}$, then $J[2^\infty] \simeq \prod J[\mathfrak{m}^\infty]$ (compare [23, §7, p. 91]). From Lemma 7.7 of [23] we see that $\mathrm{Ta}_{\mathfrak{m}} J \otimes \mathbf{Q}_2$ is free of rank two over $\mathbf{T}_{\mathfrak{m}} \otimes \mathbf{Q}_2$ (where $\mathrm{Ta}_{\mathfrak{m}} J := \mathrm{Hom}(\mathbf{Q}_2/\mathbf{Z}_2, J[\mathfrak{m}^\infty](\overline{\mathbf{Q}}))$ is the $\mathfrak{m}$-adic Tate module of J), and thus that

$$J[\mathfrak{m}^\infty](\mathbf{C}) \cong (\mathbf{Q}_2/\mathbf{Z}_2)^{2g(\mathfrak{m})}. \qquad (2)$$

Let $J[2]_\mathfrak{m} := J[2] \otimes_{\mathbf{T}_2} \mathbf{T}_\mathfrak{m}$ be the 2-torsion subgroup scheme of $J[\mathfrak{m}^\infty]$.

3.5 Lemma: *For all maximal ideals $\mathfrak{m}$ of residue characteristic two there is an equality*

$$\dim_{\mathbf{Z}/2\mathbf{Z}}(J[2]_\mathfrak{m}(\mathbf{R})) = g(\mathfrak{m}).$$

Proof. The isomorphism (2) induces an isomorphism $J[2]_\mathfrak{m}(\mathbf{C}) \cong (\mathbf{Z}/2\mathbf{Z})^{2g(\mathfrak{m})}$. Let $\sigma \in \mathrm{Gal}(\mathbf{C}/\mathbf{R})$ denote complex conjugation. Then $(\sigma - 1)^2 J[2]_\mathfrak{m}(\mathbf{C}) = 0$. Thus $J[2]_\mathfrak{m}(\mathbf{R})$ (which is the kernel of $\sigma - 1$) has dimension at least $g(\mathfrak{m})$. If $\dim_{\mathbf{Z}/2\mathbf{Z}}(J_\mathfrak{m}[2](\mathbf{R})) > g(\mathfrak{m})$ for some $\mathfrak{m}$, then since

$$J[2](\mathbf{R}) = \prod J[2]_\mathfrak{m}(\mathbf{R}),$$

and since (as was noted above) $\dim_{\mathbf{Z}/2\mathbf{Z}}(J[2](\mathbf{R})) = g$, we would deduce the inequality:

$$g = \sum \dim_{\mathbf{Z}/2\mathbf{Z}}(J[2]_\mathfrak{m}(\mathbf{R})) > \sum_{\mathfrak{m}} g(\mathfrak{m}) = g,$$

which is absurd. ∎

Now let $\overline{\rho}$ be a totally real (absolutely) irreducible continuous modular representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ into $\mathrm{GL}_2(\mathbf{F}_2)$ of level $\Gamma_0(N)$, and let $\mathfrak{m}$ be the corresponding maximal ideal of $\mathbf{T}$. The main result of [2] shows that the $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-representation $J[\mathfrak{m}](\overline{\mathbf{Q}})$ is a direct sum of copies of $\overline{\rho}$. Thus, since $\overline{\rho}$ is totally real, we find that

$$\dim_{\mathbf{Z}/2\mathbf{Z}} J[\mathfrak{m}](\mathbf{R}) = \dim_{\mathbf{Z}/2\mathbf{Z}} J[\mathfrak{m}](\mathbf{C}) \geq \dim_{\mathbf{Z}/2\mathbf{Z}} \overline{\rho} = 2.$$

Combining this inequality with the inclusion $J[\mathfrak{m}](\mathbf{R}) \subseteq J[2]_\mathfrak{m}(\mathbf{R})$ and Lemma 3.5 we find that $g(\mathfrak{m}) \geq 2$, and thus that $\mathbf{T}_\mathfrak{m} \neq \mathbf{Z}_2$.

3.3. Rings of definition for modular forms. In this section, we explain what we mean by a modular form with coefficients in a ring R. Given a level structure $\Gamma := \Gamma_0(N)$ or $\Gamma_1(N)$ for some $N \geq 1$, and a weight k, the space of cuspforms $S_k(\Gamma, \mathbf{C})$ is unambiguously defined. For any subring R of $\mathbf{C}$, we let $S_k(\Gamma, R)$ denote the R-submodule of $S_k(\Gamma, \mathbf{C})$ consisting of cuspforms whose q-expansion coefficients lie in R. It is well-known that the natural map

$R \otimes_{\mathbf{Z}} S_k(\Gamma, \mathbf{Z}) \to S_k(\Gamma, R)$ is an isomorphism, and so for an arbitrary ring R we define $S_k(\Gamma, R) := R \otimes_{\mathbf{Z}} S_k(\Gamma, \mathbf{Z})$.

In the case when $\Gamma := \Gamma_1(N)$, the nebentypus action of $(\mathbf{Z}/N\mathbf{Z})^\times$ on $S_k(\Gamma, \mathbf{C})$ preserves $S_k(\Gamma, \mathbf{Z})$, and hence induces a nebentypus action on $S_k(\Gamma, R)$ for any R. If $\chi : (\mathbf{Z}/N\mathbf{Z})^\times \to \mathbf{C}^\times$ is a character, then letting $\mathbf{Z}[\chi]$ denote the subring of $\mathbf{C}$ generated by the values of χ, we let $S_k(\Gamma, \chi, \mathbf{Z}[\chi])$ denote the subspace of $S_k(\Gamma, \mathbf{Z}[\chi])$ consisting of cuspforms with nebentypus character χ. If R is any $\mathbf{Z}[\chi]$-algebra, then we let $S_k(\Gamma, \chi, R)$ denote the image of $R \otimes_{\mathbf{Z}[\chi]} S_k(\Gamma, \chi, \mathbf{Z}[\chi])$ under the tautological isomorphism $R \otimes_{\mathbf{Z}[\chi]} S_k(\Gamma, \mathbf{Z}[\chi]) \cong S_k(\Gamma, R)$. (This image is contained in the R-submodule of $S_k(\Gamma, R)$ consisting of cuspforms on which $(\mathbf{Z}/N\mathbf{Z})^\times$ acts through the character χ. However, if R is not flat over $\mathbf{Z}[\chi]$, then it need not coincide with this submodule.)

The following lemma confirms that certain elementary manipulations with the spaces $S_k(\Gamma, R)$ are permissible in the context of the above definitions.

3.6 Lemma: *If R is an $\mathbf{F}_2$-algebra, then the following maps are well-defined.*

1. *A map $S_1(\Gamma_1(M), \chi, R) \to S_2(\Gamma_0(M), R)$ which induces the identity on q-expansions, where M is any integer ≥ 1, and χ is an odd character of conductor dividing M and order two.*
2. *The level lowering map $U_2 : S_2(\Gamma_0(2^{k+1}M), R) \to S_2(\Gamma_0(2^k M), R)$, for any $M \geq 1$ and $k \geq 1$.*

Proof. It suffices to treat the case $R = \mathbf{F}_2$, since there is, by definition, an isomorphism $R \otimes_{\mathbf{F}_2} S_k(\Gamma, \mathbf{F}_2) \cong S_k(\Gamma, R)$. For part (1), lift $f \in S_1(\Gamma_1(M), \chi, \mathbf{F}_2)$ to characteristic zero (possible, by definition), and then multiply by the Eisenstein series $E_{1,\chi}$. We obtain a form g of level $\Gamma_0(M)$ which we then reduce to obtain the desired map. Similarly, for part (2), lift f to characteristic zero. The operator U_2 reduces the level (provided that $k \geq 1$) and preserves the integrality of q-expansions at ∞. Hence the reduction of $g = U_2 f$ lies in $S_2(\Gamma_0(2^k N), \mathbf{F}_2)$. ∎

Let $\mathbf{T}$ denote the $\mathbf{Z}$-algebra of endomorphisms of $S_k(\Gamma, \mathbf{C})$ (or equivalently, of $S_k(\Gamma, \mathbf{Z})$) generated by the Hecke operators. The algebra $\mathbf{T}$ acts on $S_k(\Gamma, \mathbf{Z})$, and hence acts on $S_k(\Gamma, R)$ for any ring R. Furthermore, the usual pairing $\langle f, T \rangle := a_1(Tf)$ ($f \in S_k(\Gamma, R)$, $T \in \mathbf{T}$) induces an isomorphism $S_k(\Gamma, R) \cong \mathrm{Hom}(\mathbf{T}, R)$ [29, Thm. 2.2]. (Here Hom means simply Hom of abelian groups.) A cuspform $h \in S_k(\Gamma, R)$ is an eigenform for all the Hecke operators precisely when the associated homomorphism $\mathbf{T} \to R$ is a ring homomorphism.

If $\mathfrak{m}$ is a maximal ideal in $\mathbf{T}$, then the quotient map $\mathbf{T} \to \mathbf{T}/\mathfrak{m}$ corresponds to an eigenform $\overline{f}_{\mathfrak{m}}$ defined over the finite field $\mathbf{T}/\mathfrak{m}$, associated to which is a semi-simple Galois representation $\overline{\rho}_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{T}/\mathfrak{m})$. If this Galois representation is absolutely irreducible, then Carayol [7, Thm. 3] (building on constructions of Deligne, Shimura, and Serre) has constructed a lifting to a continuous representation $\rho_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{T}_{\mathfrak{m}})$.

Let R be a complete local ring, with maximal ideal $\mathfrak{n}$, such that $R/\mathfrak{n}$ has positive residue characteristic. If $f \in S_k(\Gamma, R)$ is a Hecke eigenform, then f corresponds to a ring homomorphism $\phi : \mathbf{T} \to R$, which extends to a homomorphism $\mathbf{T}_{\mathfrak{m}} \to R$ for some maximal ideal $\mathfrak{m}$ (the preimage of $\mathfrak{n}$ under ϕ). (The eigenform f can be thought of as a lifting of the eigenform $\overline{f}_{\mathfrak{m}}$ to the ring R.) If $\overline{\rho}_{\mathfrak{m}}$ is absolutely irreducible, then pushing forward $\rho_{\mathfrak{m}}$ via ϕ, we obtain an $\mathfrak{n}$-adically continuous representation $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(R)$, which we refer to as the Galois representation associated to f.

Let $\mathfrak{m}$ be a maximal ideal of $\mathbf{T}$ for which $\mathbf{T}/\mathfrak{m} = \mathbf{F}_2$. The completion $\mathbf{T}_{\mathfrak{m}}$ is naturally a finite flat $\mathbf{Z}_2$-algebra, of say some rank $r > 0$. The isomorphism $\mathrm{Hom}(\mathbf{T}, \mathbf{F}_2) \cong S_k(\Gamma, \mathbf{F}_2)$ induces an isomorphism $\mathrm{Hom}(\mathbf{T}_{\mathfrak{m}}, \mathbf{F}_2) \cong S_k(\Gamma, \mathbf{F}_2)[\mathfrak{m}^\infty]$. (Here the target is the subspace consisting of cuspforms annihilated by some power of $\mathfrak{m}$.) Thus $\dim_{\mathbf{F}_2}(S_k(\Gamma, \mathbf{F}_2)[\mathfrak{m}^\infty]) = r$. In particular, we obtain the following lemma.

3.7 Lemma: *If there exist non-zero elements f, $g \in S_2(\Gamma, \mathbf{F}_2)$ such that $\mathfrak{m}f = \mathfrak{m}^2 g = 0$, while $\mathfrak{m}g \neq 0$, then $\mathbf{T}_{\mathfrak{m}} \neq \mathbf{Z}_2$.*

Proof. The existence of the elements f and g shows that

$$\dim_{\mathbf{F}_2}(S_k(\Gamma, \mathbf{F}_2)[\mathfrak{m}^\infty]) > 1. \qquad \blacksquare$$

If the level N of Γ is invertible in R, then we may also define the space of Katz modular forms of level Γ and weight k over R, as certain rules on elliptic curves with Γ-level structure defined over R-schemes, following the prescription of [19]. If $k \geq 2$, and if $\Gamma = \Gamma_1(N)$ with $N \geq 5$, then there is a natural isomorphism $S_k^{\mathrm{Katz}}(\Gamma, R) \cong S_k(\Gamma, R)$, uniquely determined by its compatibility with the formation of q-expansions. In the case when $\Gamma = \Gamma_0(N)$, the comparison of $S_k^{\mathrm{Katz}}(\Gamma, R)$ and $S_k(\Gamma, R)$ is more complicated, due to the fact that the modular curve $X_0(N)$ need not be a fine moduli space. (In the case when N is prime and $k = 2$, a detailed study of their relationship is given in [23, §II.4]. We will not need to apply any of the results of this study.)

3.4. $\overline{\rho}$ IS UNRAMIFIED AT 2. We now return to the situation of Theorem 1.8. Suppose that $\overline{\rho}$ is unramified at 2. This forces $\overline{\rho}$ to be ordinary. By the theory of companion forms [17] one expects that $\overline{\rho}$ arises from a mod 2 form of level $\Gamma_1(N)$ and weight 1. Although the results of [17] do not apply in this case, Wiese [36] explicitly constructs such forms when the image of $\overline{\rho}$ is dihedral, as it is in our situation. Let $f \in S_1^{\mathrm{Katz}}(\Gamma_1(N), \mathbf{F}_2)$ be this companion form for $\overline{\rho}$. Let A be the Hasse invariant modulo 2, which is a (Katz) modular form (not a cuspform) of level one with q expansion given by 1. Then Af and $g = f^2$ are elements of $S_2^{\mathrm{Katz}}(\Gamma_1(N), \mathbf{F}_2)$, and thus of $S_2(\Gamma_1(N), \mathbf{F}_2)$. (Note that it is no loss of generality to assume that $N \geq 5$, since $X_1(N)$ has genus zero for $1 \leq N \leq 4$.) Wiese's construction furthermore allows us to choose f, and hence Af and g, so as to have trivial nebentypus. A lemma of Carayol [6, §4.4][2] then assures us that Af and g in fact lie in $S_2(\Gamma_1(N), 1, \mathbf{F}_2)$ (where, in this notation, 1 denotes the trivial character of $(\mathbf{Z}/N\mathbf{Z})^\times$), that is, that Af and g lie in $S_2(\Gamma_0(N), \mathbf{F}_2)$. If f has q-expansion $f = \sum_{n=1}^\infty a_n q^n$, then Af has the same q-expansion, while g has q-expansion $g = \sum_{n=1}^\infty a_n^2 q^{2n} \equiv V_2 f$, since $a_n \in \mathbf{F}_2$. Since $a_1 = 1$, we see that f and g are linearly independent. Furthermore, one computes that $(T_\ell - a_\ell)f = (T_\ell - a_\ell)g = 0$ for all odd ℓ, that $(T_2 - a_2)f = 0$ and $(T_2 - a_2)^2 g = 0$, and that $(T_2 - a_2)g \neq 0$. Thus $\mathfrak{m}f = \mathfrak{m}^2 g = 0$, while $\mathfrak{m}g \neq 0$, and therefore, by Lemma 3.7, $\mathbf{T}_\mathfrak{m} \neq \mathbf{Z}_2$ and we are done.

In fact, one can avoid the appeal to Carayol's lemma in the above argument. The only difficult point of Wiese's construction is the case when $\overline{\rho}$ is totally real, and this case of Theorem 1.8 is already covered by Section 3.2. If we assume that $\overline{\rho}$ is not totally real, then we may construct f directly as an element of $S_1(\Gamma_1(N), \chi)$ for some character χ. (See the first paragraph of the proof of [36, Thm. 9].) One can then define $Af \in S_2(\Gamma_0(N), \mathbf{F}_2)$ by applying the map of Lemma 3.6 (1) to f, as well as $g = f^2 \in S_2(\Gamma_0(N), \mathbf{F}_2)$. The argument then proceeds just as above.

[2] The calculations of the following paragraph show that f and g are eigenforms for the Hecke operators T_ℓ for every prime ℓ not dividing $2N$, with eigenvalue equal to the trace of the image under $\overline{\rho}$ of Frobenius at ℓ. Since $\overline{\rho}$ is not induced from a character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(i))$ (we saw above that it is rather induced from a cubic character of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{\pm N}))$), Carayol's lemma applies.

3.5. $\overline{\rho}$ IS ORDINARY, COMPLEX AND RAMIFIED AT 2. Suppose that $\overline{\rho}$ is ordinary, complex and ramified at 2. It follows that $F/\mathbf{Q}$ is complex and ramified at 2, and thus that $F = \mathbf{Q}(\sqrt{-N})$ for some $N \equiv 1 \bmod 4$. Moreover, the extension L/F is unramified everywhere. Since $N \equiv 1 \bmod 4$ it follows that $H := L(\sqrt{-1})$ is also unramified everywhere over F. The field H is Galois over $\mathbf{Q}$, and clearly

$$\mathrm{Gal}(H/\mathbf{Q}) \simeq S_3 \times \mathbf{Z}/2\mathbf{Z}. \tag{3}$$

We may embed $S_3 \times \mathbf{Z}/2\mathbf{Z}$ into $\mathrm{GL}_2(\mathbf{F}_2[x]/(x^2))$ by fixing an identification of S_3 with $\mathrm{GL}_2(\mathbf{F}_2)$, and mapping a generator of $\mathbf{Z}/2\mathbf{Z}$ to the matrix

$$\begin{pmatrix} 1+x & 0 \\ 0 & 1+x \end{pmatrix}.$$

Composing the isomorphism (3) with this embedding yields a representation:

$$\rho : \mathrm{Gal}(H/\mathbf{Q}) \hookrightarrow \mathrm{GL}_2(\mathbf{F}_2[x]/(x^2)).$$

The representation ρ has trivial determinant (equivalently, determinant equal to the mod 2 cyclotomic character). We also claim that ρ is finite flat at two. To check this, it suffices to prove this over $\mathbf{Z}_2^{\mathrm{ur}}$. The representation $\rho|_{\mathrm{Gal}(\overline{\mathbf{Q}}_2/\mathbf{Q}_2^{\mathrm{ur}})}$ factors through a group of order 2, and one explicitly sees that it arises as the generic fibre of the group scheme $(D \oplus D)/\mathbf{Z}_2^{\mathrm{ur}}$, where D is the non-trivial extension of $\mathbf{Z}/2\mathbf{Z}$ by μ_2 considered in [23, Prop 4.2, p. 58]. Thus one expects ρ to arise from an $\mathbf{F}_2[x]/(x^2)$-valued modular form of weight two and level N, corresponding to a surjective map of rings $\mathbf{T}_{\mathfrak{m}} \to \mathbf{F}_2[x]/(x^2)$. This would follow if we knew that $\mathbf{T}_{\mathfrak{m}}$ coincided with the minimal deformation ring associated to $\overline{\rho}$. Rather than proving this, however, we shall use weight one forms to explicitly construct a weight two modular form giving rise to ρ.

Let χ_{4N} be the character of conductor $4N$ associated to F. Consider two faithful representations

$$\psi_1 : \mathrm{Gal}(L/\mathbf{Q}) \cong S_3 \hookrightarrow \mathrm{GL}_2(\mathbf{C}), \quad \psi_2 : \mathrm{Gal}(H/\mathbf{Q}) \cong S_3 \times \mathbf{Z}/2\mathbf{Z} \hookrightarrow \mathrm{GL}_2(\mathbf{C}).$$

Since $F/\mathbf{Q}$ is complex, these dihedral representations are odd and therefore give rise to weight one modular forms h_1, h_2 in $S_1(\Gamma_1(4N), \chi_{4N}, \mathbf{C})$.

3.8 LEMMA: *The modular forms h_1, h_2 are ordinary at 2, have coefficients in $\mathbf{Z}$, and are congruent modulo 2. Let*

$$g = \frac{(h_2 - h_1)}{2} \in \mathbf{Z}[[q]].$$

Then $g \bmod 2$ *is non-zero, and the form* $h{=}h_1{+}xg \in S_1(\Gamma_1(4N), \chi_{4N}, \mathbf{F}_2[x]/(x^2))$ *is an eigenform for all the Hecke operators, including* U_2*. The* $\mathrm{GL}_2(\mathbf{F}_2[x]/(x^2))$*-valued Galois representation associated to* h *is isomorphic to* ρ*.*

Proof. The modular forms are both ordinary at 2 because the representations ψ_1 and ψ_2 have non-trivial subspaces on which inertia at two is trivial (since I_2 acts through a group of order 2). They both have coefficients in $\mathbf{Z}$, since $2\cos(\pi/3) \in \mathbf{Z}$. The congruence $h_1 \equiv h_2 \bmod 2$ follows from the fact that both are ordinary-at-2 Hecke eigenforms, and that $a(h_1, \ell) = a(h_2, \ell)\chi_4(\ell)$ for all odd primes ℓ, where χ_4 is the character of conductor 4. From this one also sees that g is non-trivial modulo two, and that h_1, h_2, g define forms in $S_1(\Gamma_1(4N), \chi_{4N}, \mathbf{Z})$. Thus, by definition, $h \in S_1(\Gamma_1(4N), \chi_{4N}, \mathbf{F}_2[x]/(x^2))$. The claim that h is a Hecke eigenform follows formally (on q-expansions) from the fact that h_1 and h_2 are Hecke eigenforms that are congruent modulo 2. The discussion of Section 3.3 implies the existence of a Galois representation associated to h, which by comparing traces of Frobenius one easily sees is isomorphic to ρ. ∎

Now that we have constructed the weight one form h of level $4N$ giving rise to ρ, we would like to construct a corresponding weight two form of level N. Applying the map of Lemma 3.6 (1) (concretely, multiplying h by the Eisenstein series in $M_1(\Gamma_1(4N), \chi_{4N})$), we see that there is a modular form $h' \in S_2(\Gamma_0(4N), \mathbf{F}_2[x]/(x^2))$ having the same q-expansion as h. Since h, and hence h', is an ordinary U_2 eigenform, we may apply the U_2 operator to deduce (using Lemma 3.6 (2)) that $h' \in S_2(\Gamma_0(2N), \mathbf{F}_2[x]/(x^2))$. Applying Theorem 3.14 (proved in the following subsection) we then deduce that in fact $h' \in S_2(\Gamma_0(N), \mathbf{F}_2[x]/(x^2))$, and (thus) that there is a modular form $g' \in S_2(\Gamma_0(N), \mathbf{F}_2)$ having the same q-expansion as g.

As in the discussion of Section 3.3, let $\overline{f}_{\mathfrak{m}} \in S_2(\Gamma_0(N), \mathbf{F}_2)$ be the Hecke eigenform associated to $\mathfrak{m}$. Then $\mathfrak{m}\overline{f}_{\mathfrak{m}} = 0$, while an easy calculation shows that $\mathfrak{m}g \subset \mathbf{F}_2\overline{f}_{\mathfrak{m}} \setminus \{0\}$, and so also that $\mathfrak{m}^2 g = 0$. We conclude from Lemma 3.7 that $\mathbf{T}_{\mathfrak{m}} \neq \mathbf{Z}_2$.

3.6. Level-lowering for modular deformations.

The goal of this section is to prove a level-lowering result for modular forms with coefficients in Artinian rings that strengthens the case $p = 2$ of [13, Thm. 2.8] (which in turn extends a level lowering result proved by Mazur [30, Thm. 6.1] in the odd prime case).

We first establish a version of the multiplicity one theorem [37, Thm. 2.1] for $p = 2$. Under the additional assumption that $\overline{\rho}$ is not finite at 2, this theorem was proved in [4, §2] (as was the corresponding result for odd level). Thus the key point in our theorem is that $\overline{\rho}$ is allowed to be finite at 2, even though the level is taken to be even.

3.9 Theorem: *Let N be an odd natural number, and let $\mathbf{T}$ denote the full $\mathbf{Z}$-algebra of Hecke operators acting on weight two cuspforms of level $\Gamma_0(2N)$. If $\mathfrak{m}$ is a maximal ideal in $\mathbf{T}$ whose residue field k is of characteristic 2, and for which the associated residual Galois representation*

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(k)$$

is (absolutely) irreducible, ordinary, and ramified at 2, then $\mathrm{Ta}_{\mathfrak{m}} J_0(2N)$ (the $\mathfrak{m}$-adic Tate module of $J_0(2N)$) is free of rank two over the completion $\mathbf{T}_{\mathfrak{m}}$.

To be clear, the condition "ordinary at 2" means that the image of a decomposition group at 2 under $\overline{\rho}$ lies in a Borel subgroup of $\mathrm{GL}_2(k)$. Since k is of characteristic 2, we see that (for an appropriate choice of basis) the restriction of $\overline{\rho}$ to an inertia group at 2 may be written in the form

$$\overline{\rho}_{|I_2} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

The assumption that $\overline{\rho}$ is ramified at 2 then implies that $*$ is not identically zero. Thus the representation space of $\overline{\rho}$ has a unique line invariant under I_2, and so $\overline{\rho}$ is irreducible if and only if it is absolutely irreducible.

3.10 Lemma: *Let k be a finite field of characteristic 2. If*

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbf{Q}}_2/\mathbf{Q}_2) \to \mathrm{GL}_2(k)$$

is a continuous representation that is finite, ordinary, and ramified at 2, then $\overline{\rho}$ has a unique finite flat prolongation over $\mathbf{Z}_2$ (up to unique isomorphism). Furthermore, this prolongation is an extension of a rank one étale k-vector space scheme by a rank one multiplicative k-vector space scheme.

Proof. Any finite flat group scheme that prolongs an unramified continuous representation of

$$\mathrm{Gal}(\overline{\mathbf{Q}}_2/\mathbf{Q}_2)$$

on a one-dimensional k-vector space is either étale or multiplicative. Thus there are a priori four possible structures for a finite flat prolongation of $\overline{\rho}$: étale extended by étale; multiplicative extended by multiplicative; multiplicative extended by étale; or étale extended by multiplicative. However, all but the last possibility necessarily gives rise to an unramified generic fibre (note that any extension of multiplicative by étale must split, by a consideration of the connected étale sequence). Thus, since we assume $\overline{\rho}$ to be ramified, we see that any prolongation of $\overline{\rho}$ must be an extension of a rank one étale k-vector space scheme scheme by a rank one multiplicative k-vector space scheme.

To see that such a prolongation is unique, consider the maximal and minimal prolongations M and M' of $\overline{\rho}$ to a finite flat group scheme [27, Cor. 2.2.3]. Since étale (and hence multiplicative) group schemes are determined by their generic fibre, the result of the preceding paragraph shows that the natural morphism $M \to M'$ necessarily induces an isomorphism on the connected components of the identity, and on the corresponding groups of connected components (i.e., the corresponding maximal étale quotients). By the 5-lemma, this morphism is thus an isomorphism, and the lemma follows. ∎

We now show that certain results of Mazur [24] cited in the proof of [37, Thm. 2.1] extend to the case $p = 2$. We put ourselves in the context of [24, §1], and use the notation introduced therein. Namely, let K denote a finite extension of $\mathbf{Q}_p$ for some prime p, and let $\mathcal{O}$ denote the ring of integers of K. If A is an abelian variety over K, then let $A_{/\mathcal{O}}$ denote the **connected component of the identity of** the Néron model of A over $\operatorname{Spec}\mathcal{O}$. For any power p^r of p, the p^r-torsion subgroup scheme $A[p^r]_{/\mathcal{O}}$ of $A_{/\mathcal{O}}$ is then a quasi-finite flat group scheme over $\operatorname{Spec}\mathcal{O}$; we let $FA[p^r]_{/\mathcal{O}}$ denote its maximal finite flat subgroup scheme, and $A[p^r]^0_{/\mathcal{O}}$ denote the maximal connected closed subgroup scheme of $A[p^r]_{/\mathcal{O}}$. Since we took $A_{/\mathcal{O}}$ to be the connected component of the Néron model of A, the inductive limit $FA[p^\infty]_{/\mathcal{O}} := \varinjlim FA[p^r]_{/\mathcal{O}}$ is a p-divisible group, and $A[p^\infty]^0_{/\mathcal{O}} := \varinjlim A[p^r]^0_{/\mathcal{O}}$ is the maximal connected p-divisible subgroup of $FA[p^\infty]_{/\mathcal{O}}$.

The following proposition is a variation on [24, Prop. 1.3], in which we allow the ramification of K over $\mathbf{Q}_p$ to be unrestricted, at the expense of imposing more restrictive hypotheses on the reduction of the abelian varieties appearing in the exact sequence under consideration.

3.11 Proposition: *Let $0 \to A \to B \to C \to 0$ be an exact sequence of abelian varieties over K such that A has purely toric reduction, whilst C has good reduction. Then the induced sequence of p-divisible groups*

$$0 \to A[p^\infty]^0_{/\mathcal{O}} \to B[p^\infty]^0_{/\mathcal{O}} \to C[p^\infty]^0_{/\mathcal{O}} \to 0$$

is a short exact sequence of p-divisible groups over $\operatorname{Spec}\mathcal{O}$. *Equivalently, for any power p^r of p, the induced sequence*

$$0 \to A[p^r]^0_{/\mathcal{O}} \to B[p^r]^0_{/\mathcal{O}} \to C[p^r]^0_{/\mathcal{O}} \to 0$$

is a short exact sequence of finite flat group schemes over $\operatorname{Spec}\mathcal{O}$.

Proof. Since A has purely toric reduction, the group scheme $A[p^r]^0_{/\mathcal{O}}$ is of multiplicative type for each r. Thus it necessarily maps isomorphically onto its scheme theoretic image in $B_{/\mathcal{O}}$, and thus the induced map $A[p^\infty]^0_{/\mathcal{O}} \to B[p^\infty]^0_{/\mathcal{O}}$ is a closed embedding.

Let $C' \subset B$ be an abelian subvariety chosen so that the induced map $C' \to C$ is an isogeny. Then C' also has good reduction, and so $C'[p^\infty]^0_{/\mathcal{O}} \to C[p^\infty]^0_{/\mathcal{O}}$ is an epimorphism of p-divisible groups over $\operatorname{Spec}\mathcal{O}$. Thus the induced map $B[p^\infty]^0_{/\mathcal{O}} \to C[p^\infty]^0_{/\mathcal{O}}$ is also an epimorphism of p-divisible groups. A consideration of generic fibres shows that the kernel of this surjection coincides with the scheme-theoretic image of $A[p^\infty]^0_{/\mathcal{O}}$ in $B[p^\infty]^0_{/\mathcal{O}}$, and so the proposition is proved. ∎

Proof of Theorem 3.9. We closely follow the method of proof of Theorem 2.1 (ii) in [37] in the case when "$\Delta_{(p)}$ is trivial $\bmod \mathfrak{m}$" (in the terminology of that proof; see [37, pp. 485–488]). If we let A denote the connected part of the kernel of the map $J_0(2N) \to J_0(N) \times J_0(N)$ induced by Albanese functoriality applied to the two "degeneracy maps" from level $2N$ to level N, then A is an abelian subvariety of $J_0(2N)$ having purely toric reduction at 2, whilst the quotient B of $J_0(2N)$ by A has good reduction at 2. From Proposition 3.11 we obtain (for any $r \geq 1$) the short exact sequence

$$0 \to A[2^r]^0_{/\mathbf{Z}_2} \to J_0(2N)[2^r]^0_{/\mathbf{Z}_2} \to B[2^r]^0_{/\mathbf{Z}_2} \to 0$$

of connected finite flat group schemes over $\operatorname{Spec}\mathbf{Z}_2$. By functoriality of the formation of this short exact sequence, and since A is a $\mathbf{T}$-invariant subvariety of $J_0(2N)$, we see that this is in fact a short exact sequence of $\mathbf{T}$-module schemes.

If G is a 2-power torsion commutative group scheme over some base S, with an action of $\mathbf{T}$, and hence of $\mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{T}$, via endomorphisms, then by the localization $M_{\mathfrak{m}}$ we mean the kernel $G[\varepsilon']$, where the idempotent $\varepsilon' \in \mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{T}$ is defined as $\varepsilon' := 1 - \varepsilon$, with $\varepsilon \in \mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{T}$ being the idempotent corresponding to the direct factor $\mathbf{T}_{\mathfrak{m}}$ of $\mathbf{Z}_2 \otimes_{\mathbf{Z}} \mathbf{T}$. Since ε and ε' are orthogonal idempotents (by construction), the natural map $G[\varepsilon] \bigoplus G[\varepsilon'] \cong G$ is an isomorphism. Thus passage to $G_{\mathfrak{m}}$ is an exact functor on the category of 2-power torsion $\mathbf{T}$-module schemes over S.

In particular, localizing the above short exact sequence at $\mathfrak{m}$ induces the corresponding short exact sequence

$$0 \to A[2^r]^0_{\mathfrak{m}/\mathbf{Z}_2} \to J_0(2N)[2^r]^0_{\mathfrak{m}/\mathbf{Z}_2} \to B[2^r]^0_{\mathfrak{m}/\mathbf{Z}_2} \to 0. \tag{4}$$

Passing to $\overline{\mathbf{Q}}_2$-valued points induces a short exact sequence of $\mathrm{Gal}(\overline{\mathbf{Q}}_2/\mathbf{Q}_2)$-modules

$$0 \to A[2^r]^0_{\mathfrak{m}}(\overline{\mathbf{Q}}_2) \to J_0(2N)[2^r]^0_{\mathfrak{m}}(\overline{\mathbf{Q}}_2) \to B[2^r]^0_{\mathfrak{m}}(\overline{\mathbf{Q}}_2) \to 0, \tag{5}$$

which is a subexact sequence of the short exact sequence of $\mathrm{Gal}(\overline{\mathbf{Q}}_2/\mathbf{Q}_2)$-modules

$$0 \to A[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2) \to J_0(2N)[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2) \to B[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2) \to 0. \tag{6}$$

Let $A[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)^{\chi}$ (respectively $J_0(2N)[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)^{\chi}$, respectively $B[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)^{\chi}$) denote the maximal $\mathrm{Gal}(\overline{\mathbf{Q}}_2/\mathbf{Q}_2)$-subrepresentation of $A[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)$ (respectively $J_0(2N)[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)$, respectively $B[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)$) on which the inertia group acts through the 2-adic cyclotomic character χ. The short exact sequence (6) induces an exact sequence

$$0 \to A[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)^{\chi} \to J_0(2N)[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)^{\chi} \to B[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)^{\chi}. \tag{7}$$ ∎

3.12 Lemma: *Each of the groups schemes appearing in the exact sequence* (4) *is of multiplicative type, and the exact sequences* (5) *and* (7) *coincide (as subsequences of* (6)*).*

Proof. We first remark that (6) is the exact sequence of $\mathbf{T}_{\mathfrak{m}}[\mathrm{Gal}(\overline{\mathbf{Q}}_2/\mathbf{Q}_2)]$-modules underlying the corresponding exact sequence of $\mathbf{T}_{\mathfrak{m}}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-modules

$$0 \to A[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}) \to J_0(2N)[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}) \to B[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}) \to 0.$$

Since $\overline{\rho}$ is assumed irreducible as a $k[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-representation, each of the modules appearing in this exact sequence is a successive extension of copies of $\overline{\rho}$. The same is thus true of each of the modules appearing in the exact sequence (6).

Since A has purely toric reduction, it is clear that $A[2^r]^0_{\mathfrak{m}/\mathbf{Z}_2}$ is of multiplicative type, and so

$$A[2^r]^0_{\mathfrak{m}}(\overline{\mathbf{Q}}_2) \subset A[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)^{\chi}. \tag{8}$$

Fix a filtration $0 = W_0 \subset W_1 \subset \cdots \subset W_n = A[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)$ of $A[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)$ for which the successive quotients W_{i+1}/W_i are isomorphic to $\overline{\rho}$. Since A has purely toric reduction the quotient $A[2^r]_{/\mathbf{Q}_2}/A[2^r]^0_{/\mathbf{Q}_2}$ is Cartier dual to $\hat{A}[2^r]^0_{/\mathbf{Q}_2}$ (where $\hat{A}$ is the dual abelian variety to A), and so $A[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)/A[2^r]^0_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)$ is an unramified $\mathrm{Gal}(\overline{\mathbf{Q}}_2/\mathbf{Q}_2)$-representation. Since $\overline{\rho}$ is assumed ramified at 2, this implies that

$$W_i \cap A[2^r]^0_{\mathfrak{m}}(\overline{\mathbf{Q}}_2) \subsetneq W_{i+1} \cap A[2^r]^0_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)$$

for each $i \geq 0$. Furthermore,

$$W_{i+1} \not\subset A[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)^{\chi} + W_i$$

for each $i \geq 0$, because χ mod 2 is trivial. Since $W_{i+1}/W_i \cong \overline{\rho}$ is two dimensional over k for each $i \geq 0$, we conclude by induction on i that

$$W_i \cap A[2^r]^0_{\mathfrak{m}}(\overline{\mathbf{Q}}_2) = W_i \cap A[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)^{\chi}$$

for each $i \geq 0$. Taking $i = n$ then shows that the inclusion (8) is in fact an equality.

Since B has good reduction at 2, we have equality $FB[2^r]_{/\mathbf{Z}_2} = B[2^r]_{/\mathbf{Z}_2}$. As noted above, any Jordan–Hölder filtration of the localization $B[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}})$ as a $\mathbf{T}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module has all its associated graded pieces isomorphic to $\overline{\rho}$. Taking scheme-theoretic closures of such a filtration in $B[2^r]_{/\mathbf{Z}_2}$, we obtain a filtration of the localization $B[2^r]_{\mathfrak{m}/\mathbf{Z}_2}$ by finite flat closed subgroup schemes, whose associated graded pieces are prolongations of $\overline{\rho}$. Now Lemma 3.10 shows that the connected component of any such finite flat prolongation is multiplicative. Thus $B[2^r]^0_{\mathfrak{m}/\mathbf{Z}_2}$ is indeed multiplicative, whilst $B[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)/B[2^r]^0_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)$ is an unramified $\mathrm{Gal}(\overline{\mathbf{Q}}_2/\mathbf{Q}_2)$-module. Arguing as in the preceding paragraph gives the required equality

$$B[2^r]^0_{\mathfrak{m}}(\overline{\mathbf{Q}}_2) = B[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)^{\chi}.$$

Since any extension of multiplicative type groups is again of multiplicative type, we see that $J_0(2N)[2^r]^0_{\mathfrak{m}/\mathbf{Z}_2}$ is also of multiplicative type, and that the exact sequence (5) is a subsequence of the exact sequence (7). We have furthermore shown that first and third non-trivial terms of these two sequences coincide. This implies that these exact sequences do indeed coincide. ∎

Specializing Lemma 3.12 to the case $r = 1$ shows that $J_0(2N)[2]^0_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)$ is the maximal unramified $\mathrm{Gal}(\overline{\mathbf{Q}}_2/\mathbf{Q}_2)$-subrepresentation of $J_0(2N)[2]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)$ (since χ mod 2 is trivial). Recall that there is a natural isomorphism

$$\mathrm{Tan}(J_0(2N)[2]^0_{/\overline{\mathbf{F}}_2}) \cong \mathrm{Tan}(J_0(2N)_{/\overline{\mathbf{F}}_2})$$

(indeed, this is true with $J_0(2N)_{/\overline{\mathbf{F}}_2}$ replaced by any group scheme over $\overline{\mathbf{F}}_2$), and also a natural isomorphism $\mathrm{Tan}(J_0(2N)[2]^0_{/\overline{\mathbf{F}}_2}) \cong J_0(2N)[2]^0(\overline{\mathbf{Q}}_2) \otimes_{\mathbf{F}_2} \overline{\mathbf{F}}_2$ (as follows from the discussion on [37, p. 488]). Localizing at $\mathfrak{m}$, and taking into account [37, Lem. 2.2], which is valid for $p = 2$, we find that $J_0(2N)[2]^0_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)$ is a cyclic $\mathbf{T}_{\mathfrak{m}}$-module, and thus that the maximal unramified $\mathrm{Gal}(\overline{\mathbf{Q}}_2/\mathbf{Q}_2)$-subrepresentation of $J_0(2N)[2]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2)$ is a cyclic $\mathbf{T}_{\mathfrak{m}}$-module.

Let $\rho_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{T}_{\mathfrak{m}})$ denote the Galois representation associated to $\mathfrak{m}$ by [7, Thm. 3]. Carayol has proved [7, Thm. 4] that there is an isomorphism $\mathrm{Ta}_{\mathfrak{m}} J_0(2N) \cong J \otimes_{\mathbf{T}_{\mathfrak{m}}} \rho_{\mathfrak{m}}$ for some ideal J in $\mathbf{T}_{\mathfrak{m}}$, and thus an isomorphism $J_0(2N)[2]_{\mathfrak{m}}(\overline{\mathbf{Q}}_2) \cong (J/2J) \otimes_{\mathbf{T}_{\mathfrak{m}}} \rho_{\mathfrak{m}}$. We conclude that $J/2J$ is a cyclic $\mathbf{T}_{\mathfrak{m}}$-module, and hence that J is a principal ideal in $\mathbf{T}_{\mathfrak{m}}$. The discussion of [7, 3.3.2] shows that in fact $J \cong \mathbf{T}_{\mathfrak{m}}$ and that $\mathrm{Ta}_{\mathfrak{m}} J_0(2N)$ is free of rank two over $\mathbf{T}_{\mathfrak{m}}$, as claimed.

3.13 Corollary: *In the situation of Theorem 3.9, the completion $\mathbf{T}_{\mathfrak{m}}$ is a Gorenstein $\mathbf{Z}_2$-algebra.*

Proof. This follows from the theorem together with the self-duality of the $\mathfrak{m}$-adic Tate module under the Weil pairing. ∎

We now prove our level lowering result. Let A be an Artinian ring with finite residue field k of characteristic 2, and suppose given a continuous representation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(A)$ that is modular of level $\Gamma_0(2N)$ for some odd natural number N, in the sense that it arises from a Hecke eigenform $h \in S_2(\Gamma_0(2N), A)$. Let $\overline{\rho}$ denote the residual representation attached to ρ (so $\overline{\rho}$ arises from the Hecke eigenform $\overline{h} \in S_2(\Gamma_0(2N), k)$ obtained by reducing h modulo the maximal ideal of A).

3.14 Theorem: *If $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(A)$ is a modular Galois representation of level $\Gamma_0(2N)$ as above, such that*

1. *$\overline{\rho}$ is (absolutely) irreducible,*
2. *$\overline{\rho}$ is ordinary and ramified at 2, and*
3. *ρ is finite flat at 2,*

then ρ arises from an A-valued Hecke eigenform of level N.

Proof. The Hecke eigenform h corresponds to a ring homomorphism $\phi : \mathbf{T} \to A$. Since A is local of residue characteristic 2, the map ϕ factors through the completion $\mathbf{T}_{\mathfrak{m}}$ of $\mathbf{T}$ at some maximal ideal $\mathfrak{m}$ of residue characteristic 2, and the residual representation $\overline{\rho}$ is *the* residual Galois representation attached to the maximal ideal $\mathfrak{m}$. We let $\rho_{\mathfrak{m}}$ denote the Galois representation

$$\rho_{\mathfrak{m}} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{T}_{\mathfrak{m}})$$

attached to $\mathfrak{m}$ by [7, Thm. 3]. The Galois representation ρ attached to h coincides with the pushforward of $\rho_{\mathfrak{m}}$ via ϕ.

Replacing A by the image of ϕ, we may and do assume from now on that ϕ is surjective. We let $I \subset \mathbf{T}_{\mathfrak{m}}$ denote the kernel of ϕ. Since A is Artinian, we may choose $r \geq 1$ so that $2^r \in I$. Theorem 3.9 shows that the $\mathfrak{m}$-adic Tate module $\mathrm{Ta}_{\mathfrak{m}} J_0(2N)$ is isomorphic as a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-representation to $\rho_{\mathfrak{m}}$; thus $J_0(2N)[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}})$ is isomorphic to the reduction mod 2^r of $\rho_{\mathfrak{m}}$. Since $\mathbf{T}_{\mathfrak{m}}$ is a Gorenstein $\mathbf{Z}_2$-algebra, by corollary 3.13, we see that $\mathbf{T}_{\mathfrak{m}}/2^r\mathbf{T}_{\mathfrak{m}}$ is a Gorenstein $\mathbf{Z}/2^r\mathbf{Z}$-algebra, and thus that there is an isomorphism $(\mathbf{T}_{\mathfrak{m}}/2^r\mathbf{T}_{\mathfrak{m}})[I] \cong \mathrm{Hom}_{\mathbf{Z}/2^r}(\mathbf{T}_{\mathfrak{m}}/I, \mathbf{Z}/2^r)$ of $\mathbf{T}_{\mathfrak{m}}/I = A$-modules. In particular, $J_0(2N)[I](\overline{\mathbf{Q}}/\mathbf{Q}) \subset J_0(2N)[2^r]_{\mathfrak{m}}(\overline{\mathbf{Q}})$ is a faithful A-module, isomorphic as an $A[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module to $\mathrm{Hom}_{\mathbf{Z}/2^r}(\mathbf{T}_{\mathfrak{m}}/I, \mathbf{Z}/2^r) \otimes_A \rho$. To simplify notation, we will write

$$V := J_0(2N)[I](\overline{\mathbf{Q}}) \cong \mathrm{Hom}_{\mathbf{Z}/2^r}(\mathbf{T}_{\mathfrak{m}}/I, \mathbf{Z}/2^r) \otimes_A \rho. \tag{9}$$

By assumption, ρ prolongs to a finite flat group scheme $\mathcal{M}$ over $\mathrm{Spec}\,\mathbf{Z}_2$. If we fix a Jordan–Hölder filtration of ρ as an $A[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module, then the associated graded pieces are each isomorphic to $\overline{\rho}$, and so Lemma 3.10 and [5, Prop. 2.5] together imply that $\mathcal{M}$ is uniquely determined by ρ, whilst [5, Lem. 2.4] then implies that $\mathcal{M}$ is naturally an A-module scheme. From (9) we see that V also prolongs to a finite flat A-module scheme

$$\mathcal{V} \cong \mathrm{Hom}_{\mathbf{Z}/2^r}(\mathbf{T}_{\mathfrak{m}}/I, \mathbf{Z}/2^r) \otimes_A \mathcal{M}$$

over $\mathbf{Z}_2$. Again, Lemma 3.10 and [5, Prop. 2.5] show that $\mathcal{V}$ is the unique finite flat prolongation of V.

Lemma 3.10 furthermore implies that $\mathcal{M}$ is the extension of an étale A-module scheme $\mathcal{M}^{\text{ét}}$ by a multiplicative A-module scheme $\mathcal{M}^0$, each of which is free of rank one as an A-module scheme. Thus $\mathcal{V}$ is also an extension of an étale A-module scheme $\mathcal{V}^{\text{ét}}$ by multiplicative A-module scheme $\mathcal{V}^0$, each of which is faithful as an A-module scheme. Let $V^{\text{ét}}$ and V^0 denote the generic fibres of these schemes.

We write $\mathcal{J}$ to denote the Néron model of $J_0(2N)$ over $\operatorname{Spec}\mathbf{Z}_2$. For a scheme over $\mathbf{Z}_2$, use the subscript "s" to denote its special fibre over $\mathbf{F}_2$. The special fibre $\mathcal{J}_s$ admits the following filtration by $\mathbf{T}$-invariant closed subgroups:

$$0 \subset T \subset \mathcal{J}_s^0 \subset \mathcal{J}_s,$$

where T is the maximal torus contained in $\mathcal{J}_s$, and $\mathcal{J}_s^0$ is the connected component of the identity of $\mathcal{J}_s$. The quotient $\mathcal{J}_s^0/T$ is an abelian variety on which $\mathbf{T}$ acts through its quotient $\mathbf{T}_{\text{old}}$ (where $\mathbf{T}_{\text{old}}$ denotes the quotient of $\mathbf{T}$ that acts faithfully on the space of 2-old forms of level $2N$). The connected component group $\Phi := \mathcal{J}_s/\mathcal{J}_s^0$ is Eisenstein [30, Thm. 3.12].

The following lemma provides an analogue in our situation of [30, Lem. 6.2] (and generalizes one step of the argument in the proof of [13, Thm. 2.8]).

3.15 Lemma: *The Zariski closure of V in $\mathcal{J}$ is a finite flat A-module scheme over $\mathbf{Z}_2$ (which is thus isomorphic to $\mathcal{V}$).*

Proof. Since $\mathcal{V}^0$ is a multiplicative type group scheme, inertia at 2 acts on $V^0(\overline{\mathbf{Q}}_2)$ through the cyclotomic character. It follows from Lemma 3.12 that V^0 is contained in the generic fibre of $J_0(2N)[2^r]^0_{\mathfrak{m}/\mathbf{Z}_2}$, and thus that the Zariski closure of V^0 in $\mathcal{J}$ is indeed finite flat, and in fact of multiplicative type. Thus it coincides with $\mathcal{V}^0$, and so we see that the embedding of V^0 in $J_0(2N)$ prolongs to an embedding of $\mathcal{V}^0$ in $\mathcal{J}$. Since the quotient $\mathcal{V}^{\text{ét}} = \mathcal{V}/\mathcal{V}^0$ is étale, Lemma 5.9.2 of [18, Exposé IX] serves to complete the proof of the lemma. ∎

Lemma 3.15 allows us to regard $\mathcal{V}$ as a closed $\mathbf{T}$-submodule scheme of $\mathcal{J}$, and thus to regard $\mathcal{V}_s$ as a closed $\mathbf{T}$-submodule scheme of $\mathcal{J}_s$. Since $\overline{\rho}$ is irreducible and Φ is Eisenstein, we see that $\mathcal{V}_s$ is in fact contained in $\mathcal{J}_s^0$. On the other hand, since T is a torus, we see that $\mathcal{V}_s \bigcap T \subset \mathcal{V}_s^0$. Thus $\mathcal{V}_s^{\text{ét}}$ appears as a subquotient of $\mathcal{J}_s^0/T$, and in particular the $\mathbf{T}$-action on $\mathcal{V}^{\text{ét}}$ factors through the quotient $\mathbf{T}_{\mathrm{old}}$ of $\mathbf{T}$. Since $\mathcal{V}_s^{\text{ét}}$ is a faithful A-module scheme, we see that the map $\phi : \mathbf{T} \to A$ factors through $\mathbf{T}_{\mathrm{old}}$, completing the proof of the theorem. ∎

We remark that the obvious analogue of Theorem 3.14 in the case of odd residue characteristic is also true. The proof is similar but easier, relying on the uniqueness results on finite flat models due to Raynaud [27].

4. N a proper prime power

There are only finitely many elliptic curves of conductor 2^k for all k, and we may explicitly determine which have odd modular degree. Therefore we assume that E has conductor N, where $N = p^k$ with $k \geq 2$ and $p \geq 3$. Let χ be the unique quadratic character of conductor p. Let E' be the elliptic curve E twisted by χ. The curve E' also has conductor N, and moreover, the associated modular forms f_E and $f_{E'}$ are congruent modulo 2, since twisting by quadratic characters preserves $E[2]$. Since N is odd, any non-trivial congruence modulo 2 between f_E and other forms in $S_2(\Gamma_0(N))$ forces the modular degree m_E to be even [38]. Thus we are done unless $f_E = f_{E'} = f_E \otimes \chi$. It follows (for example, by [28]) that the Galois representation associated to f_E is induced from an imaginary quadratic field, and E has complex multiplication by this field. Alternatively, the equality $f_E = f_{E'}$ implies that E is isogenous to its twist, and one may deduce this way that E has CM. If E has CM and prime power conductor, then E is one of finitely many well-known elliptic curves, for which we can directly determine the modular degree by consulting current databases (for $N = 163^2$, we use the elliptic curve database of Stein–Watkins, described in [31]).

5. Further remarks

Certainly not every E satisfying the conditions of Theorem 1.1 will actually have odd modular degree, and one could try to refine this result by deducing additional necessary conditions that E must satisfy in order to have odd modular degree. In this section we say a little about the related question of whether or not 2 is a congruence prime for the associated modular form f_E, when E satisfies either of conditions (3a) or (3b) of the theorem.

For curves E with a rational two torsion point, the modular form f_E automatically satisfies a mod two congruence with an Eisenstein series, and so detecting whether f satisfies a congruence with a cuspform is a more subtle phenomenon than in the non-Eisenstein situation. One approach might be to relate the Hecke algebra to an appropriate universal deformation ring (if the latter exists). If N is prime, this can be done [5], and this enables one to determine when $\mathbf{T}_{\mathfrak{m}} = \mathbf{Z}_2$ for such representations. The specific determination of when $\mathbf{T}_{\mathfrak{m}} = \mathbf{Z}_2$, however, was already achieved (for N prime and $\overline{\rho}$ reducible) by Merel in [25]:

5.1 Theorem: *Let $N \equiv 1 \bmod 8$ be prime, and let $\mathbf{T}_{\mathfrak{m}}$ be the localization at the Eisenstein prime at 2. Then $\mathbf{T}_{\mathfrak{m}} \neq \mathbf{Z}_2$ if and only if $N = u^2 + 16v^2$ and $v \equiv (N-1)/8 \bmod 2$.*

If E is a Neumann–Setzer curve, then $N = u^2 + 64$ for some $u \in \mathbf{Z}$. The result of Merel above then clearly implies that the optimal Neumann–Setzer curve E has odd modular degree if and only if $N \not\equiv 1 \bmod 16$. (An alternative proof of this fact, relying on the results of [23], is given in [32, Thm. 2.1]). If E has composite conductor, then one might try to generalize the results of [25] or [5] to this setting.

Suppose now that E has prime conductor, that $\overline{\rho}$ is irreducible and supersingular, and that $\mathbf{Q}(E[2])$ is totally complex. If one had an $R = \mathbf{T}$ result of the type discussed in the introduction, then to obtain further necessary conditions for E to have odd modular degree, it would suffice to establish sufficient conditions for the existence of an appropriate non-trivial minimal deformation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{F}_2[x]/(x^2))$ lifting $\overline{\rho}$. For representations $\overline{\rho}$ that are complex and ramified at 2, but ordinary, we constructed such a ρ directly in subsection 3.5 by considering quadratic genus fields. When E is supersingular, such deformations ρ (when they exist) may be more subtle and cannot necessarily be constructed so directly.

References

[1] A. Agashe, *The Birch and Swinnerton-Dyer formula for modular abelian varieties of analytic rank zero*, Ph.D. Thesis, Berkeley, 2000.

[2] N. Boston, H. Lenstra and K. Ribet, *Quotients of group rings arising from two-dimensional representations*, Comptes Rendus de l'Académie des Sciences. Série I. Mathématique **312** (1991), 323–328.

[3] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild* 3*-adic exercises*, Journal of the American Mathematical Society **14** (2001), 843–939.

[4] K. Buzzard, *On level-lowering for mod 2 representations*, Mathematical Research Letters **7** (2000), 95–110.

[5] F. Calegari and M. Emerton, *On the ramification of Hecke algebras at Eisenstein primes*, Inventiones Mathematicae **160** (2005), 97–144.

[6] H. Carayol, *Sur les représentations galoisiennes mod l attachées aux formes modulaires*, Duke Mathematical Journal **59** (1989), 785–801.

[7] H. Carayol, *Formes modulaires et répresentations Galoisiennes á valeurs dans un anneau local complet*, in *p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (B. Mazur, G. Stevens, eds.)*, Contemporary Mathematics **165** (1994), 213–235.

[8] J. Cremona and M. Watkins, data available at
`http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html`

[9] E. de Shalit, *Hecke rings and universal deformation rings*, in *Modular Forms and Fermat's Last Theorem*, Springer, Boston, MA, 1995, pp. 421–445.

[10] F. Diamond, *On deformation rings and Hecke rings*, Annals of Mathematics **144** (1996), 137–166.

[11] M. Dickinson, On the modularity of certain 2-adic G*alois representations*, Duke Mathematical Journal **109** (2001), 319–382.

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

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

[14] M. Flach, *A finiteness theorem for the symmetric square of an elliptic curve*, Inventiones Mathematicae **109** (1992), 307–327.

[15] M. Flach, *On the degree of modular parametrizations*, in *Séminaire de Théorie des Nombres, Paris, 1991–92,* Progress in Mathematics, 116, Birkhäuser Boston, Boston, MA, 1993, pp. 23–36.

[16] J. Fontaine, *Il n'y a pas de variété abélienne sur* **Z**, Inventiones Mathematicae **81** (1985), 515–538.

[17] B. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Mathematical Journal **61** (1990), 445–517.

[18] A. Grothendieck, *Groups de monodromie en géométrie algébrique I, (SGA 7),* in *Séminaire de Géométrie Algébrique du Bois-Marie, 1967-1969,* Lecture Notes in Math., vol. 288, Springer, Berlin and New York, 1972, pp. 313–523.

[19] N. Katz, *p-adic properties of modular schemes and modular forms*, in *Modular Functions of One Variable, III, (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Mathematics, vol. 350, Springer, Berlin and New York, 1973, pp. 69–190.

[20] C. Khare and J. P. Wintenberger, *Serre's modularity conjecture: the odd conductor case (II)*, 2006, preprint.

[21] L. Kilford, *Some non-Gorenstein Hecke algebras attached to spaces of modular forms*, Journal of Number Theory **97** (2002), 157–164.

[22] W. Li, *Newforms and functional equations*, Mathematische Annalen **212** (1975), 285–315.

[23] B. Mazur, *Modular curves and the Eisenstein ideal*, Publications Mathématiques. Institut de Hautes Études Scientifiques **47** (1977), 33–186.

[24] B. Mazur *Rational isogenies of prime degree*, Inventiones Mathematicae **44** (1978), 129–162.

[25] L. Merel, *L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de $J_0(p)$*, Journal für die Reine und Angewandte Mathematik **477** (1996), 71–115.

[26] F. Oort and J. Tate, *Group schemes of prime order.* Annales Scientifiques de l'École Normale Supérieure. Quatrième Série **3** (1970), 1–21.

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

[28] K. Ribet, *Galois representations attached to eigenforms with Nebentypus*, in *Modular Functions of One Variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, Lecture Notes in Mathematics, vol. 601, Springer, Berlin and New York, 1977, pp. 17–51.

[29] K. Ribet, *Mod p Hecke operators and congruences between modular forms*, Inventiones Mathematicae **71** (1983), 193–205.

[30] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Inventiones Mathematicae **100** (1990), 431–476.

[31] W. Stein and M. Watkins, *A Database of Elliptic Curves—First Report*, in *Algorithmic number theory (Sydney, 2002),* Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 267–275.

[32] W. Stein and M. Watkins, *Modular parametrizations of Neumann–Setzer elliptic curves*, IMRN, (2004), 1395–1405.

[33] J. Tate, *The non-existence of certain Galois extensions of* $\mathbf{Q}$ *unramified outside* 2, in *Arithmetic Geometry (N. Childress, J. Jones, eds.)*, Contemporary Mathematics **174** (1994), 153–156.

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

[35] M. Watkins, *Computing the modular degree of an elliptic curve*, Experimental Mathematics **11** (2002), 487–502.

[36] G. Wiese, *Dihedral Galois representations and Katz modular forms*, Documenta Mathematica **9** (2004), 123–133.

[37] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Mathematics. Second Series **141** (1995), 443–551.

[38] D. Zagier, *Modular parametrizations of elliptic curves*, Canadian Mathematical Bulletin **28** (1985), 372–384.