POWERS OF 2 IN THE MODULAR DEGREE VIA 2-ADIC $R = \mathbb{T}$

PATRICK B. ALLEN

Abstract. Watkins conjectured that for an elliptic curve over the rational numbers, the 2-adic valuation of its modular degree is always greater than or equal to the rank of the elliptic curve. We prove many cases of this conjecture via a 2-adic $R = \mathbb{T}$-theorem, implementing a strategy first developed by Dummigan.

1. Introduction

In [Wat02], Watkins presented a new method for computing the modular degree of a rational elliptic curve, and using the resulting data, initiated a study of the primes dividing the modular degree. In particular, he posed the following conjecture [Wat02, Conjecture 4.1]:

Conjecture 1.1. *Let E be an elliptic curve over $\mathbb{Q}$, let N denote its conductor, r denote its rank, and m_E denote the degree of its modular parametrization $X_0(N) \to E$. Then $2^r \mid m_E$.*

For example, if m_E is odd, then the conjecture predicts that E has rank 0. Assuming $4 \nmid N$, this special case was established by Kazalicki–Kohen [KK18] building on work of Yazdani [Yaz11] and Calegari–Emerton [CE09].

Caro–Pasten [CP22] proved Conjecture 1.1 assuming E is semistable, $E[2](\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ and that either the number of primes of non-split multiplicative reduction for is odd, or there is no prime of split multiplicative reduction. An analogous situation over functions fields was studied in [Car24].

When the Galois representation on $E[2](\overline{\mathbb{Q}})$ is irreducible, Dummigan [Dum06] proved cases of Conjecture 1.1[1] assuming a certain $R = \mathbb{T}$ conjecture, Conjecture 5.3 of *loc. cit.*. Dummigan assumes that E is semistable, N is even and not divisible by 4, and that if Δ is the minimal discriminant, then $\Delta < 0$ and $\mathrm{val}_p(\Delta)$ is odd for every $p \mid N$. Under these assumptions, he relates the size of the 2-Selmer group of E to the cotangent space of an appropriate 2-adic deformation ring R at the point corresponding to the 2-adic Galois representation associated to E. Then assuming $R \cong \mathbb{T}$ and that they are finite flat local complete intersections over $\mathbb{Z}_2$, Wiles's numerical criterion equates the size of the cotangent space with the size of $\mathbb{Z}_2$ modulo the relevant congruence ideal, which can then be related to the 2-part of the modular degree. Under similar hypotheses, Dummigan–Krishnamoorthy expanded on this strategy in [DK13] to investigate powers of 2 in the degree of modular abelian varieties. In particular, they investigate a strengthening of Watkins's conjecture that also takes into account Atkin–Lehner involutions.

The goal of this paper is to unconditionally prove such a strengthened version of Watkins's conjecture for certain elliptic curves E over $\mathbb{Q}$ with $E[2](\overline{\mathbb{Q}})$ irreducible:

[1]The argument of [Dum06] actually only shows $2^{r-1} \mid m_E$. There is a small error in Lemma 5.1(2) of *loc. cit.*, a corrected version of which is a special case of [DK13, Proposition 8.2].

Theorem 1.2. *Let E be a rational elliptic curve. Let N be its conductor and let Δ be the minimal discriminant of E. Assume the following:*

(1) N is even and not divisible by 4,
(2) $E[2](\mathbb{Q}) = \{0\}$,
(3) $\mathrm{val}_p(\Delta)$ is odd for any prime p of multiplicative reduction for E.

Let $s = \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E)$ be the dimension of the 2-Selmer group of E and let n be the number of primes dividing N. Then

$$2^{s+n-1} \mid m_E. \tag{1}$$

In particular, Watkins's conjecture holds for E.

The fact that (1) implies Watkins's conjecture under our assumptions follows from the fact that the Kummer map $E(\mathbb{Q})/2E(\mathbb{Q}) \to \mathrm{Sel}_2(E)$ is injective if $E[2](\mathbb{Q}) = \{0\}$ and that N has at least one prime divisor (so $n - 1 \geq 0$). To be best of the author's knowledge, this is the first unconditional (in the sense of not relying on any conjectures) result on Watkins's conjecture in the positive rank case when $E[2](\overline{\mathbb{Q}})$ is absolutely irreducible, as well as the first result in positive rank when E is not semistable. We follow and refine Dummigan's strategy, and the main point of this article is to prove the relevant 2-adic $R = \mathbb{T}$ theorem.

1.3. **Selmer groups.** Let $V = E[2](\overline{\mathbb{Q}})$ and let

$$\overline{\rho} \colon G_{\mathbb{Q}} \to \mathrm{GL}(V) \cong \mathrm{GL}_2(\mathbb{F}_2)$$

be the $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-representation on V, where $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. As we will study the modular degree via $R = \mathbb{T}$ theorems, we assume that $\overline{\rho}$ is absolutely irreducible, equivalently that $E[2](\mathbb{Q}) = \{0\}$ and Δ is not a square. We let $\mathrm{ad}\,\overline{\rho} = \mathrm{End}_{\mathbb{F}_2}(V)$, and let $\mathfrak{z}$ and $\mathrm{ad}^0\,\overline{\rho}$ be the subspace of scalar and trace zero endomorphisms, respectively. Note that since our coefficient prime is 2, we have $\mathfrak{z} \subset \mathrm{ad}^0\,\overline{\rho}$, and the trace pairing $(X, Y) \mapsto \mathrm{tr}(XY)$ induces a duality between $\mathrm{ad}^0\,\overline{\rho}$ and $\mathrm{ad}\,\overline{\rho}/\mathfrak{z} \cong \mathrm{Sym}^2 V$.

We define a Selmer group $H^1_{\mathcal{L}}(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho})$ in §5.1 of classes that are unramified outside of N and ∞, have no condition at ∞ or primes of additive reduction, and at primes p of multiplicative reduction are represented by a cocycle that, in a basis for which $\overline{\rho}|_{G_{\mathbb{Q}_p}}$ is upper triangular, is upper triangular with diagonal entries that are unramified. The image of this Selmer group in $H^1(\mathbb{Q}, \mathrm{ad}\,\overline{\rho})$ is isomorphic to the tangent space of a natural deformation problem for $\overline{\rho}$; see §5.8. The map from this Selmer group to $H^1(\mathbb{Q}, \mathrm{ad}\,\overline{\rho})$ has one dimensional kernel, and this is the source of the -1 in the exponent of (1).

Following Dummigan, we consider the squaring map $s \colon V \to \mathrm{Sym}^2 V$ that sends $x \in V$ to the image x^2 of $x \otimes x \in V \otimes V$ in $\mathrm{Sym}^2 V$. A peculiar feature of the fact that we are working with $\mathbb{F}_2$-vector spaces is that the squaring map is linear, and we get an induced map on Galois cohomology $s_* \colon H^1(\mathbb{Q}, V) \to H^1(\mathbb{Q}, \mathrm{Sym}^2 V)$. Using a Tate parametrization, Dummigan shows that at a prime p of multiplicative reduction such that $\mathrm{val}_p(\Delta)$ is odd, the composite of the Kummer map and the squaring map has image in the dual Selmer condition $L_p^{\perp}$. For a prime p of additive reduction, and at the infinite place, we argue differently. Using the structure of $E(\mathbb{Q}_p)$, resp. $E(\mathbb{R})$, the image of the local Kummer map is easily bounded above by $\dim_{\mathbb{F}_2} H^0(G_{\mathbb{Q}_p}, V)$, resp. by $-1 + \dim_{\mathbb{F}_2} H^0(G_{\mathbb{R}}, V)$; see Lemma 5.5. The fact that

our Selmer condition is unbalanced now helps us, as this error term is accounted for in the difference

$$\dim_{\mathbb{F}_2} H^1_{\mathcal{L}}(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho}) - \dim_{\mathbb{F}_2} H^1_{\mathcal{L}^\perp}(\mathbb{Q}, \mathrm{ad}\,\overline{\rho}/\mathfrak{z});$$

see Lemma 5.6. In fact, this difference is also the source of our gain of "$+n$" in the exponent of (1). Even if we assume that there are no primes of additive reduction and that complex conjugation acts nontrivially under $\overline{\rho}$, our Selmer condition is unbalanced, unlike the situation when the coefficient prime is odd. In particular, at a prime p of multiplicative reduction, there is a non-trivial ramified class in $L_p \subset H^1(\mathbb{Q}_p, \mathrm{ad}^0\,\overline{\rho})$ that becomes a coboundary with $\mathrm{ad}\,\overline{\rho}$-coefficients; see Remark 5.3.

All of this shows that the dimension of the tangent space of our deformation ring is bounded below by the left hand side of (1). If we can then prove that our deformation ring and Hecke algebras are isomorphic and are finite flat local complete intersections over $\mathbb{Z}_2$, Wiles's numerical criterion implies that the dimension of this tangent space is bounded above by the 2-adic valuation of the congruence ideal associated to E, which can be shown equals the 2-adic valuation of the modular degree assuming $4 \nmid N$.

1.4. **The $R = \mathbb{T}$ theorem.** We have to prove our $R = \mathbb{T}$ theorem in a rather roundabout way. First, we show using a lemma of Kisin that the deformation ring R for our setup admits a good presentation, provided we assume that there is at least one prime where we allow arbitrary ramification (e.g. if there is a prime of additive reduction); see Proposition 2.8. Crucial for this is that the local lifting rings at the primes of multiplicative reduction are local complete intersections over $\mathbb{Z}_2$, which we prove assuming that $\overline{\rho}|_{G_{\mathbb{Q}_p}}$ is ramified with image of order 2, something implied by our assumption that $\mathrm{val}_p(\Delta)$ is odd (these assumptions are equivalent for p odd but for $p = 2$ the former is strictly weaker than the latter). In fact, if p is an odd prime of multiplicative reduction such that $\overline{\rho}|_{G_{\mathbb{Q}_p}}$ is trivial, then it seems likely that the appropriate deformation ring R for our setup will not be a complete intersection over $\mathbb{Z}_2$ (see [BKM24, Theorem 6.5] for such a result in the case where $\overline{\rho}$ takes values in a finite field of odd characteristic).

Using base change and the Khare–Wintenberger method together with previous results of the author [All14a], we can deduce that R is finite over $\mathbb{Z}_2$ and that all of its minimal primes come from modular forms; see Theorem 3.2. Crucial for this is that E is ordinary and that if $\Delta < 0$, then 2 does not split in $\mathbb{Q}(\sqrt{\Delta})$, assumptions implied in turn by our hypotheses that N is even and not divisible by 4 and that $\mathrm{val}_2(\Delta)$ is odd. The fact that R is finite over $\mathbb{Z}_2$, the good presentation, and a standard commutative algebra argument then shows that R is a finite flat local complete intersection over $\mathbb{Z}_2$; see Corollary 3.3. Then to show that the usual map $R \to \mathbb{T}$ is an isomorphism, it only remains to show that $R[1/2]$ is reduced, which follows from recent work of Newton–Thorne [NT23a]; see §4.6. This was all under the assumption that there is a prime at which we allow arbitrary ramification. To remove this assumption, we consider modular curves at level Nq^2 for carefully chosen prime q, use what we have just proved at level Nq^2, and then descend using Wiles's numerical criterion; see §4.11.

1.5. **Organization.** This paper is organized as follows. In §2 we set up the generalities on our deformation rings and prove the results about presentations. In §3, we

prove the result that our deformation ring is finite over $\mathbb{Z}_2$ with all minimal primes modular. In both §2 and §3 we work over general totally real fields as it requires little extra work. In §4 we specialize to $\mathbb{Q}$ and prove our $R = \mathbb{T}$-theorem. Finally, in §5.8, we define and analyze the various Selmer groups attached to our elliptic curve and deduce Theorem 1.2.

1.6. **Notation and conventions.** We let F denote a totally real field, S_2 the set of places above 2 in F, and S_∞ the archimedean places of F. We fix an algebraic closure $\overline{F}$ of F and set $G_F = \mathrm{Gal}(\overline{F}/F)$. For a place v of F, we let F_v be the completion of F at v, we fix an algebraic closure $\overline{F}_v$ of F_v, and let $G_{F_v} = \mathrm{Gal}(\overline{F}_v/F_v)$. We fix an F-linear embedding of fields $\overline{F} \hookrightarrow \overline{F}_v$ and will often identify G_{F_v} with its image under the resulting embedding of profinite groups $G_{F_v} \hookrightarrow G_F$. All algebraic extension of F (resp. of F_v) will be taken inside of $\overline{F}$ (resp. inside of $\overline{F}_v$). We let F_v^{ab}/F_v be the maximal abelian extension and let F_v^{tr}/F_v be the maximal tamely ramified extension. We denote by $\mathrm{Art}_{F_v} \colon F_v^\times \to \mathrm{Gal}(F_v^{\mathrm{ab}}/F_v)$ the Artin map normalized so that uniformizers are sent to arithmetic Frobenii.

We let $K/\mathbb{Q}_2$ be a finite extension with ring of integers $\mathcal{O}$ and residue field k. Let ϖ be a uniformizer for K. We let $\mathrm{CNL}_{\mathcal{O}}$ be the category of complete local Noetherian $\mathcal{O}$-algebras A such that the structure map $\mathcal{O} \to A$ induces an isomorphism $k \xrightarrow{\sim} A/\mathfrak{m}_A$.

Given a continuous representation

$$\overline{\rho} \colon G_F \to \mathrm{GL}_2(k),$$

we let $\mathrm{ad}\,\overline{\rho}$ denote the space of 2-by-2 matrices with coefficients in k and with adjoint G_F-action via $\overline{\rho}$, i.e. $\sigma \cdot X := \overline{\rho}(\sigma) X \overline{\rho}(\sigma)^{-1}$. We let $\mathfrak{z} \subset \mathrm{ad}\,\overline{\rho}$ denote the subspace of scalar matrices and let $\mathrm{ad}^0\,\overline{\rho} \subset \mathrm{ad}\,\overline{\rho}$ be the subspace of trace 0 matrices. Since k has characteristic 2, $\mathfrak{z} \subset \mathrm{ad}^0\,\overline{\rho}$.

Given a positive integer N, we let $Y_0(N)$ and $X_0(N)$ denote the open, resp. compact, modular curves of level $\Gamma_0(N)$, and let $J_0(N)$ denote the Jacobian of $X_0(N)$. Let $\mathbb{T}_{\mathbb{Z}}(N)$ be the $\mathbb{Z}$-subalgebra of $\mathrm{End}(J_0(N))$ generated by the Hecke operators T_p for $p \nmid N$ and U_p for $p \mid N$ under Picard functoriality. Set $\mathbb{T}(N) = \mathbb{T}_{\mathbb{Z}}(N) \otimes_{\mathbb{Z}} \mathcal{O}$. Given an integer M, we let $\mathbb{T}^M(N)$ be the subalgebra of $\mathbb{T}(N)$ generated over $\mathcal{O}$ by T_p and U_p for $p \nmid M$.

Acknowledgements. Many of the ideas for proving integral $R = \mathbb{T}$ theorems for mod p Galois representations with small residual image were developed with Preston Wake in ongoing joint work, and I would like to thank him heartily. I would like to thank Soroosh Yazdani for bringing this problem to my attention many years ago. I would also like to thank Mohammad Masih Hamidi, Chandrashekhar Khare, and Jeff Manning for helpful discussions. Parts of this work were completed while I was a guest at the École normale supérieure de Lyon and at the Université Paris–Saclay and I would like to thank both institutions for their hospitality and for providing excellent working environments. This work was supported by NSERC.

2. Deformation theory

Recall that F is a totally real field. Let S be a finite set of places of F containing $S_2 \cup S_\infty$. Let

$$\overline{\rho} \colon G_F \to \mathrm{GL}_2(k)$$

be a continuous absolutely irreducible representation and $\psi\colon G_F \to \mathcal{O}^\times$ a continuous finite order character satisfying the following.

- $\overline{\rho}$ and ψ are both unramified outside of S.
- $\det \overline{\rho} = \overline{\psi\epsilon} := \psi\epsilon \bmod \varpi$.
- For each $v \in S_2$, $\overline{\rho}|_{G_{F_v}}$ has image of order 2 and is ramified.

2.1. **Local deformation conditions.** For any place v of F, we let $D_v^\square$ be the lifting functor for $\overline{\rho}|_{G_{F_v}}$ defined on the category $\mathrm{CNL}_\mathcal{O}$, and let $R_v^\square$ denote the universal lifting ring representing it. A *local deformation condition* is a subfunctor $D_v \subseteq D_v^\square$ satisfying the following two properties:

- For any $A \in \mathrm{CNL}_\mathcal{O}$, $\rho \in D_v(A)$, and $g \in \ker(\mathrm{GL}_2(A) \to \mathrm{GL}_2(k))$, we have $g\rho g^{-1} \in D_v(A)$.
- D_v is represented by a quotient R_v of $R_v^\square$.

Any lift ρ of $\overline{\rho}|_{G_{F_v}}$ to the dual numbers $k[\epsilon] = k[\epsilon]/(\epsilon^2)$ can be written uniquely as $\rho = (1 + \epsilon\kappa)\overline{\rho}$ for a 1-cocycle $\kappa \in Z^1(G_{F_v}, \operatorname{ad}\overline{\rho})$ with coefficient in $\operatorname{ad}\overline{\rho}$. This defines an isomorphism of k-vector spaces

$$Z^1(G_{F_v}, \operatorname{ad}\overline{\rho}) \cong D_v^\square(k[\epsilon]) \cong \mathrm{Hom}_k(\mathfrak{m}_{R_v^\square}/(\varpi, \mathfrak{m}_{R_v^\square}^2), k). \tag{2}$$

Under this isomorphism, modifying a cocycle κ by the coboundary $\sigma \mapsto \sigma \cdot X - X$, $X \in \operatorname{ad}\overline{\rho}$, corresponds to conjugating $(1 + \epsilon\kappa)\overline{\rho}$ by $g = 1 + \epsilon X$.

A local deformation problem $D_v \subseteq D_v^\square$ defines a subspace $L_v^1 \subseteq Z^1(G_{F_v}, \operatorname{ad}\overline{\rho})$ via (2) and the natural inclusion $D_v(k[\epsilon]) \subseteq D_v^\square(k[\epsilon])$. This subspace L_v^1 contains the subspace $B^1(G_{F_v}, \operatorname{ad}\overline{\rho}) \subseteq Z^1(G_{F_v}, \operatorname{ad}\overline{\rho})$ of all coboundaries.

Lemma 2.2. *Let v be a finite place of F such that $\overline{\rho}|_{G_{F_v}}$ has image of order 2 and is ramified. Let $L_k \subset k^2$ be the unique line stable under $\overline{\rho}|_{G_{F_v}}$.*

Let $D_v \subseteq D_v^\square$ be the subfunctor of lifts $\rho\colon G_{F_v} \to \mathrm{GL}_2(A)$ such that $\det\rho = \psi\epsilon$ and such that there is a free rank 1 direct summand $L_A \subset A^2$ lifting L_k that is stable under ρ and such that G_{F_v} acts on A^2/L by an unramified character. Then D_v is a local deformation problem and the quotient R_v of $R_v^\square$ representing D_v has a presentation $R_v \cong \mathcal{O}[\![x_1, \dots, x_g]\!]/(f_1, \dots, f_r)$ with

$$g - r = \begin{cases} 3 + [F_v : \mathbb{Q}_2] & \text{if } v \mid 2, \\ 3 & \text{if } v \nmid 2. \end{cases}$$

Proof. We may assume that $\overline{\rho}|_{G_{F_v}} = \begin{pmatrix} 1 & \alpha \\ & 1 \end{pmatrix}$ with $\alpha\colon G_{F_v} \to k$ a ramified homomorphism of order 2. Let $D_B \subset D_v^\square$ be the be the subfunctor of upper-triangular lifts $\rho = \begin{pmatrix} \psi\epsilon\chi_v^{-1} & * \\ & \chi_v \end{pmatrix}$ with χ_v unramified. We will show below that D_B is represented by a $\mathrm{CNL}_\mathcal{O}$-algebra R_B that admits a presentation $R_B \cong \mathcal{O}[\![x_1, \dots, x_g]\!]/(f_1, \dots, f_r)$ with

$$g - r = \begin{cases} 2 + [F_v : \mathbb{Q}_2] & \text{if } v \mid 2, \\ 2 & \text{if } v \nmid 2. \end{cases}$$

Then the proof of [AKT22, Proposition 4.1] shows that D_v is representable, and that if R_v is the quotient of $R_v^\square$ representing D_v, then $R_v \cong R_B[\![z]\!]$.

First assume that $v \nmid 2$ and let q be the size of the residue field of v. Let F_v^{tr}/F_v be the maximal tamely ramified extension in $\overline{F}_v$. Any lift of $\overline{\rho}$ must factor through $\mathrm{Gal}(F_v^{\mathrm{tr}}/F_v)$. Fix a topological generator $t \in I_{F_v^{\mathrm{tr}}/F_v} \subset \mathrm{Gal}(F_v^{\mathrm{tr}}/F_v)$ of

the inertia subgroup, and choose a lift $\phi \in \mathrm{Gal}(F_v^{\mathrm{tr}}/F_v)$ of Frobenius such that $\overline{\rho}(\phi) = 1$. Using the relation $\phi t \phi^{-1} = t^q$, it is easy to see that D_B is represented by $R_B = \mathcal{O}[\![a, b, x]\!]/(\psi(\phi)(1+a)^2 - 1)$ with universal lift ρ given by

$$\rho(\phi) = \begin{pmatrix} \psi(\phi)q(1+a) & b \\ 0 & (1+a)^{-1} \end{pmatrix} \quad \rho(t) = \begin{pmatrix} 1 & 1+x \\ 0 & 1 \end{pmatrix}.$$

Now assume that $v \mid 2$. Let F_v^{ab}/F_v be the maximal abelian extension of F_v in $\overline{F}_v$ and let $I_{F_v^{\mathrm{ab}}/F_v} \subseteq \mathrm{Gal}(F_v^{\mathrm{ab}}/F_v)$ be the inertia subgroup. Let $D_B^{\mathrm{big}} \subset D_v^{\square}$ be the subfunctor of upper-triangular lifts $\rho = \begin{pmatrix} \psi\epsilon\theta^{-1} & * \\ 0 & \theta \end{pmatrix}$ such that θ_v is trivial on the torsion subgroup of $I_{F_v^{\mathrm{ab}}/F_v} \cong \mathcal{O}_{F_v}^{\times}$. Then [All14a, Proposition 1.4.8] and its proof shows that D_B^{big} is represented $R_B^{\mathrm{big}} \cong \mathcal{O}[\![x_1, \dots, x_g]\!]/(f_1)$ with $g = 3 + 2[F_v : \mathbb{Q}_p]$. Let $(\mathcal{O}_{F_v}^{\times})^f$ be the quotient of $\mathcal{O}_{F_v}^{\times}$ by its torsion subgroup, let $\Lambda = \mathcal{O}[\![(\mathcal{O}_{F_v}^{\times})^f]\!]$, and let $\mathfrak{a} \subset \Lambda$ be the kernel of the augmentation $\Lambda \to \mathcal{O}$ sending every element of $(\mathcal{O}_{F_v}^{\times})^f$ to 1. If $\rho = \begin{pmatrix} \psi\epsilon\theta^{-1} & * \\ 0 & \theta \end{pmatrix}$ is the universal R_B^{big}-valued lift, then $\theta \circ \mathrm{Art}_{F_v} \colon (\mathcal{O}_{F_v}^{\times})^f \to (R_B^{\mathrm{big}})^{\times}$ determines a local $\mathcal{O}$-algebra morphism $\Lambda \to R_B^{\mathrm{big}}$ and we have $R_B = R_B^{\mathrm{big}}/\mathfrak{a}R_B^{\mathrm{big}}$. Since Λ is isomorphic to a power series ring over $\mathcal{O}$ in $[F_v : \mathbb{Q}_p]$ variables, we have $R_B \cong \mathcal{O}[\![x_1, \dots, x_g]\!]/(f_1, \dots, f_r)$ with $g - r = 2 + [F_v : \mathbb{Q}_p]$. □

The local deformation problems of Lemma 2.2 will be the ones we wish to use for our applications to Watkins's conjecture. The modularity results of [All14a] that we rely on also use the following local deformation rings.

Lemma 2.3. *Let $v \nmid 2$ be a finite place of F such that $\overline{\rho}|_{G_{F_v}}$ is trivial and let $\gamma \colon G_{F_v} \to \mathcal{O}^{\times}$ be an unramified character that is trivial mod ϖ. Then there is a local deformation problem $D_v \subset D_v^{\square}$ represented by a quotient R_v of $R_v^{\square}$ uniquely characterized by the following property: R_v is $\mathcal{O}$-flat and for any finite extension K'/K, a continuous $\mathcal{O}$-algebra morphism $R_v^{\square} \to K'$ factors through R_v if and only if $x \circ \rho^{\square}$ is an extension of γ by $\gamma\epsilon$.*

Proof. This is a special case of [KW09c, Theorem 3.1]. □

Lemma 2.4. *Let $v \nmid 2$ be a finite place of F such that $\overline{\rho}|_{G_{F_v}}$ is trivial and let $\gamma \colon G_{F_v} \to \mathcal{O}^{\times}$ be an unramified character that is trivial mod ϖ. Let A be a $\mathrm{CNL}_{\mathcal{O}}$-algebra domain and let $\rho \in D_v^{\square}(A)$ be a lift such that*

$$\mathrm{tr}\, \rho(\sigma) = \gamma\epsilon(\sigma) + \gamma(\sigma), \quad \det \rho(\sigma) = \epsilon\gamma^2(\sigma)$$

for all $\sigma \in G_{F_v}$. Then the $\mathrm{CNL}_{\mathcal{O}}$-algebra map $R_v^{\square} \to A$ corresponding to ρ factors through the R_v of Lemma 2.3.

Proof. Without loss of generality, we may assume that the map $R_v^{\square} \to A$ is surjective, so $\mathrm{Spec}\, A \subseteq \mathrm{Spec}\, R_v^{\square}$. Twisting everything by γ^{-1}, we may assume that $\gamma = 1$. Then the image of ρ is pro-p and ρ is tamely ramified.

Let $\mathfrak{p} \in \mathrm{Spec}\, A$, let $k(\mathfrak{p})$ be its residue field, and let $x \colon A \to k(\mathfrak{p})$ be the canonical homomorphism. Then if $t, \phi \in \mathrm{Gal}(F_v^{\mathrm{tr}}/F_v)$ are a topological generator of the inertia subgroup and a lift of Frobenius, respectively, the characteristic polynomials of $x \circ \rho(t)$ and $x \circ \rho(\phi)$ are $(X-1)^2$ and $(X-q)(X-1)$, respectively. This and the relation $\phi t \phi^{-1} = t^q$ implies that $x \circ \rho(t)$ is unipotent and that $x \circ \rho$ is an extension

of the trivial character by ϵ. In particular, if $\mathfrak{p}$ is a maximal ideal of $A[1/2]$, then $k(\mathfrak{p})$ is a finite extension of K and $\mathfrak{p} \in \operatorname{Spec} R_v \subseteq \operatorname{Spec} R_v^{\square}$ by Lemma 2.3. If A is a characteristic 0 domain, then the maximal ideals of $A[1/2]$ are Zariski dense in $\operatorname{Spec} A$, so $\operatorname{Spec} A \subseteq \operatorname{Spec} R_v \subseteq \operatorname{Spec} R_v^{\square}$ and $R_v^{\square} \to A$ factors through R_v.

If A is a domain of characteristic 2, we apply the observations of the above paragraph to the generic point of $\operatorname{Spec} A$ and deduce that for all $\sigma, \tau \in G_{F_v}$, we have

$$(\rho(\sigma) - 1)(\rho(\tau) - 1) = (\epsilon(\sigma) - 1)(\rho(\tau) - 1).$$

Let $\rho^{\square} \colon G_{F_v} \to \mathrm{GL}_2(R_v^{\square})$ be the universal lift, and let J be the ideal of $R_v^{\square}$ generated by the equations

$$\operatorname{tr} \rho^{\square}(\sigma) = \epsilon(\sigma) + 1, \quad \det \rho^{\square}(\sigma) = \epsilon(\sigma)$$

as well as the matrix entries of

$$(\rho^{\square}(\sigma) - 1)(\rho^{\square}(\tau) - 1) = (\epsilon(\sigma) - 1)(\rho^{\square}(\tau) - 1)$$

as we range over all $\sigma, \tau \in G_{F_v}$. Then the surjection $R_v^{\square} \to A$ factors through $R_v^{\square}/(\varpi, J)$. Now the proof of [All14a, Proposition 1.5.4] shows that the natural surjection $R_v^{\square} \to R_v$ factors through $R_v^{\square}/J$ and induces an isomorphism $R_v^{\square}/(\varpi, J) \cong R_v/(\varpi)$. Thus, $R_v^{\square} \to A$ factors through R_v. □

The following is contained in [KW09c, Proposition 3.3], it's proof, and the remark following it.

Lemma 2.5. *Let $v \mid \infty$ and let $D_v \subseteq D_v^{\square}$ be the subfunctor of lifts ρ such that for $1 \neq c_v \in G_{F_v}$, the characteristic polynomial of $\rho(c_v)$ is $X^2 - 1$. Then D_v is a local deformation problem and the quotient R_v of $R_v^{\square}$ representing D_v has a presentation $R_v \cong \mathcal{O}[\![x_1, x_1, x_3]\!]/(f)$.*

Lemma 2.6. *Let $v \mid \infty$. For any continuous 1-cocycle $\kappa \colon G_{F_v} \to \operatorname{ad}^0 \overline{\rho}$, the lift $(1 + \epsilon\kappa)\overline{\rho}|_{G_{F_v}}$ is of the type considered in Lemma 2.5.*

Proof. Let $1 \neq c_v \in G_{F_v}$ and let $\rho = (1 + \epsilon\kappa)\overline{\rho}$. Since κ has coefficients in $\operatorname{ad}^0 \overline{\rho}$, we have $\det \rho(c_v) = \det \overline{\rho}(c_v) = 1$ and it remains to show that $\operatorname{tr} \rho(c_v) = 0$. If $\overline{\rho}(c_v) = 1$, then

$$\operatorname{tr} \rho(c_v) = \operatorname{tr}(1) + \epsilon \operatorname{tr} \kappa(c_v) = 0 + 0 = 0.$$

Now assume that $\overline{\rho}(c_v) \neq 1$. Then we can fix a basis of $\overline{\rho}|_{G_{F_v}}$ such that $\overline{\rho}(c_v) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Write $\kappa(c_v) = \begin{pmatrix} a & b \\ c & a \end{pmatrix}$. The cocycle identity imples

$$0 = \kappa(1) = \kappa(c_v^2) = \overline{\rho}(c_v)\kappa(c_v)\overline{\rho}(c_v) + \kappa(c_v) = \begin{pmatrix} 0 & b + c \\ b + c & 0 \end{pmatrix},$$

so $b = c$. Then

$$\operatorname{tr} \rho(c_v) = \operatorname{tr} \overline{\rho}(c_v) + \epsilon \operatorname{tr}(\kappa(c_v)\overline{\rho}(c_v)) = \operatorname{tr} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \epsilon \operatorname{tr} \begin{pmatrix} b & a \\ a & b \end{pmatrix} = 0. \qquad \square$$

2.7. **Global deformation problems.** Say we have a subset $T \subset S$ and for each $v \in T$, a local deformation problem D_v for $\overline{\rho}|_{G_{F_v}}$. We refer to the tuple

$$\mathcal{D} = (F, S, \mathcal{O}, \overline{\rho}, \psi, \{D_v\}_{v \in T})$$

as a *deformation datum*. Then a deformation $\rho \colon G_F \to \mathrm{GL}_2(A)$ of $\overline{\rho}$ to $A \in \mathrm{CNL}_{\mathcal{O}}$ is of *type* $\mathcal{D}$ if

- ρ is unramified outside of S,

- $\det \rho = \psi\epsilon$,
- for each $v \in T$, any (equivalently one) lift in the equivalence class of $\rho|_{G_{F_v}}$ lies in $D_v(A)$.

There is a set-valued functor $D_{\mathcal{D}}$ on $\mathrm{CNL}_{\mathcal{O}}$ that sends A to the set of deformations of $\overline{\rho}$ to A that are of type $\mathcal{D}$, and it is represented by a quotient $R_{\mathcal{D}}$ of the universal deformation ring for $\overline{\rho}$.

For each $v \in T$, let $L_v^1 \subseteq Z^1(G_{F_v}, \mathrm{ad}\,\overline{\rho})$ be the subspace of 1-cocycles corresponding to $D_v(k[\epsilon])$ (see §2.1) and let $L_v \subseteq H^1(G_{F_v}, \mathrm{ad}\,\overline{\rho})$ be its image in cohomology. Let $H^1(G_{F,S}, \mathrm{ad}^0\,\overline{\rho})'$ be the image of $H^1(G_{F,S}, \mathrm{ad}^0\,\overline{\rho})$ in $H^1(G_{F,S}, \mathrm{ad}\,\overline{\rho})$. Finally, let

$$H^1_{\mathcal{D}}(\mathrm{ad}\,\overline{\rho}) := \{\phi \in H^1(G_{F,S}, \mathrm{ad}^0\,\overline{\rho})' : \mathrm{res}_v(\phi) \in L_v \text{ for each } v \in T\}.$$

Then if $\phi \in H^1_{\mathcal{D}}(\mathrm{ad}\,\overline{\rho})$ and $\kappa\colon G_{F,S} \to \mathrm{ad}^0\,\overline{\rho}$ is a cocycle representing ϕ, the map that sends ϕ to the deformation class of the lift $(1+\epsilon\kappa)\overline{\rho}$ of $\overline{\rho}$ is well-defined and gives an isomomorphism of k-vector spaces

$$H^1_{\mathcal{D}}(\mathrm{ad}\,\overline{\rho}) \cong \mathrm{Hom}_k(\mathfrak{m}_{R_{\mathcal{D}}}/(\varpi, \mathfrak{m}_{R_{\mathcal{D}}}^2), k).$$

The following proposition will play an important role in the proofs of our main theorems.

Proposition 2.8. *Let $\overline{\rho}$ be as in the beginning of this section and let $T \subset S$ be a subset containing S_2 and S_∞ and such that for any finite $v \in T$, the restriction $\overline{\rho}|_{G_{F_v}}$ has image of order 2 and is ramified. Consider the global deformation datum*

$$\mathcal{D} = (F, S, \mathcal{O}, \overline{\rho}, \psi, \{D_v\}_{v\in T}),$$

where

- *D_v is as in Lemma 2.2 for finite $v \in T$, and*
- *D_v is as in Lemma 2.5 for $v \in S_\infty$.*

Then if $S \setminus T \neq \emptyset$, there is a presentation $R_{\mathcal{D}} \cong \mathcal{O}[\![x_1, \dots, x_g]\!]/(f_1, \dots, f_g)$.

Proof. For each $v \in T$, let R_v be the object representing D_v, and set $R^{\mathrm{loc}} = \widehat{\otimes}_{v\in T} R_v$, the completed tensor product being taken over $\mathcal{O}$. Then Lemmas 2.2 and 2.5 imply that we have a presentation

$$R^{\mathrm{loc}} \cong \mathcal{O}[\![x_1, \dots, x_a]\!]/(f_1, \dots, f_b) \quad \text{with} \quad a - b = 3|T|. \tag{3}$$

We now appeal to [Kis07, Proposition 4.1.5 and Remark 4.1.7]. Because there is a finite place in $S \setminus T$, our setup satisfies the condition (†) of *loc. cit.* We deduce there is a presentation

$$R_{\mathcal{D}} \cong R^{\mathrm{loc}}[\![y_1, \dots, y_c]\!]/(g_1, \dots, g_d) \quad \text{with} \quad c - d = -3|T|. \tag{4}$$

Equations (3) and (4) imply the proposition. □

3. Finiteness of deformation rings

We fix the following data.

(1) A totally real field F and a finite set of places S of F containing $S_2 \cup S_\infty$.
(2) A continuous irreducible representation
$$\overline{\rho}\colon G_F \to \mathrm{GL}_2(k)$$
unramified outside of S.
(3) A finite order character $\psi\colon G_F \to \mathcal{O}^\times$ unramified outside of S such that $\psi\epsilon$ lifts $\det \overline{\rho}$.

(4) A subset $T \subset S$ containing S_2 and S_∞ and such that $\overline{\rho}|_{G_{F_v}}$ has image of order 2 and is ramified for any finite $v \in T$. In particular, we assume that $\overline{\rho}|_{G_{F_v}}$ has image of order 2 and is ramified for every $v \mid 2$.
(5) For finite $v \in T$, we let D_v be the local deformation problem of Lemma 2.2, and for $v \in S_\infty$, let D_v be the local deformation problem of Lemma 2.5.

We then define the global deformation datum

$$\mathcal{D} = (F, S, \mathcal{O}, \overline{\rho}, \psi, \{D_v\}_{v \in T}),$$

we let $R_{\mathcal{D}}$ be the resulting type $\mathcal{D}$ universal deformation ring, and let

$$\rho_{\mathcal{D}} \colon G_F \to \mathrm{GL}_2(R_{\mathcal{D}})$$

be be the univeral deformation.

We say a cuspidal automorphic representation π of $\mathrm{GL}_2(\mathbb{A}_F)$ is *regular algebraic of weight 0* if for each $v \mid \infty$, π_v has the same infiniessimal character as the trivial algebraic representation of GL_{2/F_v}. If $F = \mathbb{Q}$, then π is regular algebraic of weight 0 if and only if it is the cuspidal automorphic representation generated by a weight $k = 2$ cuspidal newform f for some congruence subgroup (our normalization is such that a weight $k \geq 1$ cuspidal newform generates an automorphic representation with central character $|\cdot|^{2-k}$ at infinity).

Let $\iota \colon \overline{\mathbb{Q}}_2 \cong \mathbb{C}$ be an isomorphism and let π be a regular algebraic weight 0 cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$. Let $v \mid 2$ and let ϖ_v be a choice of uniformizer for F_v. For $n \geq 0$, let

$$U_1(v^n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : c, a-1, d-1 \in (\varpi_v^n) \right\},$$

and let $(\iota^{-1}\pi_v)^{n,\mathrm{ord}}$ be the maximal subspace of $\iota^{-1}\pi_v := \pi_v \otimes_{\mathbb{C},\iota^{-1}} \overline{\mathbb{Q}}_2$ on which the double coset operator $\mathsf{U}_v = [U_1(v^n) \begin{pmatrix} \varpi_v & 0 \\ 0 & 1 \end{pmatrix} U_1(v^n)]$ acts by a 2-adic unit. We then set $(\iota^{-1}\pi_v)^{\mathrm{ord}} = \varinjlim_n (\iota^{-1}\pi_v)^{n,\mathrm{ord}}$. This space has dimension at most 1 by [Hid89, Corollary 2.2], and we say that π is *ι-ordinary* if $(\iota^{-1}\pi_v)^{\mathrm{ord}} \neq 0$ for each $v \mid 2$. If $F = \mathbb{Q}$ and π is generated by a weight 2 newform f, then π is ι-ordinary if and only if f is ordinary in the classical sense: $\iota^{-1}(a_p)$ is a p-adic unit, where a_p is the T_p or U_p-eigenvalue of f if the level of f is prime to p or divisible by p, respectively.

Lemma 3.1. *Let $\mathfrak{q}$ be a prime ideal of $R_{\mathcal{D}}$. Set $A = R_{\mathcal{D}}/\mathfrak{q}$ and let $\rho \colon G_F \to \mathrm{GL}_2(A)$ be the pushforward of $\rho_{\mathcal{D}}$ by $R \to A$. Then there is a finite solvable totally real extension L/F, a finite set of places S_L of L containing all those above 2 and ∞, and a deformation datum*

$$\mathcal{D}_L = (L, S_L, \mathcal{O}, \overline{\rho}|_{G_L}, \psi|_{G_L}, \{D_w\}_{w \in S_L})$$

satisfying the following.

(1) L/F is disjoint from $\overline{F}^{\ker(\overline{\rho})}/F$.
(2) For each $w \mid 2$ in L, $[L_w : \mathbb{Q}_2] \geq 4$ and $\overline{\rho}|_{G_{L_w}}$ has image of order 2 and is ramified.
(3) The local deformation problems are as follows.
- *D_w is as in Lemma 2.2 for $w \mid 2$,*
- *D_w is as in Lemma 2.5 for $w \mid \infty$.*
- *D_w is as in Lemma 2.3 for $w \in S_L$ not above 2 or ∞.*

(4) *The deformation* $\rho|_{G_L}$ *of* $\overline{\rho}|_{G_L}$ *is of type* $\mathcal{D}_L$ *and defines a finite* $\mathrm{CNL}_{\mathcal{O}}$*-algebra map* $R_{\mathcal{D}_L} \to A$.

Proof. First, we choose finite extensions F'_v/F_v for each $v \in S$. If $v \mid 2$, the we let F'_v/F_v be any unramified extension such that $[F'_v : \mathbb{Q}_2] \geq 4$. Note that $\overline{\rho}|_{G_{F'_v}}$ still satisfies the assumptions of Lemma 2.2 and the lift $\rho|_{G_{F'_v}}$ of $\overline{\rho}|_{G_{F'_v}}$ is of the type defined there. If $v \mid \infty$, we take $F'_v = F_v$. Set $\Sigma = S \setminus (S_2 \cup S_\infty)$, and let $\Sigma_{\mathrm{ur}} \subseteq \Sigma$, resp. $\Sigma_{\mathrm{ram}} \subset \Sigma$, denote the subset of $v \in \Sigma$ such that $\rho|_{G_{F_v}}$ is, resp. is not, potentially unramified. For $v \in \Sigma_{\mathrm{ur}}$, let F'_v/F_v be any finite extension such that $\rho|_{G_{F'_v}}$ is unramified.

Finally, if Σ_{ram}, we let F'_v/F_v be a finite extension such that $\rho|_{G_{F'_v}}$ and factors through $\mathrm{Gal}(F_v^{\mathrm{tr}}/F_v)$, with F_v^{tr}/F_v the maximal tamely ramified extension in $\overline{F}_v$, and such that $\overline{\rho}|_{G_{F'_v}}$ and $\psi|_{G_{F'_v}}$ are trivial. Let $t, \phi \in \mathrm{Gal}(F_v^{\mathrm{tr}}/F_v)$ be a topological generator of the inertia subgroup and lift of the Frobenius, respectively. Let q be the cardinality of the residue field of F'_v. The relation $\phi t \phi^{-1} = t^q$ implies that the eigenvalues of $\rho(t)$ in an algebraic closure of $\mathrm{Frac}(A)$ are stable under qth powers, hence are roots of unity. Replacing F'_v by a further finite extension, we can assume that all these eigenvalues are 1. But $\rho(t) \neq 1$ since $v \in \Sigma_{\mathrm{ram}}$. So we can find $g \in \mathrm{GL}_2(\mathrm{Frac}(A))$ such that $g\rho(t)g^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. The the relation $\phi t \phi^{-1} = t^q$ implies that $g\rho(\phi)g^{-1} = \begin{pmatrix} q\alpha & * \\ 0 & \alpha \end{pmatrix}$ with $\alpha = \pm 1$. Letting $\gamma \colon G_{F'_v} \to \mathcal{O}^\times$ be the unramified character sending $\mathrm{Frob}_{F'_v}$ to α, we see that

$$\mathrm{tr}\, \rho(\sigma) = \epsilon\gamma(\sigma) + \gamma(\sigma), \quad \det \rho(\sigma) = \epsilon\gamma^2(\sigma)$$

for all $\sigma \in G_{F'_v}$. Then Lemma 2.4 implies that the lift $\rho|_{G_{F'_v}}$ of $\overline{\rho}|_{G_{F'_v}}$ is of the type considered in Lemma 2.3.

Now choose a finite set of finite primes S' of F, disjoint from S, such that $\{\overline{\rho}(\mathrm{Frob}_u) : u \in S'\}$ exhaust all conjugacy classes in $\mathrm{im}(\overline{\rho})$. For $u \in S'$, set $F'_u = F_u$. Then we we choose a finite solvable Galois extension L/F such that if w is a place of L above $v \in S \cup S'$, then $L_w \cong F'_v$ for our fixed choices F'_v (see [Tay, Lemma 2.2], for example). Since L/F is split at any $u \in S'$, this extension is disjoint from $\overline{F}^{\ker(\overline{\rho})}/F$. Let S_L be the set of places of L above $S_2 \cup S_\infty \cup \Sigma_{\mathrm{ram}}$. We have shown that the deformation $\rho|_{G_L}$ of $\overline{\rho}|_{G_L}$ is of type $\mathcal{D}_L$, so we get a $\mathrm{CNL}_{\mathcal{O}}$-algebra map $R_{\mathcal{D}_L} \to A$. Let $\mathfrak{m}_L \subseteq R_{\mathcal{D}_\mathcal{L}}$ be the maximal ideal. The representation $\rho \bmod \mathfrak{m}_L A \colon G_F \to \mathrm{GL}_2(A/\mathfrak{m}_L A)$ factors through $\mathrm{Gal}(L\overline{F}^{\ker(\overline{\rho})}/F)$, so $R_{\mathcal{D}_L} \to A$ is finite by [KW09a, Lemma 3.6] and Nakayama's lemma. □

Theorem 3.2. *Fix an isomorphism* $\iota \colon \overline{\mathbb{Q}}_2 \cong \mathbb{C}$ *and assume that* $\overline{\rho} \cong \overline{\rho}_{\pi,\iota}$ *for an* ι*-ordinary regular algebraic weight 0 cuspidal automorphic representation* π *of* $\mathrm{GL}_2(\mathbb{A}_F)$. *Then*

(1) $R_{\mathcal{D}}$ *is a finite* $\mathcal{O}$*-algebra.*
(2) *For any continuous* $\mathcal{O}$*-algebra homomorphism* $x \colon R_{\mathcal{D}} \to \overline{\mathbb{Q}}_2$, *there is an* ι*-ordinary regular algebraic weight 0 cuspidal automorphic representation* π *of* $\mathrm{GL}_2(\mathbb{A}_F)$ *such that* $x \circ \rho_{\mathcal{D}} \cong \rho_{\pi,\iota}$.

Proof. Part 2 follows from [All14a, Theorem 5.2.1]. Since $R_{\mathcal{D}}$ is Noetherian, letting $\mathrm{Min}(R_{\mathcal{D}})$ be the (finite) set of minimal primes of $R_{\mathcal{D}}$, the map $R_{\mathcal{D}} \to$

$\prod_{\mathfrak{q}\in\mathrm{Min}(R_{\mathcal{D}})} R_{\mathcal{D}}/\mathfrak{q}$ has finite kernel and it suffices to prove part 1 with $R_{\mathcal{D}}$ replaced by $A := R_{\mathcal{D}}/\mathfrak{q}$ for some fixed $\mathfrak{q} \in \mathrm{Min}(R_{\mathcal{D}})$. Let $\rho\colon G_F \to \mathrm{GL}_2(A)$ be the pushforward of $\rho_{\mathcal{D}}$ by $R_{\mathcal{D}} \to A$. We now apply Lemma 3.1, and letting L, S_L, and $\mathcal{D}_L$ be as in the lemma, it suffices to prove that $R_{\mathcal{D}_L}$ is finite over $\mathcal{O}$.

For each $w \mid 2$ in L, let $\mathcal{O}_{L_w}^\times(2)^f$, resp. $L_w^\times(2)^f$, be the quotient of the pro-2 completion of $\mathcal{O}_{L_w}^\times$, resp. of $L_w^\times$, by its torsion subgroup. Set $\Lambda = \mathcal{O}[\![\prod_{w|2} \mathcal{O}_{L_w}^\times(2)^f]\!]$ and $\widetilde{\Lambda} = \mathcal{O}[\![\prod_{w|2} \mathcal{O}_{L_w}^\times(2)^f]\!]$. For $w \mid 2$, since the local deformation problem D_w is as in Lemma 2.2, there is a free rank 1 direct summand $L \subset R^2_{\mathcal{D}_L}$ of the representation space for $\rho_{\mathcal{D}_L}|_{G_{L_w}}$ such that G_{L_w} acts on $R^2_{\mathcal{D}_L}/L$ by an unramified character χ_w. Then the tuple $(\chi_w \circ \mathrm{Art}_{L_w})_{w|2}$ defines a $\mathrm{CNL}_{\mathcal{O}}$-algebra map $\widetilde{\Lambda} \to R_{\mathcal{D}_L}$ such that its restriction to Λ factors through the natural augmentation $\Lambda \to \mathcal{O}$. It thus suffices to prove that $R_{\mathcal{D}_L}$ is finite over Λ. But $R_{\mathcal{D}_L}$ is a quotient of the $\widetilde{\Lambda}$-algebra $\overline{R}^{\psi|_{G_L}}_{L,S_L}$ of [All14a, §4.1] (where it is denoted $\overline{R}^{\psi}_{F,S}$) and [All14b, Proposition 4.4.3] implies that $(\overline{R}^{\psi|_{G_L}}_{L,S_L})^{\mathrm{red}}$ is isomorphic to an ordinary Hecke algebra (denoted $\mathbf{T}_\psi(U,1)_{\mathfrak{m}}$ there), which is finite over Λ. Thus $\overline{R}^{\psi|_{G_L}}_{L,S_L}$ is finite over Λ, and hence so is $R_{\mathcal{D}_L}$. □

Corollary 3.3. *Let the assumptions be as above and assume further that $S \setminus T \neq \emptyset$. Then $R_{\mathcal{D}}$ is a finite flat local complete intersection over $\mathcal{O}$*

Proof. The assumption that $\overline{\rho}$ is automorphic in Theorem 3.2 implies that $\dim R_{\mathcal{D}} \geq 1$, and part 1 of the conclusion gives that $R_{\mathcal{D}}/(\varpi)$ is a finite ring. But since $S \setminus T \neq \emptyset$, we can apply Proposition 2.8, and we have a presentation $R_{\mathcal{D}} \cong \mathcal{O}[\![x_1,\dots,x_g]\!]/(f_1,\dots,f_g)$ for some $g \geq 0$. We then see that $f_1,\dots,f_g,\varpi$ is a regular sequence and the corollary follows from a standard argument. □

4. An $R = \mathbb{T}$-theorem

We now specialize to the case $F = \mathbb{Q}$ and fix

$$\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(k)$$

a continuous representation. Let $N(\overline{\rho})$ be the prime-to-2 Artin conductor of $\overline{\rho}$. We make the following assumptions:

(1) $\overline{\rho}$ is absolutely irreducible,
(2) $\det \overline{\rho} = \overline{\epsilon}$,
(3) $\overline{\rho}|_{G_{\mathbb{Q}_2}}$ has image of order 2 and is très ramifiée.

We fix a finite set of places S of $\mathbb{Q}$ containing 2 and ∞ and all primes at which $\overline{\rho}$ is ramified. We fix a subset $T \subseteq S$ satisfying $\{2,\infty\} \subseteq T \subseteq \{2,\infty\} \cup \{p \parallel N(\overline{\rho})\}$. For a prime p, we let n_p be the p-adic valuation of $N(\overline{\rho})$. Define

$$N = \prod_{\infty\neq p\in T} p \times \prod_{p\in S\setminus T} p^{\max(2,n_p)}.$$

A theorem of Tate implies that $N(\overline{\rho}) > 1$, so $N \geq 2N(\overline{\rho}) \geq 4$. We recall that $\mathbb{T}(N) = \mathbb{T}_{\mathbb{Z}}(N) \otimes_{\mathbb{Z}} \mathcal{O}$ where $\mathbb{T}_{\mathbb{Z}}(N)$ is the $\mathbb{Z}$-subalgebra of $\mathrm{End}(J_0(N))$ generated by the Hecke operators T_p for $p \nmid N$ and U_p for $p \mid N$ under Picard functoriality.

We define the global deformation problem

$$\mathcal{D} = (\mathbb{Q}, S, \mathcal{O}, \overline{\rho}, \epsilon, \{D_p\}_{p\in T}),$$

where

- for $\infty \neq p \in T$, D_p is the local deformation problem of Lemma 2.2,
- D_∞ is the local deformation problem in Lemma 2.5.

Let $R_{\mathcal{D}}$ be the resulting type $\mathcal{D}$ universal deformation ring and let $\rho_{\mathcal{D}}$ denote a representative for the universal deformation.

Theorem 4.1. *Enlarging $\mathcal{O}$ if necessary, there is an augmentation $\lambda\colon \mathbb{T}(N) \to \mathcal{O}$ such that the maximal ideal $\mathfrak{m} = (\varpi, \ker \lambda)$ is defined by*

- *$T_p \bmod \mathfrak{m} = \operatorname{tr} \overline{\rho}(\mathrm{Frob}_p)$ for any $p \nmid N$,*
- *$U_p - 1 \in \mathfrak{m}$ for $p \in T$,*
- *$U_p \in \mathfrak{m}$ for $p \in S \setminus T$.*

Proof. First, $\overline{\rho}$ is modular by [KW09b, Theorem 9.1] and [Kis09, Theorem 0.1]. Then [Buz00a, Proposition 2.4 and Theorem 3.1] implies that $\overline{\rho}$ arrises from a weight 2 normalized eigenform of level $2N(\overline{\rho})$. Then by [CDT99, Lemma 4.4], enlarging $\mathcal{O}$ if necessary, there is a normalized eigenform

$$g = q + \sum_{n \geq 2} a_n(g) q^n \in S_2(\Gamma_0(N), \mathcal{O})$$

such that

- $a_p(g) \equiv \operatorname{tr} \overline{\rho}(\mathrm{Frob}_p) \pmod{\varpi}$ for any $p \nmid N$,
- $a_p(g) \equiv 1 \pmod{\varpi}$ for $p \in T$,
- $a_p(g) \equiv 0 \pmod{\varpi}$ for $p \in S \setminus T$.

The augmentation $\lambda\colon \mathbb{T}(N) \to \mathcal{O}$ given by $T_p \mapsto a_p(g)$ for $p \nmid N$ and $U_p \mapsto a_p(g)$ for $p \mid N$ then satisfies the properties of the theorem. □

Proposition 4.2. *Let $\mathfrak{m}$ be as in Theorem 4.1. There is a surjective local $\mathcal{O}$-algebra homomorphism $\phi_{\mathcal{D}}\colon R_{\mathcal{D}} \to \mathbb{T}(N)_{\mathfrak{m}}$ satisfying the property that for $p \nmid N$,*

$$\phi_{\mathcal{D}}(\operatorname{tr} \rho_{\mathcal{D}}(\mathrm{Frob}_p)) = T_p.$$

Moreover, for any multiple M of N, $\mathbb{T}(N)_{\mathfrak{m}}$ is generated over $\mathcal{O}$ by $\{T_p : p \nmid M\}$.

Proof. This is standard. See for example, [DDT97, Lemma 3.27 and Proposition 4.7]. □

Our goal is to prove the following theorem.

Theorem 4.3. *The map $\phi_{\mathcal{D}}$ of Proposition 4.2 is an isomorphism of flat local complete intersections over $\mathcal{O}$.*

Wiles's numerical criterion [DDT97, Theorem 5.3] then yields the following corollary.

Corollary 4.4. *Let $\lambda\colon \mathbb{T}(N)_{\mathfrak{m}} \to \mathcal{O}$ be an augmentation. Let $I = \operatorname{Ann}_{\mathbb{T}(N)_{\mathfrak{m}}}(\ker(\lambda))$, $\eta = \lambda(I)$, and $\mathfrak{p} = \ker(\lambda \circ \phi_{\mathcal{D}})$. Then $\operatorname{length}_{\mathcal{O}} \mathfrak{p}/\mathfrak{p}^2 = \operatorname{length}_{\mathcal{O}} \mathcal{O}/\eta$.*

Corollary 4.5. $\dim_k \mathfrak{m}_{R_{\mathcal{D}}}/(\varpi, \mathfrak{m}_{R_{\mathcal{D}}}^2) \leq \operatorname{length}_{\mathcal{O}} \mathcal{O}/\eta$.

Proof. This follows from Corollary 4.4 since

$$\mathfrak{m}_{R_{\mathcal{D}}}/(\varpi, \mathfrak{m}_{R_{\mathcal{D}}}^2) \cong (\mathfrak{p}, \varpi)/(\varpi, \mathfrak{p}^2)$$

is a quotient of $\mathfrak{p}/\mathfrak{p}^2$. □

We divide the proof of Theorem 4.3 into two cases: $T \neq S$ and $T = S$.

4.6. **Proof of Theorem 4.3 when $T \neq S$.** Part 2 of Theorem 3.2 and local-global compatibility imply that ϕ induces a bijection $\operatorname{Spec} R_{\mathcal{D}}(\overline{\mathbb{Q}}_2) \cong \operatorname{Spec} \mathbb{T}_{\mathfrak{m}}(\overline{\mathbb{Q}}_2)$. Using Corollary 3.3, it then only remains to show that $R_{\mathcal{D}}[1/2]$ is reduced.

Since $R_{\mathcal{D}}$ is finite over $\mathcal{O}$, $R_{\mathcal{D}}[1/2]$ is reduced if and only if the localization and completion $(R_{\mathcal{D}})^{\wedge}_{\mathfrak{p}}$ is reduced for every minimal prime $\mathfrak{p}$ of $R_{\mathcal{D}}$. Fix one such $\mathfrak{p}$, let $k(\mathfrak{p})$ denote its residue field (a finite extension of K), and let $\rho_{\mathfrak{p}} \colon G_F \to \mathrm{GL}_2(k(\mathfrak{p}))$ be the pushforward of the universal $R_{\mathcal{D}}$-valued deformation via the map $R_{\mathcal{D}} \to k(\mathfrak{p})$. Choosing an embedding $k(\mathfrak{p}) \hookrightarrow \overline{\mathbb{Q}}_2$ and an isomorphism $\iota \colon \overline{\mathbb{Q}}_2 \cong \mathbb{C}$, we have $\rho_{\mathfrak{p}} \cong \rho_{f,\iota}$ for a weight 2 cuspidal eigenform f of level $\Gamma_0(N)$. By the argument of [All16, Proposition 1.3.12] (see also [NT23b, Proposition 2.17]), and using [All16, Lemma 1.1.3 and Remark 1.2.9], the tangent space of $(R_{\mathcal{D}})^{\wedge}_{\mathfrak{p}}$ is isomorphic to a subspace of the Bloch–Kato Selmer group $H^1_f(F, \mathrm{ad}^0 \rho_{\mathfrak{p}})$, which is trivial by [NT23b, Theorem B]. □

4.7. **Auxiliary primes.** Our strategy to prove Theorem 4.3 in the case $T = S$ is to first choose a certain auxiliary prime q, apply the $T \neq S$ case at level Nq^2, and then use Wiles's numerical criterion to deduce the theorem at level N.

Lemma 4.8. *There are infinitely many primes $q \nmid N$ such that $q \equiv 3 \pmod 4$ and $\overline{\rho}(\mathrm{Frob}_q)$ is regular semisimple.*

Proof. Our assumption that $\overline{\rho}|_{G_{\mathbb{Q}_2}}$ has image of order 2 and is très ramifiée implies that $\overline{\rho}$ is not an induction from $\mathbb{Q}(i)$. We can then apply [Buz00b, Lemma 2.5] and Chebotarev density. □

We fix one such prime q as in Lemma 4.8 and define the augmented deformation problem

$$\mathcal{D}' = (\mathbb{Q}, S \cup \{q\}, \mathcal{O}, \overline{\rho}, \epsilon, \{D_v\}_{v \in T}).$$

For $i = 0, 1, 2$, let $\beta_{q^i} \colon X_0(Nq^2) \to X_0(N)$ be the map induced by the map on the upper half plane $z \mapsto q^i z$. Then we obtain a map $J_0(N) \to J_0(Nq^2)$ given by $x \mapsto q\beta_1^*(x) - \beta_q^*(T_q x) + \beta_{q^2}^*(x)$. This induces a $\mathcal{O}$-algebra homomorphism $g \colon \mathbb{T}(Nq^2) \to \mathbb{T}(N)$ sending T_p to T_p and U_p to U_p for $p \neq q$ and sending U_q to 0. Letting $\mathfrak{m}' = g^{-1}(\mathfrak{m})$ and applying Proposition 4.2 at levels N and Nq^2, we obtain a commutative diagram

$$\begin{array}{ccc} R_{\mathcal{D}'} & \xrightarrow{\phi_{\mathcal{D}'}} & \mathbb{T}(Nq^2)_{\mathfrak{m}'} \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} \\ R_{\mathcal{D}} & \xrightarrow{\phi_{\mathcal{D}}} & \mathbb{T}(N)_{\mathfrak{m}}, \end{array}$$

with all arrows surjective. Enlarging $\mathcal{O}$ if necessary, we let $\lambda \colon \mathbb{T}_{\mathfrak{m}} \to \mathcal{O}$ be an augmentation as in Theorem 4.1 and set $\lambda' = \lambda \circ g$. We then define

$$I = \mathrm{Ann}_{\mathbb{T}(N)_{\mathfrak{m}}}(\ker(\lambda)) \quad \text{and} \quad I' = \mathrm{Ann}_{\mathbb{T}(Nq^2)_{\mathfrak{m}'}}(\ker(\lambda'))$$
$$\eta = \lambda(I) \quad \text{and} \quad \eta' = \lambda'(I')$$
$$\mathfrak{p} = \ker(\lambda \circ \phi_{\mathcal{D}}) \quad \text{and} \quad \mathfrak{p}' = \ker(\lambda' \circ \phi_{\mathcal{D}'}).$$

The surjection $\mathbb{T}(Nq^2)_{\mathfrak{m}'} \to \mathbb{T}(N)_{\mathfrak{m}}$ induces a map $I' \to I$, hence an inclusion $\eta' \subseteq \eta$.

Lemma 4.9. $\eta' = 2\eta$.

Proof. Set $\mu_q = (q-1)(T_q^2 - (1+q)^2)$. Wiles's proof that $\eta' = \lambda(\mu_q)\eta$ [Wil95, Proposition 2.6] as outlined in [DDT97, §4.4] (in particular, p.g. 130–137 of *loc. cit.*) carries over in our situation, i.e. when $\mathrm{char}(k) = 2$, upon updating references in two places:

(1) The multiplicity one result [DDT97, Theorem 4.26] is proved for residual characteristic 2 in [Buz00b, Proposition 2.4] under assumptions satisfied by our $\overline{\rho}$ (it is here we use the assumption that $\overline{\rho}|_{G_{\mathbb{Q}_2}}$ is très ramifiée).
(2) Wiles's exact sequence [DDT97, Lemma 4.28(b)] assumes the coefficient prime ℓ is odd. Inspecting the proof in [Wil95, Lemma 2.5], this is only used to check that $H^2(\mathrm{SL}_2(\mathbb{F}_q), \mathbb{F}_\ell) = 0$ by restricting to a Sylow ℓ-subgroup, which is cyclic. For q odd, the Sylow 2-subgroup of $\mathrm{SL}_2(\mathbb{F}_q)$ is no longer cyclic, but we still have $H^2(\mathrm{SL}_2(\mathbb{F}_q), \mathbb{F}_2) = 0$ by [FP78, Chapter IV, §5], so the proof in [Wil95, Lemma 2.5] carries over upon inserting this reference.

(See also [Dic01, §10].) Now since $q \equiv 3 \pmod 4$ and $\overline{\rho}(\mathrm{Frob}_q)$ has distinct eigenvalues, $\lambda(\mu_q) = 2u$ for some $u \in \mathcal{O}^\times$. □

Lemma 4.10. *The $\mathcal{O}$-module map $\mathfrak{p}'/\mathfrak{p}'^2 \to \mathfrak{p}/\mathfrak{p}^2$ induced by f is surjective with kernel isomorphic to $\mathcal{O}/2\mathcal{O}$.*

Proof. The fact that the map is surjective follows from the fact that f is surjective.

Let $\rho\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$ be the type $\mathcal{D}$ deformation of $\overline{\rho}$ classified by the $\mathrm{CNL}_{\mathcal{O}}$-morphism $\lambda \circ \phi_{\mathcal{D}}\colon R_{\mathcal{D}} \to \mathcal{O}$. Let $\mathrm{ad}\,\rho$ be the module of 2×2 matrices over $\mathcal{O}$ with adjoint $G_{\mathbb{Q}}$-action, let $\mathfrak{z} \subset \mathrm{ad}\,\rho$ be the submodule of scalar matrices, and let $\mathrm{ad}^0\,\rho \subset \mathrm{ad}\,\rho$ be the trace zero subspace. For any $n \geq 1$, let $\mathrm{ad}\,\rho_{\mathcal{O}/\varpi^n}$ be the mod ϖ^n reduction of $\mathrm{ad}\,\rho$ and let $\mathrm{ad}^0\,\rho_{\mathcal{O}/\varpi^n}$ be the trace zero subspace of $\mathrm{ad}\,\rho_{\mathcal{O}/\varpi^n}$. Note that $\mathrm{ad}^0\,\rho_{\mathcal{O}/\varpi^n}$ is not the ϖ^n reduction of $\mathrm{ad}^0\,\rho$ (this will be important for us). We let

$$H^1_{\mathcal{D}}(\mathrm{ad}^0\,\rho_{\mathcal{O}/\varpi^n}) \subseteq H^1_{\mathcal{D}'}(\mathrm{ad}^0\,\rho_{\mathcal{O}/\varpi^n}) \subseteq H^1(\mathbb{Q}, \mathrm{ad}^0\,\rho_{\mathcal{O}/\varpi^n})$$

be the subspace of classes ψ such that for any cocycle κ representing ψ, the $\mathcal{O} \oplus \epsilon\mathcal{O}/\varpi^n$-valued lift $(1+\epsilon\kappa)\rho$ of $\overline{\rho}$ is of type $\mathcal{D}$ and type $\mathcal{D}'$, respectively. Multiplication by ϖ on $\mathrm{ad}\,\rho$ induces isomorphisms $\varpi\,\mathrm{ad}^0\,\rho_{\mathcal{O}/\varpi^{n+1}} \cong \mathrm{ad}^0\,\rho_{\mathcal{O}/\varpi^n}$, yielding a directed system, and we then define

$$H^1_{\mathcal{D}}(\mathrm{ad}^0\,\rho_{K/\mathcal{O}}) = \varinjlim H^1_{\mathcal{D}}(\mathrm{ad}^0\,\rho_{\mathcal{O}/\varpi^n}),$$
$$H^1_{\mathcal{D}'}(\mathrm{ad}^0\,\rho_{K/\mathcal{O}}) = \varinjlim H^1_{\mathcal{D}'}(\mathrm{ad}^0\,\rho_{\mathcal{O}/\varpi^n}).$$

Define also $H^1(\mathbb{Q}, \mathrm{ad}\,\rho_{K/\mathcal{O}}) = \varinjlim H^1(\mathbb{Q}, \mathrm{ad}\,\rho_{\mathcal{O}/\varpi^n})$ and

$$H^1_{\mathcal{D}}(\mathrm{ad}\,\rho_{K/\mathcal{O}}) = \mathrm{im}(d_{\mathcal{D}}\colon H^1_{\mathcal{D}}(\mathrm{ad}^0\,\rho_{K/\mathcal{O}}) \to H^1(\mathbb{Q}, \mathrm{ad}\,\rho_{K/\mathcal{O}})),$$
$$H^1_{\mathcal{D}'}(\mathrm{ad}\,\rho_{K/\mathcal{O}}) = \mathrm{im}(d_{\mathcal{D}'}\colon H^1_{\mathcal{D}'}(\mathrm{ad}^0\,\rho_{K/\mathcal{O}}) \to H^1(\mathbb{Q}, \mathrm{ad}\,\rho_{K/\mathcal{O}})).$$

The kernels of $d_{\mathcal{D}}$ and $d_{\mathcal{D}'}$ are contained in the images of the coboundary map

$$\delta\colon K/\mathcal{O} \to H^1(\mathbb{Q}, \mathrm{ad}^0\,\rho_{K/\mathcal{O}}).$$

Since ρ is unramified at q, the image of δ consists of classes unramified at q, and $\ker d_{\mathcal{D}} = \ker d_{\mathcal{D}'}$. We deduce that the inclusion $i\colon H^1_{\mathcal{D}}(\mathrm{ad}^0\,\rho_{K/\mathcal{O}}) \subseteq H^1_{\mathcal{D}'}(\mathrm{ad}^0\,\rho_{K/\mathcal{O}})$ induces an inclusion $j\colon H_{\mathcal{D}}(\mathrm{ad}\,\rho_{K/\mathcal{O}}) \subseteq H_{\mathcal{D}'}(\mathrm{ad}\,\rho_{K/\mathcal{O}})$ such that $\mathrm{coker}(i) \cong \mathrm{coker}(j)$.

Letting $M \mapsto M^\vee := \mathrm{Hom}_{\mathcal{O}}(M, K/\mathcal{O})$ denote Pontryagin duality on the category of finitely generated $\mathcal{O}$-modules, we have isomorphisms

$$(\mathfrak{p}/\mathfrak{p}^2)^\vee \cong H^1_{\mathcal{D}}(\mathrm{ad}\,\rho_{K/\mathcal{O}}) \quad \text{and} \quad (\mathfrak{p}'/\mathfrak{p}'^2)^\vee \cong H^1_{\mathcal{D}'}(\mathrm{ad}\,\rho_{K/\mathcal{O}})$$

such that the Pontryagin dual of surjection $\mathfrak{p}'/\mathfrak{p}'^2 \to \mathfrak{p}/\mathfrak{p}^2$ induced by f is the inclusion j above. We then wish to show $\mathrm{coker}(j) \cong \mathrm{coker}(i) \cong \mathcal{O}/2\mathcal{O}$.

First, $\mathrm{coker}(i)$ injects into $H^1(I_q, \mathrm{ad}^0\,\rho_{K/\mathcal{O}})^{G_q/I_q}$. Let $\chi\colon G_{\mathbb{Q}} \to 2^{-1}\mathcal{O}/\mathcal{O}$ be the homomorphism that factors through $\mathrm{Gal}(\mathbb{Q}(\sqrt{-q})/\mathbb{Q})$ and sends the nontrivial element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{-q})/\mathbb{Q})$ to $2^{-1}+\mathcal{O} \in 2^{-1}\mathcal{O}/\mathcal{O}$. This χ is a class in $H^1(\mathbb{Q}, 2^{-1}\mathcal{O}/\mathcal{O})$ that is unramified outside of q and ∞ and whose restriction to $H^1(I_q, 2^{-1}\mathcal{O}/\mathcal{O})$ has order 2. For any $n \geq 1$, if $a \in \mathcal{O}$ satisfies $2a \in (\varpi^n)$, then the scalar matrix $\begin{pmatrix} a & \\ & a \end{pmatrix} \pmod{\varpi}^n$ lies in $\mathrm{ad}^0\,\rho_{\mathcal{O}/\varpi^n}$. We deduce a $G_{\mathbb{Q}}$-equivariant injection $\iota\colon 2^{-1}\mathcal{O}/\mathcal{O} \to \mathrm{ad}^0\,\rho_{K/\mathcal{O}}$ with $G_{\mathbb{Q}}$ acting trivially on $2^{-1}\mathcal{O}/\mathcal{O}$. We then consider the image $\iota_*(\chi) \in H^1(\mathbb{Q}, \mathrm{ad}^0\,\rho_{K/\mathcal{O}})$. This class lies in $H^1_{\mathcal{D}'}(\mathrm{ad}^0\,\rho_{K/\mathcal{O}})$ and we claim its restriction to $H^1(I_q, \mathrm{ad}^0\,\rho_{K/\mathcal{O}})$ generates a submodule isomorphic to $\mathcal{O}/2\mathcal{O}$. Indeed, since ρ is unramified at q, the map $H^1(I_q, 2^{-1}\mathcal{O}/\mathcal{O}) \to H^1(I_q, \mathrm{ad}^0\,\rho_{K/\mathcal{O}})$ is injective. The claim then follows from the commutativity of the diagram

$$\begin{array}{ccc} H^1(\mathbb{Q}, 2^{-1}\mathcal{O}/\mathcal{O}) & \longrightarrow & H^1(\mathbb{Q}, \mathrm{ad}^0\,\rho_{K/\mathcal{O}}) \\ \downarrow & & \downarrow \\ H^1(I_q, 2^{-1}\mathcal{O}/\mathcal{O}) & \longrightarrow & H^1(I_q, \mathrm{ad}^0\,\rho_{K/\mathcal{O}}). \end{array}$$

We have shown that there is an injection $\mathcal{O}/2\mathcal{O} \hookrightarrow \mathrm{coker}(i)$, so it only remains to show the latter has length at most $\mathrm{length}_{\mathcal{O}}\,\mathcal{O}/2\mathcal{O}$. The trace pairing induces an isomorphism between $(\mathrm{ad}\,\rho/\mathfrak{z})^\vee \cong \mathrm{ad}^0\,\rho_{K/\mathcal{O}}$. The argument of [CDT99, Corollary 1.4.3] (see also [Dic01, §11.3]) then shows that $\mathrm{coker}(\iota)$ has length at most

$$\mathrm{length}_{\mathcal{O}}(\mathrm{ad}\,\rho/\mathfrak{z})(1)^{I_q}/(\mathrm{Frob}_q - 1)(\mathrm{ad}\,\rho/\mathfrak{z})(1)^{I_q}.$$

The prime q is chosen so that ρ is unramified at q and $\overline{\rho}(\mathrm{Frob}_q)$ is regular semisimple. Enlarging $\mathcal{O}$ if necessary, we can compute in a basis in which $\rho(\mathrm{Frob}_q)$ is the diagonal matrix $\begin{pmatrix} \alpha & \\ & \beta \end{pmatrix}$. In particular, if $X = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{ad}\,\rho(1)$, we have

$$(\mathrm{Frob}_q - 1)X = \begin{pmatrix} (q-1)a & (q\alpha/\beta - 1)b \\ (q\beta/\alpha - 1)c & (q-1)d \end{pmatrix}.$$

Then since $\alpha/\beta \neq 1 \pmod{\varpi}$ and $q \equiv 3 \pmod 4$, we compute that

$$(\mathrm{Frob}_q - 1)(\mathrm{ad}\,\rho)(1) + \mathfrak{z}(1) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a \equiv d \bmod 2\mathcal{O} \right\},$$

and

$$(\mathrm{ad}\,\rho/\mathfrak{z})(1)^{I_q}/(\mathrm{Frob}_q - 1)(\mathrm{ad}\,\rho/\mathfrak{z})(1)^{I_q} \cong \mathcal{O}/2\mathcal{O}. \qquad \square$$

4.11. **Proof of Theorem 4.3 when $T = S$.** The $T \neq S$ case proved in §4.6 implies that $\phi_{\mathcal{D}'}$ is an isomorphism of flat local complete intersections over $\mathcal{O}$, and thus

$$\mathrm{length}_{\mathcal{O}}\,\mathfrak{p}'/\mathfrak{p}'^2 = \mathrm{length}_{\mathcal{O}}\,\mathcal{O}/\eta'$$

by Wiles's numerical criterion [DDT97, Theorem 5.3]. This, Lemmas 4.9 and 4.10, and another application of the numerical criterion imply that $\phi_{\mathcal{D}}$ is an isomorphism of flat local complete intersections over $\mathcal{O}$. □

5. Selmer groups and Watkins's conjecture

Throughout this section we fix an elliptic curve E over $\mathbb{Q}$. We let N be the conductor of E, and let Δ be the discriminant of (some model of) E. We let

$$\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{GL}(V) \cong \mathrm{GL}_2(\mathbb{F}_2)$$

be the Galois representation on the 2-torsion points $V = E[2](\overline{\mathbb{Q}})$ of E.

We assume the following.

(1) N is even and not divisible by 4.
(2) $E[2](\mathbb{Q}) = \{0\}$
(3) $\mathrm{val}_p(\Delta)$ is odd for any prime p of multiplicative reduction for E.

5.1. **Selmer groups for V and $\mathrm{Sym}^2 V$.** We let $\delta\colon E(\mathbb{Q})/2E(\mathbb{Q}) \to H^1(\mathbb{Q}, V)$ be the (global) Kummer map, and for any place v of $\mathbb{Q}$, let $\delta_v\colon E(\mathbb{Q}_v)/2E(\mathbb{Q}_v) \to H^1(\mathbb{Q}_v, V)$ be the (local) Kummer map at v. Then the 2-Selmer group of E is defined as

$$\mathrm{Sel}_2(E) = \{\phi \in H^1(\mathbb{Q}, V) : \mathrm{res}_v(\phi) \in \mathrm{im}(\delta_v) \text{ for every } v\}$$

We let $\mathrm{ad}\,\overline{\rho} = \mathrm{Hom}_{\mathbb{F}_2}(V, V)$ be the adjoint representation of $\overline{\rho}$. We let $\mathrm{ad}^0\,\overline{\rho} \subset \mathrm{ad}\,\overline{\rho}$ be its trace 0 subspace and let $\mathfrak{z} \subset \mathrm{ad}\,\overline{\rho}$ be the subspace of scalar endomorphisms. The pairing $(X, Y) \to \mathrm{tr}(XY)$ is perfect and induces a duality between $\mathrm{ad}^0\,\overline{\rho}$ and $\mathrm{ad}\,\overline{\rho}/\mathfrak{z}$. The Weil pairing defines and isomorphism $V \cong V^*$, which then induces isomorphisms $\mathrm{ad}\,\overline{\rho} \cong V \otimes V^* \cong V \otimes V$ descending to an isomorphism $\mathrm{ad}\,\overline{\rho}/\mathfrak{z} \cong \mathrm{Sym}^2 V$. (We use a different convention than [Dum06]: for us $\mathrm{Sym}^2 V$ denotes the quotient of $V \otimes V$ by the action of the symmetric group on two elements.)

For $x, y \in V$, we let xy denote the image of $x \otimes y$ in $\mathrm{Sym}^2 V$. The map $s\colon V \to \mathrm{Sym}^2 V$ given by $x \mapsto x^2$ is $\mathbb{F}_2$-linear and $G_{\mathbb{Q}}$-equivariant. We again denote by s the composite of this map with our fixed isomorphism $\mathrm{Sym}^2 V \cong \mathrm{ad}\,\overline{\rho}/\mathfrak{z}$. In particular, it induces a linear map

$$s_*\colon H^1(\mathbb{Q}, V) \to H^1(\mathbb{Q}, \mathrm{ad}\,\overline{\rho}/\mathfrak{z})$$

that will play an important role.

Lemma 5.2. *We have $G_{\mathbb{Q}}$-equivariant decompositions $\mathrm{ad}^0\,\overline{\rho} \cong \mathbb{F}_2 \oplus V$ and $\mathrm{ad}\,\overline{\rho}/\mathfrak{z} \cong \mathbb{F}_2 \oplus \mathrm{im}(s) \cong \mathbb{F}_2 \oplus V$.*

Proof. Since $\mathrm{ad}^0\,\overline{\rho}$ is dual to $\mathrm{ad}\,\overline{\rho}/\mathfrak{z}$ and both $\mathbb{F}_2$ and V are self-dual, it suffices to prove the claim for $\mathrm{ad}\,\overline{\rho}/\mathfrak{z}$.

It is clear that $s\colon V \to \mathrm{Sym}^2 V$ is injective and that $\mathrm{im}(s) = \mathbb{F}_2 x^2 + \mathbb{F}_2 y^2$. A computation shows that $x^2 + xy + y^2$ is invariant under $\mathrm{GL}_2(\mathbb{F}_2)$, and the result follows. □

Define subspaces $L_v \subset H^1(\mathbb{Q}_v, \mathrm{ad}^0\,\overline{\rho})$ for each place v of $\mathbb{Q}$ as follows.

- Let $v = p$ be a prime of multiplicative reduction for E. Our assumptions imply there is a basis for V such that $\overline{\rho}|_{G_p} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. We fix such a basis and then identify $\mathrm{ad}^0\,\overline{\rho}$ with the space of 2×2 matrices with entries in

$\mathbb{F}_2$ and trace 0. Let $\mathfrak{n} \subset \mathfrak{b} \subset \mathrm{ad}^0\,\overline{\rho}$ be the subspaces of upper triangular nilpotent and upper triangular trace 0 matrices, respectively. So $\mathfrak{b} = \mathfrak{z} \oplus \mathfrak{n}$. We let

$$L_p(\mathfrak{b}) = \ker(H^1(\mathbb{Q}_p, \mathfrak{b}) \to H^1(I_{\mathbb{Q}_p}, \mathfrak{b}/\mathfrak{n}))$$

and then define

$$L_p = \mathrm{im}(L_p(\mathfrak{b}) \to H^1(\mathbb{Q}_p, \mathrm{ad}^0\,\overline{\rho})).$$

- For $v = p$ a prime at which E has additive reduction, wet let $L_p = H^1(\mathbb{Q}_p, \mathrm{ad}^0\,\overline{\rho})$.
- For all over finite places v, we let $L_v = H^1_{\mathrm{ur}}(\mathbb{Q}_v, \mathrm{ad}^0\,\overline{\rho})$.
- For $v = \infty$, we let $L_\infty = H^1(\mathbb{Q}_\infty, \mathrm{ad}^0\,\overline{\rho})$.

We then let $L_v^\perp \subset H^1(\mathbb{Q}_v, \mathrm{ad}\,\overline{\rho}/\mathfrak{z})$ be the dual local condition, i.e. the annihilator of L_v under local Tate duality.

Finally, we define the Selmer group

$$H^1_{\mathcal{L}}(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho}) = \{\phi \in H^1(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho}) : \mathrm{res}_v(\phi) \in L_v \text{ for all } v\},$$

and the dual Selmer group

$$H^1_{\mathcal{L}^\perp}(\mathbb{Q}, \mathrm{ad}\,\overline{\rho}/\mathfrak{z}) = \{\phi \in H^1(\mathbb{Q}, \mathrm{ad}\,\overline{\rho}/\mathfrak{z}) : \mathrm{res}_v(\phi) \in L_v^\perp \text{ for all } v\}.$$

Remark 5.3. Let p be an odd prime of multiplicative reduction for E. Another natural choice for our local condition at p would be the unramified classes

$$L_p^{\mathrm{ur}} := \mathrm{im}(H^1(\mathbb{Q}_p^{\mathrm{ur}}/\mathbb{Q}_p, (\mathrm{ad}^0\,\overline{\rho})^{I_{\mathbb{Q}_p}}) \xrightarrow{\mathrm{inf}} H^1(\mathbb{Q}_p, \mathrm{ad}^0\,\overline{\rho})).$$

We have a containment $L_p^{\mathrm{ur}} \subset L_p$ but unlike in the case when the coefficient prime is odd, this containment is strict. With the notation as in the definition of L_p above, the $G_{\mathbb{Q}_p}$-action on $\mathfrak{b}$ is trivial, so there is a ramified class in L_p given by a ramified homomorphism $G_{\mathbb{Q}_p} \to \mathfrak{n}$. In the case of odd coefficient prime, the analogous cocycle would be a coboundary, but it is not in our case. This class does however become a coboundary with $\mathrm{ad}\,\overline{\rho}$ coefficients and so both L_p^{ur} and L_p have the same image in $H^1(\mathbb{Q}_p, \mathrm{ad}\,\overline{\rho})$ and both can be used to describe the tangent space of our local deformation problem. This is advantageous for us via Lemma 5.6 below.

Another plausible condition to take would be the subspace $L'_p \subset L_p$ of classes that restrict to 0 in $H^1(\mathbb{Q}_p, \mathfrak{b}/\mathfrak{n})$. This would correspond to the deformation condition where the diagonal characters of the deformation are fixed as in Lemma 2.3. Again, when the coefficient prime is odd, these spaces are the same, but in our situation they are distinct because of unramified quadratic twists. Using the local condition L'_p, one would naturally be lead to compare deformation rings using the local deformation condition of Lemma 2.3 with Hecke algebras acting on quotients of the modular curve by Atkin–Lehner automorphisms as in [DK13, §12]. We do not pursue this here.

Notation 5.4. We will write $h^i(\_, M)$ for the $\mathbb{F}_2$-dimension of a cohomology group with coefficients in an $\mathbb{F}_2$-vector space M. We use the similar notation for Selmer and dual Selmer groups, i.e.

$$\mathrm{sel}_2(E) := \dim_{\mathbb{F}_2} \mathrm{Sel}_2(E)$$
$$h^1_{\mathcal{L}}(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho}) := \dim_{\mathbb{F}_2} H^1_{\mathcal{L}}(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho}),$$
$$h^1_{\mathcal{L}^\perp}(\mathbb{Q}, \mathrm{ad}\,\overline{\rho}/\mathfrak{z}) := \dim_{\mathbb{F}_2} H^1_{\mathcal{L}^\perp}(\mathbb{Q}, \mathrm{ad}\,\rho/\mathfrak{z}).$$

Lemma 5.5. *Let Q be the set of primes at which E has additive reduction. We have*

$$\mathrm{sel}_2(E) \leq h_{\mathcal{L}^\perp}(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho}) - 1 + \sum_{v \in Q \cup \{\infty\}} h^0(\mathbb{Q}_v, V).$$

Proof. Let $\mathrm{Sel}_2(E)^0 = \{\phi \in \mathrm{Sel}_2(E) : \mathrm{res}_v(\phi) = 0 \text{ for all } v \in Q \cup \{\infty\}\}$ and let $\mathrm{sel}_2(E)^0$ denote its dimension. If $v = q$ is a prime of additive reduction, we apply [MR10, Lemma 2.2(i)]: since $E(\mathbb{Q}_q)$ contains a pro-q subgroup with finite index and $q \neq 2$, we have

$$\dim_{\mathbb{F}_2} \mathrm{im}(\delta_q) = \dim_{\mathbb{F}_2} E(\mathbb{Q}_q)/2E(\mathbb{Q}_q) = \dim_{\mathbb{F}_2} E[2](\mathbb{Q}_q) = h^0(G_q, V).$$

Similarly, if $v = \infty$, then either $E(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ and G_∞ acts on V by an involution with 1-dimensional invariant subspace, or $E(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{R}/\mathbb{Z}$ and G_∞ acts trivially on V. In either case, we have

$$\dim_{\mathbb{F}_2} \mathrm{im}(\delta_\infty) = \dim_{\mathbb{F}_2} E(\mathbb{R})/2E(\mathbb{R}) = h^0(G_\infty, V) - 1.$$

Thus

$$\mathrm{sel}_2(E) \leq \mathrm{sel}_2(E)^0 - 1 + \sum_{v \in Q \cup \{\infty\}} h^0(\mathbb{Q}_v, V).$$

By Lemma 5.2, s_* is injective, so we are reduced to showing that $s_*(\mathrm{Sel}_2(E)^0)$ is contained in $H_{\mathcal{L}^\perp}(\mathbb{Q}, \mathrm{ad}\,\overline{\rho}/\mathfrak{z})$. Fix $\phi \in \mathrm{Sel}_2(E)^0$.

If p is a prime of good reduction, then $\mathrm{res}_p(\phi) \in H^1_{\mathrm{ur}}(\mathbb{Q}_p, V)$. Since s_* takes unramified classes to unramified classes, $\mathrm{res}_p(s_*(\phi)) = s_*(\mathrm{res}_p(\phi)) \in H^1_{\mathrm{ur}}(\mathbb{Q}_p, \mathrm{ad}\,\overline{\rho}/\mathfrak{z}) = L_p^\perp$. If $v \in Q \cup \{\infty\}$, our definition of $\mathrm{Sel}_2(E)^0$ implies that $\mathrm{res}_v(s_*(\phi)) = s_*(\mathrm{res}_v(\phi)) = 0 \in L_v^\perp = \{0\}$.

Finally, let p be a prime at which E has multiplicative reduction. Let $\psi\colon \overline{\mathbb{Q}}_p/q^{\mathbb{Z}} \xrightarrow{\sim} E(\overline{\mathbb{Q}}_p)$ be the Tate parametrization. We fix the basis $\{x, y\} = \{\psi(-1), \psi(q^{1/2}\}$ of $E[2](\overline{\mathbb{Q}}_p)$. In this basis, we let $\mathfrak{n} \subset \mathfrak{b} \subset \mathrm{ad}^0\,\overline{\rho}$ be the subspaces of upper triangular nilpotent and upper triangular trace 0 matrices, respectively. We claim that $s_*(\phi)$ is contained in the image of $H^1(\mathbb{Q}_p, \mathfrak{b}/\mathfrak{z}) \to H^1(\mathbb{Q}_p, \mathrm{ad}\,\overline{\rho}/\mathfrak{z})$. Since $\mathfrak{b}/\mathfrak{z} \subset \mathfrak{b}^\perp \subset \mathrm{ad}\,\overline{\rho}/\mathfrak{z}$ and L_p is contained in the image of $H^1(\mathbb{Q}_p, \mathfrak{b}) \to H^1(\mathbb{Q}_p, \mathrm{ad}^0\,\overline{\rho})$, we conclude that $s_*(\phi) \subseteq L_p^\perp$.

That $s_*(\phi)$ is contained in the image of $H^1(\mathbb{Q}_p, \mathfrak{b}/\mathfrak{z}) \to H^1(\mathbb{Q}_p, \mathrm{ad}\,\overline{\rho}/\mathfrak{z})$ is contained in parts (2) and (3) of the proof of [Dum06, Lemma 4.1]. Since the argument is short, we repeat it here for the convenience of the reader. Choose $P \in E(\mathbb{Q}_p)$ such that ϕ is the image of P under the Kummer map, and choose $u \in \overline{\mathbb{Q}}_p^\times$ with $\psi(u) = P$. Choose $v \in \overline{\mathbb{Q}}_p^\times$ with $v^2 = u$ and let $Q = \psi(v)$. So the class ϕ is represented by the cocycle $\sigma \mapsto \sigma(Q) - Q$. If E has split multiplicative, then ψ is Galois equivariant, we can assume that $u \in \mathbb{Q}_p^\times$, and we have $\sigma(Q) - Q = \psi(\sigma(v)/v)$. But since $(\sigma(v)/v)^2 = \sigma(u)/u = 1$, we have $\sigma(Q) - Q \in \mathbb{F}_2 x$. If E has nonsplit reduction at p, then letting χ denotes the nontrivial quadratic character of $G_{\mathbb{Q}_p}$, the isomorphism ψ satisfies $\psi(\sigma(y)) = \chi(y)\sigma(\psi(y))$ for any $y \in \overline{\mathbb{Q}}_p^\times$ and $\sigma \in G_{\mathbb{Q}_p}$. In this case, we can assume $u \in \mathbb{Q}_{p^2}^\times$ and $\mathrm{Nm}_{\mathbb{Q}_{p^2}/\mathbb{Q}_p}(u) = 1$ (see [Sil94, Corollary V.5.4], for example). Then for $\sigma \in G_{\mathbb{Q}_{p^2}}$, we have $\sigma(u)^{\chi(\sigma)} = u^1 = u$, and for $\sigma \in G_{\mathbb{Q}_p} \setminus G_{\mathbb{Q}_{p^2}}$, we have $\sigma(u)^{\chi(\sigma)} = (u^{-1})^{-1} = u$. Thus $(\sigma(v)^{\chi(\sigma)}/v)^2 = 1$ and we again deduce that

$\sigma(Q) - Q \in \mathbb{F}_2 x$ for any $\sigma \in G_{\mathbb{Q}_p}$. Finally, since $\{x, y\}$ are a symplectic basis for $E[2](\overline{\mathbb{Q}}_p)$, the squaring map s sends x to $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ mod $\mathfrak{z}$ in this basis. □

Lemma 5.6. *Let Q be the set of primes at which E has additive reduction and let n be the number of distinct prime divisors of N. Then*

$$h^1_{\mathcal{L}}(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho}) - h^1_{\mathcal{L}^\perp}(\mathbb{Q}, \mathrm{ad}\,/\mathfrak{z}) = n - 1 + \sum_{v \in Q \cup \{\infty\}} h^0(\mathbb{Q}_q, V).$$

Proof. In our situation, the Greenberg–Wiles formula is

$$h^1_{\mathcal{L}}(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho}) - h^1_{\mathcal{L}^\perp}(\mathbb{Q}, \mathrm{ad}\,/\mathfrak{z})) = h^0(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho}) - h^0(\mathbb{Q}, \mathrm{ad}\,\overline{\rho}/\mathfrak{z}) + \sum_v (\ell_v - h^0(\mathbb{Q}_v, \mathrm{ad}^0\,\overline{\rho})),$$

where we have written $\ell_v = \dim_{\mathbb{F}_2} L_v$. Since $\overline{\rho}$ is absolutely irreducible, Lemma 5.2 implies that $h^0(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho}) = h^0(\mathbb{Q}, \mathrm{ad}\,\overline{\rho}/\mathfrak{z}) = 1$. If $v \nmid N$ is finite, we have $h^1_{\mathrm{ur}}(\mathbb{Q}_v, \mathrm{ad}^0\,\overline{\rho}) = h^0(\mathbb{Q}_v, \mathrm{ad}^0\,\overline{\rho})$. We are thus reduced to showing that

$$\sum_{v \in \{p|N\} \cup \{\infty\}} (\ell_v - h^0(\mathbb{Q}_v, \mathrm{ad}^0\,\overline{\rho})) = n - 1 + \sum_{v \in Q \cup \{\infty\}} h^0(\mathbb{Q}_q, V). \tag{5}$$

First take $v = \infty$ and let $1 \neq c \in G_\infty$. Either $\overline{\rho}(c) = 1$ or $\overline{\rho}(c)$ is conjugate to $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and thus one computes that

$$\ell_v - h^0(G_\infty, \mathrm{ad}^0\,\overline{\rho}) = h^1(G_\infty, \mathrm{ad}^0\,\overline{\rho}) - h^0(G_\infty, \mathrm{ad}^0\,\overline{\rho}) = \begin{cases} 1 - 2 = -1 & \text{if } \overline{\rho}(c) \neq 1, \\ 3 - 3 = 0 & \text{if } \overline{\rho}(c) = 1. \end{cases}$$

In either case, we have

$$\ell_v - h^0(G_\infty, \mathrm{ad}^0\,\overline{\rho}) = h^0(G_\infty, V) - 2. \tag{6}$$

If $v = q \in Q$ is a prime of additive reduction, we have $L_q = H^1(\mathbb{Q}_q, \mathrm{ad}^0\,\overline{\rho})$. Then the local Euler characteristic, local Tate duality, and Lemma 5.2 give

$$\ell_q - h^0(\mathbb{Q}_q, \mathrm{ad}^0\,\overline{\rho}) = h^0(\mathbb{Q}_q, \mathrm{ad}\,\overline{\rho}/\mathfrak{z}) = 1 + h^0(\mathbb{Q}_q, V). \tag{7}$$

Now consider $v = p$ a prime of multiplicative reduction. We will show that for such p,

$$\ell_p - h^0(\mathbb{Q}_p, \mathrm{ad}^0\,\overline{\rho}) = \begin{cases} 2 & \text{if } p = 2 \\ 1 & \text{otherwise,} \end{cases} \tag{8}$$

Summing (6), (7), and (8) yields (5).

Our assumptions imply that there is a basis for V such that $\overline{\rho}|_{G_{\mathbb{Q}_p}} = \begin{pmatrix} 1 & \alpha \\ & 1 \end{pmatrix}$ with $\alpha \colon G_{\mathbb{Q}_p} \to \mathbb{F}_2$ a ramified homomorphism. Fixing such a basis, we let $\mathfrak{n} \subset \mathfrak{b} \subset \mathrm{ad}^0\,\overline{\rho}$ be the subspaces of upper triangular nilpotent and upper triangular trace 0 matrices, respectively. One computes directly that $H^0(\mathbb{Q}_p, \mathrm{ad}^0\,\overline{\rho}) = \mathfrak{b} = \mathfrak{z} \oplus \mathfrak{n}$, which is 2-dimensional. We claim that

$$\ell_p = \begin{cases} 4 & \text{if } p = 2, \\ 3 & \text{otherwise.} \end{cases}$$

Fix the following basis for $\mathrm{ad}^0\,\overline{\rho}$,

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Taking cohomlogy of the exact sequence

$$0 \to \mathfrak{b} \to \mathrm{ad}^0\,\overline{\rho} \to \mathrm{ad}^0\,\overline{\rho}/\mathfrak{b} \to 0,$$

we find that $H^1(\mathbb{Q}_p, \mathfrak{b}) \to H^1(\mathbb{Q}_p, \mathrm{ad}^0\,\overline{\rho})$ has 1-dimensional kernel, spanned by the class of $\sigma \mapsto \alpha(\sigma)(z+e)$. Since α is ramified, this class is not contained in $L_p(\mathfrak{b})$, so $L_p(\mathfrak{b}) \cong L_p$. Since $\mathfrak{b} = \mathfrak{z} \oplus \mathfrak{n}$ has trivial $G_{\mathbb{Q}_p}$-action, we see that

$$L_p(\mathfrak{b}) = H^1_{\mathrm{ur}}(\mathbb{Q}_p, \mathfrak{z}) \oplus H^1(\mathbb{Q}_p, \mathfrak{n}) \cong \mathrm{Hom}_{\mathrm{cts}}(G_{\mathbb{Q}_p}/I_{\mathbb{Q}_p}, \mathbb{F}_2) \oplus \mathrm{Hom}_{\mathrm{cts}}(G_{\mathbb{Q}_p}, \mathbb{F}_2)$$

which has dimension $1+3=4$ if $p=2$ and dimension $1+2=3$ if p is odd. □

Combining Lemmas 5.5 and 5.6 yields the following lemma.

Lemma 5.7. *Let n be the number of distinct prime divisors of N. Then*

$$h^1_{\mathcal{L}}(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho}) \geq \mathrm{sel}_2(E) + n.$$

5.8. $R = T$ **and Watkins's conjecture.** Let $S = \{p \mid N\} \cup \{\infty\}$, let $T = \{p \parallel N\} \cup \{\infty\}$, and define the deformation datum

$$\mathcal{D} = (\mathbb{Q}, S, \mathbb{Z}_2, \overline{\rho}, \epsilon, \{D_v\}_{v \in T}),$$

as in §2.7, where

- D_p is as in Lemma 2.2 for $p \parallel N$, and
- D_∞ is as in Lemma 2.5.

Let $R_{\mathcal{D}}$ be the universal type $\mathcal{D}$ deformation ring.

Lemma 5.9. *Let $H^1_{\mathcal{L}}(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho})$ be the Selmer group of §5.1. The map $H^1_{\mathcal{L}}(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho}) \to H^1(\mathbb{Q}, \mathrm{ad}\,\overline{\rho})$ has 1-dimensional kernel and image contained in*

$$H^1_{\mathcal{D}}(\mathrm{ad}\,\overline{\rho}) \cong \mathrm{Hom}_k(\mathfrak{m}_{R_{\mathcal{D}}}/(2, \mathfrak{m}^2_{R_{\mathcal{D}}}), \mathbb{F}_2).$$

Proof. Taking cohomology of the exact sequence

$$0 \to \mathrm{ad}^0\,\overline{\rho} \to \mathrm{ad}\,\overline{\rho} \to \mathrm{ad}\,\overline{\rho}/\,\mathrm{ad}^0\,\overline{\rho} \to 0 \tag{9}$$

shows that the kernel of $H^1(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho}) \to H^1(\mathbb{Q}, \mathrm{ad}\,\rho)$ is 1-dimensional. We claim this 1-dimensional space lies in $H^1_{\mathcal{L}}(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho})$. Let ϕ be a nonzero element of this kernel. Then ϕ is unramified at any prime at which $\overline{\rho}$ is unramified, so $\mathrm{res}_v(\phi) \in L_v = H^1_{\mathrm{ur}}(\mathbb{Q}_v, \mathrm{ad}^0\,\overline{\rho})$ for $v \notin S$. For $v = p$ a prime of multiplicative reduction, fix a basis for V such that $\overline{\rho}|_{G_{\mathbb{Q}_p}} = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$. Then choosing $X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ as a lift of a nonzero element of $\mathrm{ad}\,\overline{\rho}/\,\mathrm{ad}^0\,\overline{\rho}$, we compute that $\mathrm{res}_p(\phi)$ is represented by the cocycle

$$\sigma \mapsto \sigma X \sigma^{-1} - X = \begin{pmatrix} 0 & \alpha(\sigma) \\ 0 & 0 \end{pmatrix},$$

so $\mathrm{res}_p(\phi) = 0 \in L_p$ by definition of L_p. The conditions at primes of additive reduction or at $v = \infty$ are automatic.

We now check the image lies in $H^1_{\mathcal{D}}(\mathrm{ad}\,\overline{\rho})$. Let $\phi = [\kappa] \in H^1_{\mathcal{L}}(\mathbb{Q}, \mathrm{ad}^0\,\overline{\rho})$ be represented by a cocycle $\kappa\colon G_F \to \mathrm{ad}^0\,\overline{\rho}$. We need to check that the lift $\rho = (1+\epsilon\kappa)\overline{\rho}\colon G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_2[\epsilon])$ is of type $\mathcal{D}$. Since ϕ is unramified outside of S, so is ρ.

Also, since κ has coefficients in $\mathrm{ad}^0\,\overline{\rho}$, $\det\rho = \det\overline{\rho} = \overline{\epsilon}_2$. It remains to check that $\rho|_{G_{\mathbb{Q}_v}}$ satisfies our condition D_v for any $v \in T$.

For $v = \infty$, Lemma 2.6 implies that $\rho|_{G_{\mathbb{Q}_\infty}}$ satisfies our condition D_∞. Now let $v = p \in T$ be a (finite) prime. Fix a basis for V such that $\overline{\rho}|_{G_{\mathbb{Q}_p}} = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$. By definition of L_p, after possibly modifying κ by a coboundary, we can assume that $\kappa(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ 0 & a(\sigma) \end{pmatrix}$ for $\sigma \in G_{\mathbb{Q}_p}$ and that $a(\sigma) = 0$ for $\sigma \in I_{\mathbb{Q}_p}$. Then $(1+\epsilon\kappa)\overline{\rho}|_{G_{\mathbb{Q}_p}}$ is of type D_p. □

Proof of Theorem 1.2. Let $J_0(N)$ be the Jacobian of the (compact) modular curve $X_0(N)$, let $\mathbb{T}_{\mathbb{Z}}(N)$ be the subalgebra of $\mathrm{End}(J_0(N))$ generated by the Hecke operators T_p for $p \nmid N$ and U_p for $p \mid N$, and set $\mathbb{T}(N) = \mathbb{T}_{\mathbb{Z}}(N) \otimes_{\mathbb{Z}} \mathbb{Z}_2$. The elliptic curve E defines an augmentation $\lambda\colon \mathbb{T}(N) \to \mathbb{Z}_2$ by sending T_p for $p \nmid N$, resp. U_p for $p \mid N$, to $a_p(E)$. Let $\mathfrak{m} = (2, \ker(\lambda)) \subset \mathbb{T}(N)$, $I = \mathrm{Ann}_{\mathbb{T}(N)_{\mathfrak{m}}}(\ker(\lambda))$, and $\eta = \lambda(I)$. Then the argument of [Dum06, Proposition 5.4] or [DK13, Theorem 9.4] (see also [ARS12, Theorem 2.1 and Remark 5.3]) shows that $\mathrm{length}_{\mathbb{Z}_2}\,\mathbb{Z}_2/\eta = \mathrm{val}_2(m_E)$ with m_E the modular degree of E. The main theorem then follows by combining Lemmas 5.7 and 5.9 and Corollary 4.5. □

References

[AKT22] Patrick B. Allen, Chandrashekhar Khare, and Jack A. Thorne, *Modularity of* $\mathrm{GL}_2(\mathbb{F}_p)$*-representations over cm fields*, 2022.

[All14a] Patrick B. Allen, *Modularity of nearly ordinary 2-adic residually dihedral Galois representations*, Compos. Math. **150** (2014), no. 8, 1235–1346. MR 3252020

[All14b] ———, *Modularity of nearly ordinary 2-adic residually dihedral Galois representations*, Compos. Math. **150** (2014), no. 8, 1235–1346. MR 3252020

[All16] ———, *Deformations of polarized automorphic Galois representations and adjoint Selmer groups*, Duke Math. J. **165** (2016), no. 13, 2407–2460. MR 3546966

[ARS12] Amod Agashe, Kenneth A. Ribet, and William A. Stein, *The modular degree, congruence primes, and multiplicity one*, Number theory, analysis and geometry, Springer, New York, 2012, pp. 19–49. MR 2867910

[BKM24] Gebhard Böckle, Chandrashekhar B. Khare, and Jeffrey Manning, *Wiles defect of Hecke algebras via local-global arguments*, J. Inst. Math. Jussieu **23** (2024), no. 6, 2461–2541, With an appendix by Najmuddin Fakhruddin and Khare. MR 4825120

[Buz00a] Kevin Buzzard, *On level-lowering for mod 2 representations*, Math. Res. Lett. **7** (2000), no. 1, 95–110. MR 1748291

[Buz00b] ———, *On level-lowering for mod 2 representations*, Math. Res. Lett. **7** (2000), no. 1, 95–110. MR 1748291

[Car24] Jerson Caro, *Watkins's conjecture for elliptic curves over function fields*, Math. Z. **308** (2024), no. 3, Paper No. 50, 13. MR 4808956

[CDT99] Brian Conrad, Fred Diamond, and Richard Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), no. 2, 521–567. MR 1639612

[CE09] Frank Calegari and Matthew Emerton, *Elliptic curves of odd modular degree*, Israel J. Math. **169** (2009), 417–444. MR 2460912

[CP22] Jerson Caro and Hector Pasten, *Watkins's conjecture for elliptic curves with non-split multiplicative reduction*, Proc. Amer. Math. Soc. **150** (2022), no. 8, 3245–3251. MR 4439450

[DDT97] Henri Darmon, Fred Diamond, and Richard Taylor, *Fermat's last theorem*, Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993), Int. Press, Cambridge, MA, 1997, pp. 2–140. MR 1605752

[Dic01] Mark Dickinson, *On the modularity of certain 2-adic Galois representations*, Duke Math. J. **109** (2001), no. 2, 319–382. MR 1845182

[DK13] Neil Dummigan and Srilakshmi Krishnamoorthy, *Powers of 2 in modular degrees of modular abelian varieties*, J. Number Theory **133** (2013), no. 2, 501–522. MR 2994371

[Dum06] Neil Dummigan, *On a conjecture of Watkins*, J. Théor. Nombres Bordeaux **18** (2006), no. 2, 345–355. MR 2289428

[FP78] Zbigniew Fiedorowicz and Stewart Priddy, *Homology of classical groups over finite fields and their associated infinite loop spaces*, Lecture Notes in Mathematics, vol. 674, Springer, Berlin, 1978. MR 513424

[Hid89] Haruzo Hida, *Nearly ordinary Hecke algebras and Galois representations of several variables*, Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988), Johns Hopkins Univ. Press, Baltimore, MD, 1989, pp. 115–134. MR 1463699

[Kis07] Mark Kisin, *Modularity of 2-dimensional Galois representations*, Current developments in mathematics, 2005, Int. Press, Somerville, MA, 2007, pp. 191–230. MR 2459302

[Kis09] ———, *Modularity of 2-adic Barsotti-Tate representations*, Invent. Math. **178** (2009), no. 3, 587–634. MR 2551765

[KK18] Matija Kazalicki and Daniel Kohen, *On a special case of Watkins' conjecture*, Proc. Amer. Math. Soc. **146** (2018), no. 2, 541–545. MR 3731689

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger, *On Serre's conjecture for 2-dimensional mod p representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Ann. of Math. (2) **169** (2009), no. 1, 229–253. MR 2480604

[KW09b] ———, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504. MR 2551763

[KW09c] ———, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586. MR 2551764

[MR10] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575. MR 2660452

[NT23a] James Newton and Jack A. Thorne, *Adjoint selmer groups of automorphic galois representations of unitary type*, 2023.

[NT23b] James Newton and Jack A. Thorne, *Adjoint Selmer groups of automorphic Galois representations of unitary type*, J. Eur. Math. Soc. (JEMS) **25** (2023), no. 5, 1919–1967. MR 4592862

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994. MR 1312368

[Tay]

[Wat02] Mark Watkins, *Computing the modular degree of an elliptic curve*, Experiment. Math. **11** (2002), no. 4, 487–502. MR 1969641

[Wil95] Andrew Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR 1333035

[Yaz11] Soroosh Yazdani, *Modular abelian varieties of odd modular degree*, Algebra Number Theory **5** (2011), no. 1, 37–62. MR 2833784