COMPOSITIO MATHEMATICA

Level raising mod 2 and arbitrary 2-Selmer ranks

Bao V. Le Hung and Chao Li

Compositio Math. **152** (2016), 1576–1608.

doi:10.1112/S0010437X16007454

Compositio Math. 152 (2016) 1576–1608
doi:10.1112/S0010437X16007454

Level raising mod 2 and arbitrary 2-Selmer ranks

Bao V. Le Hung and Chao Li

Abstract

We prove a level raising mod $\ell = 2$ theorem for elliptic curves over $\mathbb{Q}$. It generalizes theorems of Ribet and Diamond–Taylor and also explains different sign phenomena compared to odd ℓ. We use it to study the 2-Selmer groups of modular abelian varieties with common mod 2 Galois representation. As an application, we show that the 2-Selmer rank can be arbitrary in level raising families.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. The modularity theorem [Wil95, TW95, BCDT01] associates to E a weight 2 cusp newform f of level $\Gamma_0(N)$. Let ℓ be a prime such that $E[\ell]$ is an absolutely irreducible $G_{\mathbb{Q}} = \mathrm{Gal}\,(\overline{\mathbb{Q}}/\mathbb{Q})$-representation. For primes $q \nmid N\ell$ satisfying the level raising condition $a_q \equiv \pm(q+1) \bmod \ell$, Ribet's theorem [Rib90] ensures the existence of a weight 2 cusp form g of level $\Gamma_0(Nq)$ that is new at q and $g \equiv f \pmod{\ell}$.

When $\ell > 2$, Diamond and Taylor [DT94a, DT94b] generalized Ribet's theorem and allowed one to level raise at multiple primes $q_1, \dots, q_m$ simultaneously while keeping the form g new at each q_i. At a prime p where g has conductor 1 (i.e. the primes $p \| N$ and $p = q_i$), the local representation of g is either the Steinberg representation or its unramified quadratic twist. The two cases are distinguished by the U_p-eigenvalue, which we call the *sign of* g at p (because it also dictates the sign of the local functional equation at p). At $p \| N$, the sign of g is the same as the sign of f by the mod ℓ congruence, since $\ell > 2$. At $q_i \not\equiv -1 \pmod{\ell}$, the sign of g is uniquely determined by the mod ℓ congruence as well. At $q_i \equiv -1 \pmod{\ell}$, both signs may occur as the sign of g.

When $\ell = 2$, the signs cannot be detected from the mod ℓ congruence. In fact, it is not always possible to keep the same signs at all $p \| N$ when level raising (see Examples 2.14 and 2.15). Nevertheless, we are able to prove the following simultaneous level raising theorem for $\ell = 2$, which allows one to prescribe any signs at q_i and also keep the signs at all but one chosen $p \| N$.

Theorem 1.1. *Let $E/\mathbb{Q}$ be an elliptic curve satisfying (1)–(4) of Assumption 2.1. Let*

$$f = \sum_{n \geqslant 1} a_n q^n \in S_2(N)$$

be the newform associated to E. Let $q_1, \dots, q_m$ be distinct level raising primes for E (Definition 2.7). Given prescribed signs $\varepsilon_1, \dots, \varepsilon_m \in \{\pm 1\}$ and $\epsilon_p \in \{\pm 1\}$ for $p \| N$, there exist a newform

$$g = \sum_{n \geqslant 1} b_n q^n \in S_2(N \cdot q_1 \cdots q_m)$$

Received 12 March 2015, accepted in final form 1 April 2016, published online 1 June 2016.
2010 Mathematics Subject Classification 11F33 (primary), 11G05, 11G10 (secondary).
Keywords: modular forms, Selmer groups.

and a prime λ *of the Hecke field* $F = \mathbb{Q}(\{b_n\}_{n\geqslant 1})$ *above 2 such that*

$$b_p \equiv a_p \pmod{\lambda}, \quad p \nmid N \cdot q_1 \cdots q_m; \quad b_{q_i} = \varepsilon_i, \quad i = 1, \ldots, m,$$

and

$$b_p = \epsilon_p \quad \textit{for all but possibly one chosen } p \| N.$$

Remark 1.2. See Theorem 2.9 for a more general statement including sufficient conditions to when we can prescribe signs at all $p\|N$.

Remark 1.3. Given f, one may ask which signs can occur for congruent newforms g of the same level N (i.e. the case $m = 0$). An argument of Ribet communicated to us shows that if $N = p$ is a prime, then there always exists a congruent newform g of level p with U_p-eigenvalue $+1$. This is best possible as the example $p = 11$ shows: there is a unique newform of level $p = 11$ and only $+1$ occurs as the U_p-eigenvalue. Though Theorem 1.1 does not treat this case, it follows from our method that if there is an odd number of primes $p\|N$, then there always exists a congruent newform g of level N with U_p-eigenvalues $+1$ for all $p\|N$ (see Remark 5.10). This gives a different proof of Ribet's result in the case $N = p$.

For such a level raised newform g, the Eichler–Shimura construction associates to it a modular abelian variety A with real multiplication by $\mathcal{O}_F$. We say that A is *obtained from* E *via level raising* (mod 2). Then E and A are congruent mod 2, i.e.

$$E[2] \otimes k \cong A[\lambda]$$

as $G_{\mathbb{Q}}$-representations, where $k = \mathcal{O}_F/\lambda$ is the residue field. In this way we can view both the 2-Selmer group $\mathrm{Sel}_2(E/\mathbb{Q}) \otimes k$ (extending scalars to k) of E and the λ-Selmer group $\mathrm{Sel}(A) := \mathrm{Sel}_\lambda(A/\mathbb{Q})$ of A as k-subspaces of $H^1(\mathbb{Q}, E[2] \otimes k) = H^1(\mathbb{Q}, A[\lambda])$ cut out by different local conditions. One may ask how the Selmer rank $\dim \mathrm{Sel}(A)$ is distributed when A varies over all abelian varieties obtained from E via level raising. In particular, one may ask if $\dim \mathrm{Sel}(A)$ can take arbitrarily large or small values in this level raising family. We prove the following theorem, which gives an affirmative answer to the latter question.

Theorem 1.4. *Let* $E/\mathbb{Q}$ *be an elliptic curve satisfying Assumption 2.1. Then, for any given integer* $n \geqslant 0$*, there exist infinitely many abelian varieties* A *obtained from* E *via level raising, such that* $\dim \mathrm{Sel}(A) = n$*. In particular, there exist infinitely many abelian varieties* A *obtained from* E *via level raising, such that* $\mathrm{rank}\, A(\mathbb{Q}) = 0$.

Remark 1.5. Mazur and Rubin [MR10] investigated 2-Selmer groups in quadratic twist families over arbitrary number fields in connection with Hilbert's tenth problem. In particular, they proved that if $\mathrm{Gal}\,(\mathbb{Q}(E[2])/\mathbb{Q}) \cong S_3$ and E has negative discriminant Δ, then there exist infinitely many quadratic twists of $E/\mathbb{Q}$ of any given 2-Selmer rank. Theorem 1.4 is an analogue, replacing quadratic twist families with level raising families. In contrast to quadratic twisting, the level raising procedure never introduces places of additive reduction (at the cost of working with modular abelian varieties of higher dimension).

Remark 1.6. Our work is originally motivated by the recent work of Zhang [Zha14], who used the level raising technique to prove the ℓ-part of the Birch and Swinnerton-Dyer conjecture in the analytic rank one case when $\ell > 3$. The strategy is to choose an auxiliary imaginary quadratic

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

field K (over which Heegner points exist) and prove that it is possible to lower the ℓ-Selmer rank over K from one to zero via level raising (mod ℓ). Then the Jochnowitz congruence of Bertolini and Darmon [BD99] (relating the ℓ-parts of $L'(E/K,1)$ and $L(A/K,1)$) allows one to reduce the rank one case to the rank zero case, which is known thanks to the work of Skinner–Urban and Kato (see [SU14, Theorem 2]). In contrast to Theorem 1.4, it is not true that one can obtain arbitrary 2-Selmer rank *over* K. In fact, there is an obstruction for lowering the 2-Selmer rank over K from one to zero, as shown in [Li15]. Thus, this strategy would not naively work for $\ell = 2$ due to the aforementioned obstruction for rank lowering.

We now outline the strategy of the proofs. The level raising problem with prescribed U_p-eigenvalues can be thought of as the problem of constructing a modular lift ρ of the mod 2 representation $\overline{\rho} = \overline{\rho}_{E,2}$ with prescribed local types. For example, at a level raising prime p we wish to force the local Galois representation $\rho|_{G_{\mathbb{Q}_p}}$ to lie in the Steinberg or twisted Steinberg component (depending on the prescribed sign) of a local lifting ring. The usual technique to construct such lifts (e.g. as in [Gee11, BLGGT14]) is to write down a global deformation problem with prescribed local types, and then show that the deformation ring R has modular points. This is achieved by showing that R has positive Krull dimension, while at the same time being a finite $\mathbb{Z}_2$-algebra. The first fact is usually established by a Galois cohomology computation, whereas the second fact follows from a suitable modularity lifting theorem. In our situation, the Galois cohomology computation only shows that $\dim R \geqslant 0$, while the image of $\overline{\rho}$ being dihedral causes trouble in applying modularity lifting theorems at $\ell = 2$. When $\overline{\rho}$ is ordinary at 2, the modularity lifting theorem of Allen [All14] supplies the second ingredient (Theorem 4.2). While the Krull dimension estimate fails, it is possible to salvage it by looking at a slightly different deformation problem, for which we prescribe the local types at all but one auxiliary prime, where we do not prescribe anything (Theorem 4.1). This allows us to construct (still in the ordinary case) the desired level raising form, except that it might be ramified at our auxiliary prime. However, with a well-chosen auxiliary prime, it turns out that the form thus constructed is either unramified or its quadratic twist is unramified (Corollary 3.6). Twisting back allows us to get rid of this auxiliary prime at the cost of not prescribing the U_p-eigenvalue at one prime $p \| N$. This establishes Theorem 1.1 in the ordinary case. This part of the argument generalizes well to totally real fields.

In the non-ordinary case, we do not have sufficiently strong modularity lifting theorems to make the above argument work. However, it turns out that one can adapt the arguments of [DT94b] in this case. In the definite case, the level raising result (Lemma 5.4) is known to experts (e.g. Kisin [Kis09]). In the indefinite case, the crucial point is that while Fontaine–Laffaille theory breaks down at $\ell = 2$, there is a version of it that works for unipotent objects (Lemma 5.6). This produces a level raising form (Proposition 5.9), but with no control on the U_p-eigenvalues. One then shows that the existence of one such level raising form implies the existence of others, where we can change the U_p-eigenvalue. To make this work, we need to work with Shimura varieties at neat level, and thus we can only manipulate the signs at the cost of allowing ramification at an auxiliary prime. The same method in the previous paragraph will allow us to get rid of this auxiliary prime.

The proof of the main theorem (Theorem 1.4) consists of two parts: rank lowering (Theorem 7.7) and rank raising (Theorem 8.9). In each case, we proceed by induction on the number of level raising primes. When raising the level by one prime q, we can keep all the local conditions the same except at q (Lemma 6.6). We then use a parity argument inspired by Gross and Parson [GP12] to lower or raise the Selmer rank by one (Lemmas 7.1 and 8.5). A Chebotarev

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

density argument in fact shows that a positive density set of primes q would work at each step (Propositions 7.6 and 8.8).

Implementing the parity argument encounters several complications for $\ell = 2$.

(1) The mod 2 Galois representation $\overline{\rho} = \overline{\rho}_{E,2}$ has small image ($\cong S_3$ under Assumption 2.1) and Frob_q is either trivial or of order 2 for a level raising prime q. Thus, it is not possible to choose Frob_q with distinct eigenvalues as in [GP12]. Nevertheless, we can make use of the order 2 Frob_q to pin down the local condition at q when the sign at q is $+1$ (Lemma 6.6(3)). Since the signs are not detected in the mod 2 congruence, it is crucial to have prescribed signs when raising the level, which is guaranteed by Theorem 1.1.

(2) Since a finite group scheme over $\mathbb{Q}_2$ killed by 2 does not have a unique finite flat model over $\mathbb{Z}_2$ (unlike the case $\ell > 2$), there is an extra uncertainty for the local condition at 2 even when E has good reduction at 2. This uncertainty goes away when imposing Assumption 2.1(4) by Lemma 6.6(4). This same assumption is also needed for proving the level raising theorem (Theorem 1.1) (see Remark 2.5).

(3) In characteristic 2, it is crucial to work with not only the local Tate pairing but also a quadratic form giving rise to it (Remark 8.4). We utilize the quadratic form constructed by Zarhin [Zar74, § 2] using Mumford's Heisenberg group. Its properties were studied in O'Neil [O'Ne02] and Poonen and Rains [PR12] and we provide an explicit formula for it in the proof of Lemma 8.6.

The paper is organized as follows: § 2 contains definitions and examples on level raising. Section 3 discusses the auxiliary primes needed for level raising. Sections 4 and 5 prove the level raising theorem. Section 6 contains basic facts about Selmer groups. Sections 7 and 8 prove Theorem 1.4.

2. Main definitions and examples

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let $\overline{\rho} = \overline{\rho}_{E,2} : G_{\mathbb{Q}} \to \mathrm{Aut}\,(E[2]) \cong \mathrm{GL}_2(\mathbb{F}_2)$ be the Galois representation on the 2-torsion points. By the modularity theorem, $\overline{\rho}$ comes from a weight 2 cusp newform of level N. We make the following mild assumptions.

Assumption 2.1.

(1) E has good or multiplicative reduction at 2 (i.e. $4 \nmid N$).
(2) $\overline{\rho}$ is surjective and not induced from $\mathbb{Q}(i)$.
(3) The Serre conductor $N(\overline{\rho})$ is equal to the odd part of N. If $2 \mid N$, $\overline{\rho}$ is ramified at 2.
(4) If $2 \nmid N$, $\overline{\rho}|_{G_{\mathbb{Q}_2}}$ is non-trivial.
(5) E has negative discriminant Δ.

Remark 2.2. Assumption (2) that $\overline{\rho}$ is surjective implies that the 2-torsion field $L = \mathbb{Q}(E[2])$ is a $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$-extension over $\mathbb{Q}$ and $\mathrm{Gal}\,(L/\mathbb{Q}) \cong S_3$ acts on $E[2]$ via the 2-dimensional irreducible representation. The unique quadratic subextension of L is $\mathbb{Q}(\sqrt{\Delta})$ (see [Ser72, p. 305]).

Remark 2.3. When $\overline{\rho}$ is induced from $\mathbb{Q}(i)$, a variant of Theorem 1.1 holds where we cannot control the ramification at one chosen $p|N$. Nevertheless, the proof of Theorem 1.4 still goes through in this case because the local condition at p would be trivial.

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

Remark 2.4. All the level raised forms will be automatically new at $p \mid N$ due to Assumption (3). This assumption is also equivalent to saying that the component group of the Neron model of E at any $p \mid N$ has odd order (see [GP12, Lemma 4]).

Remark 2.5. Notice that $\bar{\rho}|_{G_{\mathbb{Q}_2}}$ is trivial if and only if 2 splits in L, if and only if E is ordinary at 2 and 2 splits in the quadratic subfield $\mathbb{Q}(\sqrt{\Delta}) \subseteq L$. Assumption (4) is only needed for the proof of Lemma 6.6(4) and for fulfilling the last assumption of Theorem 4.2. See Remarks 6.7 and 7.3.

Remark 2.6. Assumption (5) that $\Delta < 0$ implies that the complex conjugation acts non-trivially on $E[2]$. Assumption (5) is needed for the proof of Theorem 1.4 (used in Lemma 6.6(2) and 8.7) but not for Theorem 1.1 (see Theorem 2.9 and Remark 3.3).

Under these assumptions, $E[2]$ (as a $G_{\mathbb{Q}}$-module) together with the knowledge of reduction type at a prime q pins down the local condition defining $\mathrm{Sel}_2(E/\mathbb{Q})$ at q (see Lemma 6.6 for more precise statements). We would like to keep $E[2]$, but at a prime $q \nmid 2N$ of choice, to switch good reduction to multiplicative reduction and thus change the local condition at q. For this to happen, a necessary condition is that $\bar{\rho}(\mathrm{Frob}_q) = \left(\begin{smallmatrix} q & * \\ 0 & 1 \end{smallmatrix}\right) \pmod 2$ (up to conjugation). Namely, $\bar{\rho}(\mathrm{Frob}_q) = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ (order 1 or 2 in S_3).

Definition 2.7. We call $q \nmid 2N$ a *level raising prime* for E if Frob_q is of order 1 or 2 acting on $E[2]$. Notice that there are lots of level raising primes: by the Chebotarev density theorem, they make up 2/3 of all primes. If we write $f = \sum_{n \geqslant 1} a_n q^n \in S_2(N)$ (normalized so that $a_1 = 1$) to be the newform associated to the elliptic curve E, then by definition $q \nmid 2N$ is a level raising prime for E if and only if a_q is even.

The level raising theorem of Ribet ensures that this necessary condition is also sufficient.

Theorem 2.8 [Rib90, Theorem 1]. *Assume that $2 \nmid N$, $\bar{\rho}$ is surjective and $N(\bar{\rho}) = N$. Let $q \nmid 2N$ be a level raising prime. Then $\bar{\rho}$ comes from a weight 2 newform of level Nq.*

So, whenever q is a level raising prime, there exists a newform $g = \sum_{n \geqslant 1} b_n q^n \in S_2(Nq)$ of level Nq such that

$$g \equiv f \pmod 2.$$

More precisely, there exists a prime $\lambda \mid 2$ of the (totally real) Hecke field $F = \mathbb{Q}(\{b_n\}_{n \geqslant 1})$ such that we have a congruence $b_p \equiv a_p \pmod \lambda$ for any $p \neq q$.

In the next two sections, we will prove the following theorem generalizing Theorem 2.8.

Theorem 2.9. *Let $E/\mathbb{Q}$ be an elliptic curve satisfying (1)–(4) of Assumption 2.1. Let*

$$f = \sum_{n \geqslant 1} a_n q^n \in S_2(N)$$

be the newform associated to E. Let $q_1, \ldots, q_m$ be distinct level raising primes for E. Given any prescribed signs $\varepsilon_1, \ldots, \varepsilon_m \in \{\pm 1\}$ and $\epsilon_p \in \{\pm 1\}$ for $p \| N$, there exist a newform

$$g = \sum_{n \geqslant 1} b_n q^n \in S_2(N \cdot q_1 \cdots q_m)$$

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

and a prime λ *of the Hecke field* $F = \mathbb{Q}(\{b_n\}_{n\geqslant 1})$ *above* 2 *such that*

$$b_p \equiv a_p \pmod{\lambda}, \quad p \nmid N \cdot q_1 \cdots q_m; \quad b_{q_i} = \varepsilon_i, \quad i = 1, \dots, m,$$

and

$$b_p = \epsilon_p \quad \text{for all but possibly one chosen } p \| N.$$

Moreover, if either of the following two assumptions holds:

(1) *there exists* $p|N$ *such that* $\operatorname{ord}_p(N) > 1$ *and* $\operatorname{ord}_p(\Delta)$ *is odd; or*
(2) E *has discriminant* $\Delta > 0$,

then one can further require that

$$b_p = \epsilon_p \quad \text{for all } \ p \| N.$$

Remark 2.10. Our proof of this level raising theorem is divided into two parts according to whether E is good ordinary or multiplicative at 2 (which we call the *ordinary* case) or E is good supersingular at 2 (which we call the *supersingular* case). The proof in the ordinary case indeed only relies on the fact that $\bar{\rho}|_{G_{\mathbb{Q}_2}}$ is reducible.

This level raised newform g, via Eichler–Shimura construction, determines an abelian variety A over $\mathbb{Q}$ up to isogeny, of dimension $[F : \mathbb{Q}]$, with real multiplication by F. We will choose an A in this isogeny class so that A admits an action by the maximal order $\mathcal{O}_F$. By Assumption 2.1(2), A is unique up to a prime-to-λ isogeny. By construction, for almost all primes p, Frob_p has the same characteristic polynomials on $E[2] \otimes k$ and $A[\lambda]$. Hence, by Chebotarev's density theorem and the Brauer–Nesbitt theorem, we have

$$E[2] \otimes k \cong A[\lambda]$$

as $G_{\mathbb{Q}}$-representations.

DEFINITION 2.11. We say that A is obtained from E *via level raising* at $q_1, \dots, q_m$ and that A and E are *congruent mod 2*. We denote the *sign of* A at q_i by $\varepsilon_i(A) = \varepsilon_i$.

Remark 2.12. We make the following convention: E itself is understood as obtained from E via level raising at $m = 0$ primes. This is convenient for the induction argument later.

Example 2.13. Consider the elliptic curve $E = X_0(11) : y^2+y = x^3-x^2-10x-20$ with Cremona's label $11a1$. We list the first few Hecke eigenvalues of the modular form f associated to its isogeny class $11a$ in Table 1. We see that $q = 7$ is a level raising prime (so are $q = 13, 17, 19$). The space of newforms of level 77 has dimension 5, which corresponds to three isogeny classes of elliptic curves $(77a, 77b, 77c)$ and one isogeny class of abelian surfaces $(77d)$. Among them $(77a, 77b)$ are congruent to E mod 2: i.e. obtained from E via level raising at 7. Their first few Hecke eigenvalues are listed in Table 1. Notice that both signs $\pm$ occur at 7 via level raising, but only the sign $-$ occurs at 11.

Example 2.14. We list all the possible signs in level raising families obtained from $E = X_0(11)$ in Table 2 at $(q_i) = (7), (13), (17), (7, 13), (7, 19)$. We have also included the dimension of the level raised abelian variety A in the table. Notice that any prescribed signs at q_i can occur as predicted by Theorem 2.9. But only one sign occurs at 11 for $(q_i) = (7), (13), (7, 13), (7, 19)$,

Example 2.15. Table 3 illustrates possible signs obtained from $E = 35a1 : y^2+y = x^3+x^2+9x+1$ via level raising at $q = 19, 23, 31$. All possible eight combinations of signs occur for $q = 31$. For $q = 19$, 23, only the combinations $(+, +)$ and $(-, -)$ occur as the signs at $(5, 7)$. But all four combinations at $(5, q)$ or $(7, q)$ occur, as predicted by Theorem 2.9.

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

Table 1. Level raising at 7.

	2	3	5	7	11	13	17	19
$11a$	-2	-1	1	-2	1	4	-2	0
$77a$	0	-3	-1	-1	-1	-4	2	-6
$77b$	0	1	3	1	-1	-4	-6	2

Table 2. $E = 11a1$.

	11	7	13	17	dim A		11	7	13	dim A
$11a$	+				1	$1001a$	+	−	−	1
$77a$	−	−			1	$1001j$	+	−	+	5
$77b$	−	+			1	$1001k$	+	+	−	5
$143a$	−		−		1	$1001n$	+	+	+	11
$143c$	−		+		6		11	7	19	
$187a$	+			−	1	$1463c$	+	−	+	7
$187c$	+			+	2	$1463e$	+	+	−	9
$187d$	+			−	2	$1463g$	+	+	+	15
$187e$	−			−	3	$1463i$	+	−	−	16
$187f$	−			+	4					

Table 3. $E = 35a1$.

	5	7	19	dim A		5	7	31	dim A
$665a$	+	+	−	1	$1085a$	+	−	+	1
$665b$	+	+	+	1	$1085f$	+	−	−	1
$665h$	−	−	+	4	$1085g$	+	−	+	1
$665i$	−	−	−	6	$1085h$	+	−	−	1
	5	7	23		$1085k$	−	+	+	3
$805c$	−	−	−	1	$1085l$	+	−	+	3
$805d$	−	−	+	1	$1085m$	+	−	−	4
$805g$	+	+	−	4	$1085n$	+	+	−	4
$805m$	+	+	+	8	$1085o$	−	−	+	7
					$1085p$	−	+	−	7
					$1085q$	−	−	−	8
					$1085r$	+	+	+	11

3. Auxiliary primes

In the next three sections, the elliptic curve E is assumed to satisfy (1)–(4) of Assumption 2.1. Recall that $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_2)$ is the mod 2 Galois representation of E and $q_1, \ldots, q_m$ are distinct level raising primes for E.

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

DEFINITION 3.1. A prime $q_0 \nmid Nq_1 \cdots q_m$ is called an *auxiliary* prime for $\overline{\rho}$ if:

(1) $q_0 \equiv 3 \bmod 4$;
(2) $\overline{\rho}(\mathrm{Frob}_{q_0})$ has order 3;
(3) the Legendre symbol $(p/q_0) = 1$ for all $p | Nq_1 \cdots q_m$ except one chosen prime $p = p_1$ such that ord $_{p_1}(N)$ is odd.

LEMMA 3.2. *The set of auxiliary primes q_0 has positive density in the set of all primes.*

Proof. Observe that the first and last conditions are equivalent to demanding that Frob_{q_0} decomposes in a particular way in the extension

$$M = \mathbb{Q}(\sqrt{-1}, \sqrt{p_2}, \ldots, \sqrt{p_s}, \sqrt{q_1}, \ldots, \sqrt{q_m})/\mathbb{Q},$$

where p_i are prime factors of N. On the other hand, the second condition demands that Frob_{q_0} has order 3 in $S_3 = \mathrm{Gal}\,(\mathbb{Q}(E[2])/\mathbb{Q})$. Since $K = \mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{Q}(E[2])$ is the unique even degree subextension (Remark 2.2), it follows that $\mathbb{Q}(E[2])/\mathbb{Q}$ and $M/\mathbb{Q}$ are linearly disjoint Galois extensions (by Assumption 2.1(2) that $K \neq \mathbb{Q}(\sqrt{-1})$). The Chebotarev density theorem thus implies the lemma. □

Remark 3.3. Note also that when $\Delta > 0$, it is possible to get the third item also at $p = p_1$. This is because in this case $\mathbb{Q}(E[2]) \cap \mathbb{Q}(\sqrt{-1}, \sqrt{p_1}, \ldots, \sqrt{p_s}, \sqrt{q_1}, \ldots, \sqrt{q_m}) = \mathbb{Q}(\sqrt{|\Delta|}) = \mathbb{Q}(\sqrt{\Delta})$, and the second and third requirements of q_0 give the same requirement on the splitting behavior of Frob_{q_0} in $\mathbb{Q}(\sqrt{\Delta})$.

The following lemma imposes a strong restriction on the lifts of $\overline{\rho}|_{G_{\mathbb{Q}_{q_0}}}$ to characteristic 0.

LEMMA 3.4. *Let $\mathcal{O}$ be a sufficiently large finite extension of $\mathbb{Z}_2$ with residue field $\mathbb{F}$. Let K be a finite extension of $\mathbb{Q}_p$ with $p \neq 2$, whose residue field k has order $q \equiv 3$ mod 4. Let $\overline{r} : G_K \to \mathrm{GL}_2(\mathbb{F})$ be an unramified representation with $\det \overline{r}$ trivial and $\overline{r}(\mathrm{Frob}_K)$ has distinct eigenvalues in $\mathbb{F}$. Suppose that $r : G_K \to \mathrm{GL}_2(\mathcal{O})$ lifts $\overline{r}$ with cyclotomic determinant. Then $r|_{I_K} \otimes \eta$ is unramified, where $\eta : I_K \to \mathcal{O}^\times$ is a quadratic character.*

Proof. Let $P_K \subset I_K$ be the wild inertia group of K, and choose a tame generator $I_K/P_K = \langle \tau \rangle$. Let $\mathfrak{m}$ denote the maximal ideal of $\mathcal{O}$. Let σ be a choice of Frobenius of K. Because $\overline{r}$ is unramified, $r(P_K) = 1$, and r is determined by the two matrices $r(\sigma)$, $r(\tau)$, which are subject to the relations

$$\begin{aligned} r(\sigma)r(\tau)r(\sigma)^{-1} &= r(\tau)^q, \\ \det r(\tau) &= 1, \\ \det r(\sigma) &= q^{-1}. \end{aligned}$$

Without loss of generality, we may assume that $r(\sigma) = \left(\begin{smallmatrix} \alpha & 0 \\ 0 & \beta \end{smallmatrix}\right)$ with $\bar{\alpha} \neq \bar{\beta}$. Writing $r(\tau) = 1 + \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $a, b, c, d \in \mathfrak{m}$, we obtain

$$1 + \begin{pmatrix} a & \alpha\beta^{-1}b \\ \alpha^{-1}\beta c & d \end{pmatrix} = \left(1 + \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)^q.$$

Expanding gives

$$\begin{pmatrix} (1-q)a & (\alpha\beta^{-1} - q)b \\ (\alpha^{-1}\beta - q)c & (1-q)d \end{pmatrix} = \binom{q}{2} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 + \cdots + \begin{pmatrix} a & b \\ c & d \end{pmatrix}^q.$$

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

Suppose that we know that $b, c \in \mathfrak{m}^k$ for some $k \geqslant 1$. Then comparing terms in the above equation we obtain $(\alpha\beta^{-1} - q)b \in \mathfrak{m}^{k+1}$, $(\alpha^{-1}\beta - q)c \in \mathfrak{m}^{k+1}$. Because $\alpha\beta^{-1} - q, \alpha^{-1}\beta - q$ are units (since $\bar{\alpha} \neq \bar{\beta}$), we have $b, c \in \mathfrak{m}^{k+1}$. Continuing inductively, we get $b, c \in \cap \mathfrak{m}^k = 0$. Thus, $r(\tau)$ must be diagonal, and must furthermore satisfy

$$\begin{aligned}(1+a)^q &= (1+a),\\ (1+d)^q &= (1+d),\\ (1+a)(1+d) &= 1.\end{aligned}$$

Thus, the image $r(I_K)$ is a subgroup of μ_{q-1}. On the other hand, because $\overline{r}(I_K) = 1$, $r(I_K)$ is a pro-2 group and, since $q \equiv 3 \bmod 4$, we must have $r(I_K) \subset \mu_2$. □

Remark 3.5. If we do not impose the condition that the determinant of the lift is the cyclotomic character (or just unramified), the same computation as above shows that the determinant of the lift restricted to I_K is the unique non-trivial quadratic character.

Corollary 3.6. *If g is an eigenform with corresponding automorphic representation $\pi = \otimes\pi_p$ such that its mod 2 representation $\overline{\rho}_g \cong \overline{\rho}$ and q_0 is an auxiliary prime, then either π_g is unramified at q_0 or $\pi_q \otimes \chi_{q_0}$ is unramified, where χ_{q_0} is the unique quadratic character which is ramified at q_0 and unramified everywhere else.*

Remark 3.7. The role of the auxiliary prime is to resolve the following tension: on the one hand, the space of automorphic forms that we need to investigate behaves well only when the level subgroup U is 'sufficiently small'; on the other hand, we want to construct automorphic forms with prescribed local behavior at *all* primes. If the residual characteristic $\ell > 2$ and a suitable largeness condition on the image of $\overline{\rho}$ holds, this problem can be resolved by allowing extra ramification at an auxiliary prime with the property that any automorphic form congruent to $\overline{\rho}$ will automatically be unramified at the auxiliary prime (this is what is done in [DT94b], for example). In the situation we are interested in, it is not possible to find auxiliary primes that achieve this; however, Corollary 3.6 shows that we can ensure that automorphic forms lifting $\overline{\rho}$ will have at most quadratic ramification at the auxiliary primes. This turned out to be sufficient for our purposes, by making a quadratic twist to get rid of the extra ramification.

4. Simultaneous level raising: ordinary case

We fix a finite extension E of $\mathbb{Q}_2$ which is sufficiently large, with ring of integers $\mathcal{O}$ and residue field $\mathbb{F}$. Let π denote a uniformizer. Let $\mathfrak{Art}_{\mathcal{O}}$ be the category of Artinian local $\mathcal{O}$ algebras with residue field identified with $\mathbb{F}$ via the $\mathcal{O}$-algebra structure. Let F be a totally real field. We fix a finite set of places S of F, and a subset $\Sigma \subset S$ which contains all places $v|p$ and $v|\infty$. Let $\overline{\rho} : G_{F,S} \to \mathrm{GL}_2(\mathbb{F})$ be an absolutely irreducible representation, where $G_{F,S}$ is the Galois group of the maximal extension of F unramified outside the finite places in S. Denote by $V_{\mathbb{F}} = \mathbb{F}^2$ the $G_{F,S}$-module induced by $\overline{\rho}$ and $\beta_{\mathbb{F}}$ the standard basis of $V_{\mathbb{F}}$. Let $\psi : G_{F,S} \to \mathcal{O}^\times$ be a character lifting $\det \overline{\rho}$. If $v|2$, denote by $\Lambda(G_{F_v})$ the completed group algebra $\mathcal{O}[[G_{F_v}^{\mathrm{ab}}(2)]]$ of the maximal pro-2 quotient of $G_{F_v}^{\mathrm{ab}}$. It is a complete local Noetherian commutative ring with residue field $\mathbb{F}$, and we let $\mathfrak{Art}_{\Lambda(G_{F_v})}$ be the category of local Artinian $\Lambda(G_{F_v})$-algebras with residue field $\mathbb{F}$. Note that $\Lambda(G_{F_v})$ carries the universal character that is trivial modπ. Similarly, let $\Lambda'(G_{F_v})$ be the completed group algebra $\mathcal{O}[[I_{F_v}{}^{\mathrm{ab}}(2)]]$. It is a subalgebra of $\Lambda(G_{F_v})$, and the restriction of the aforementioned universal character to I_{F_v} takes values in this subalgebra.

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

For each place v of F, let D_v be the functor on $\mathfrak{Art}_{\mathcal{O}}$ that assigns to $(A, m_A) \in \mathfrak{Art}_{\mathcal{O}}$ the set of isomorphism classes of tuples (V_A, ι_A, β), where V_A is a finite free A module with G_{F_v} action, β a basis of V_A and $\iota_A : V_A/m_A \cong V_{\mathbb{F}}$ an isomorphism of G_{F_v}-modules such that $\iota_A(\beta) = \beta_{\mathbb{F}}$. This data is the same as a homomorphism $\rho_A : G_{F_v} \to \mathrm{GL}_2(A)$ lifting $\overline{\rho}|_{G_{F_v}}$. This functor is pro-representable by a complete local Noetherian $\mathcal{O}$-algebra $R_v^{\square}$. The subfunctor D_v^{ψ} consisting of lifts with determinant ψ is pro-represented by a quotient $R_v^{\psi,\square}$ of $R_v^{\square}$. A *deformation condition at* v is a relatively representable subfunctor $\overline{D}_v^{\psi} \subset D_v^{\psi}$ satisfying the dimension conditions in [Boe, 5.4]. The condition of being in $\overline{D}_v^{\psi}(A)$ is assumed to not depend on the choice of basis of V_A. When $v|2$, we also consider some other subfunctors of $D_v \widehat{\otimes}_{\mathcal{O}} \Lambda(G_{F_v})$ on $\mathfrak{Art}_{\Lambda(G_{F_v})}$ as in [All14, 1.4.3].

A *deformation problem* is the data of $(\overline{\rho}, F, \Sigma \subset S, (\overline{D}_v^{\psi})_{v\in\Sigma})$. Given such data, let $\overline{D}_{F,\Sigma,S}^{\psi,\square}$ be the functor which assigns to $(A, m_A) \in \mathfrak{Art}_{\mathcal{O}}$ the set of isomorphism classes of tuples $(V_A, \iota_A, (\beta_v)_{v\in\Sigma})$, where:

- V_A is a free A-module with $G_{F,S}$ action and $\iota_A : V_A/m_A \cong V_{\mathbb{F}}$ is an isomorphism of $G_{F,S}$-modules;
- β_v is a basis of V_A such that $\iota_A(\beta_v) = \beta_{\mathbb{F}}$;
- the lifting of $\overline{\rho}|_{G_{F_v}}$ determined by (V_A, ι_A, β_v) (viewed as a G_{F_v}-module by restriction) is in $\overline{D}_v^{\psi}(A) \subset D_v(A)$;
- the determinant of V_A is given by ψ.

The functor $\overline{D}_{F,\Sigma,S}^{\psi,\square}$ is pro-representable and we denote by $\overline{R}_{F,\Sigma,S}^{\psi,\square}$ the corresponding deformation ring. We define the functor $\overline{D}_{F,\Sigma,S}^{\psi}$ in exactly the same way as $\overline{D}_{F,\Sigma,S}^{\psi,\square}$, except that we do not add the data of (β_v). Because $\overline{\rho}$ is absolutely irreducible, the functor $\overline{D}_{F,\Sigma,S}^{\psi}$ is pro-representable and we denote by $\overline{R}_{F,\Sigma,S}^{\psi}$ the corresponding deformation ring.

The E-points of $\operatorname{Spec} \overline{R}_{F,\Sigma,S}^{\psi}$ are precisely the set of deformations ρ of $\overline{\rho}$ to $\mathcal{O}$ with determinant ψ such that for each $v \in \Sigma$, $\rho_{G_{F_v}}$ satisfies the deformation condition $\overline{D}_v^{\psi}$. The problem of simultaneous level raising will be reduced to showing that this set is non-empty for suitable deformation conditions.

Let $\delta = \dim_{\mathbb{F}} \operatorname{Ker}(H^0(G_{F,S}, (\mathrm{ad}^0\overline{\rho})^*) \to \bigoplus_{v\in S\setminus\Sigma} H^0(G_{F_v}, (\mathrm{ad}^0\overline{\rho})^*))$, where the superscript $*$ means Pontryagin dual. Note that $\delta = 0$ if $S\setminus\Sigma \neq \emptyset$. We have the following estimate [Boe, Theorem 5.4.1].

Theorem 4.1. *If* $\delta = 0$, *then* $\dim \overline{R}_{F,\Sigma,S}^{\psi} \geqslant 1$.

Let us now assume that our deformation problem is of the following form.

– For $v|\infty$: we let $\overline{D}_v^{\psi}$ be the subfunctor represented by the quotient of $R_v^{\square}$ which is cut out by the equation $\det(\rho(c_v) - X) = X^2 - 1$, where c_v is the complex conjugation. That is, we look at odd deformations.

– For $v|2$: assume that $\overline{\rho}$ has a G_{F_v}-stable line L such that G_{F_v} acts on $V_{\mathbb{F}}/L$ via a character $\overline{\chi}$, and that ψ is a ramified character. Then there is a unique $\mathcal{O}$-flat quotient $\tilde{R}_v^{\psi,\square}$ of $R_v^{\square}$ such that for any finite extension E' of E, an E'-point x of $\operatorname{Spec} R_v^{\square}$ with corresponding representation ρ_x factors through this quotient if and only if $\det \rho_x = \psi$, and ρ_x has a Galois-stable line $L \subset V_x$ such that the Galois action on V_x/L is unramified. In the notation of [All14, 1.4.3], this is (the $\mathcal{O}$-flat quotient with the same generic fiber of) $R_{\Lambda(G_{F_v})}^{\Delta,\psi} \otimes_{\Lambda'(G_{F_v})} \mathcal{O}$, where the homomorphism

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

$\Lambda'(G_{F_v}) \to \mathcal{O}$ is the specialization homomorphism from the character $I_{F_v} \to \Lambda'(G_{F_v})^\times$ to the trivial character. Note that, a priori, $R^{\Delta,\psi}_{\Lambda(G_{F_v})} \otimes_{\Lambda'(G_{F_v})} \mathcal{O}$ need not be a quotient of $R^{\square}_v$, because it keeps track of the character Galois acts on the line L. However, with the assumption that ψ is ramified, the line L is uniquely determined by the deformation and hence it is in fact a quotient of $R^{\square}_v$. We let $\overline{D}^{\psi}_v$ be the subfunctor represented by an $\mathcal{O}$-torsion free quotient of $R^{\square}_v$ corresponding to an irreducible component of $\tilde{R}^{\psi,\square}_v[\frac{1}{2}]$, and let $\overline{D}^{\mathrm{big},\psi}_v$ be the functor represented by the quotient $R^{\Delta,\psi}_{\Lambda(G_{F_v})}$ of $R^{\psi,\square}_v \widehat{\otimes}_{\mathcal{O}} \Lambda(G_{F_v})$ in the category $\mathfrak{Art}_{\Lambda(G_{F_v})}$. When $\psi = \psi_2$ is the cyclotomic character, the generic fiber of $\tilde{R}^{\psi,\square}_v$ consists of the following three types of irreducible components: components whose generic E'-point gives rise to an extension of the trivial character by ψ_2, a quadratic unramified twist of an extension of the trivial character by ψ_2 or a crystalline ordinary representation. There is at most one component of the first two types, and possibly more than one component of the third type. This fact, and the fact that $\tilde{R}^{\psi,\square}_v$ satisfy the dimension requirement of [Boe, 5.4], follow from the arguments in [Kis09, 2.4] and [Sno11, 4.1–4.3].

– For $v \in \Sigma$, $v \nmid 2$: let $R^{\psi,\square}_v$ be the ring pro-representing the subfunctor of D_v classifying lifts of fixed determinant ψ. It is known (see [Boe, 3], [Pil]) that $R^{\psi,\square}_v[\frac{1}{2}]$ is equidimensional of dimension 3, with smooth irreducible components. The deformation conditions we take are those given by a choice of (union of) irreducible components, that is the subfunctor represented by the unique $\mathcal{O}$-torsion free quotient of $R^{\psi,\square}_v$ whose generic fiber is the chosen (union of) components. On each irreducible component, the inertial Weil–Deligne type is constant. Either there is no irreducible component whose inertial Weil–Deligne type is $(1 \oplus 1, N \neq 0)$, or there are exactly two of them, which differ by an unramified quadratic twist. In the case where these components correspond to the Steinberg representation and its unramified quadratic twist, we call them the *Steinberg component* and the *twisted Steinberg component*.

If F' is a totally real finite extension such that $\overline{\rho}|_{G_{F'}}$ is still absolutely irreducible, one can consider the 'base change' deformation problem by replacing S, Σ with the set S', Σ' of primes in F' above them, and restricting the inertial Weil–Deligne types. If we denote by $\overline{R}^{\psi}_{F',\Sigma',S'}$ the corresponding deformation ring, the argument in [BLGGT14, Lemma 1.2.3] shows that $\overline{R}^{\psi}_{F,\Sigma,S}$ is a finite $\overline{R}^{\psi}_{F',\Sigma',S'}$-algebra.

Theorem 4.2. *Let $(\overline{\rho}, F, \Sigma \subset S, (\overline{D}^{\psi}_v)_{v\in\Sigma})$ be a deformation problem as above. Assume that:*

– *$\psi\psi_2^{-1}$ is a finite order character, where ψ_2 is the 2-adic cyclotomic character;*
– *$S\backslash\Sigma \neq \emptyset$;*
– *for $v \in S\backslash\Sigma$, assume that no component of $R^{\psi,\square}_v$ has inertial Weil–Deligne type with $N \neq 0$;*
– *for $v \in \Sigma$, assume that $\overline{D}^{\psi}_v$ is given by one component of $R^{\psi,\square}_v[\frac{1}{2}]$ (or of $\tilde{R}^{\psi,\square}_v[\frac{1}{2}]$ when $v|2$);*
– *$\mathrm{Im}\,\overline{\rho}$ is dihedral, induced from a quadratic extension K/F;*
– *if K is imaginary CM, then there is a prime $v|2$ of F which does not split in K.*

Then $\overline{R}^{\psi}_{F,\Sigma,S}[\frac{1}{2}] \neq 0$. In particular, there is a deformation $\rho : G_{F,S} \to \mathrm{GL}_2(E')$ satisfying the deformation conditions of the deformation problem, with E' a finite extension of E. Furthermore, all such deformations are modular.

Proof. We indicate how to deduce this from the main result of [All14]. First we replace F by a solvable totally real extension F' as in the proof of [All14, Theorem 5.2.1]. This has the effect

of making the assumptions in § 4.4 there hold. Let us denote by $\overline{R}^{\mathrm{big},\psi}_{F',S'}$ the deformation ring defined as in [All14, p. 1316]. It is the deformation ring representing the deformation functor $\overline{D}^{\mathrm{big},\psi}_{F',S',S'}$, which is defined as the deformation problem in the category of local Artinian $\Lambda(G_{F'}) = \hat{\bigotimes}_{v|2}\Lambda(G_{F'_v})$-algebra such that the local deformation condition at $v|2$ is given by $\overline{D}^{\mathrm{big},\psi}_v$, and the local deformation conditions at the other places are given by the component that contains the image under the map of local lifting rings of the components in the definition of $\overline{R}^{\psi}_{F,\Sigma,S}$. By enlarging F' if needed, the local deformation conditions at the finite places in Σ' obtained in this way are either the unramified or an unramified twist of the Steinberg component, while the deformation conditions at the places in $S'\backslash\Sigma'$ become the unramified component. This shows that we are indeed in the setting of [All14]. Let $\Lambda'(G_{F'}) = \hat{\bigotimes}_{v|2}\Lambda'(G_{F'_v})$. There is a homomorphism $\phi : \Lambda'(G_{F'}) \to \mathcal{O}$ ('weight 2 specialization') such that there is a surjection $\overline{R}^{\mathrm{big},\psi}_{F',S'} \otimes_{\Lambda'(G_{F'}),\phi} \mathcal{O} \twoheadrightarrow \overline{R}^{\psi}_{F,\Sigma',S'}$.

Now, by [All14, Proposition 4.4.3], every prime of $\overline{R}^{\mathrm{big},\psi}_{F',S'}$ is pro-modular and hence $(\overline{R}^{\mathrm{big},\psi}_{F',S'})^{\mathrm{red}}$ is identified with a localized Hida Hecke algebra of F'. In particular, $(\overline{R}^{\mathrm{big},\psi}_{F',S'})^{\mathrm{red}}$ is a finite $\Lambda'(G_{F'})$-algebra. Because $\overline{R}^{\mathrm{big},\psi}_{F',S'}$ is Noetherian, $\overline{R}^{\mathrm{big},\psi}_{F',S'}$ is also a finite $\Lambda'(G_{F'})$-algebra. But this implies that $\overline{R}^{\psi}_{F',\Sigma',S'}$ is a finite $\mathcal{O}$-algebra and hence $\overline{R}^{\psi}_{F,\Sigma,S}$ is a finite $\mathcal{O}$-algebra. Because $\dim \overline{R}^{\psi}_{F,\Sigma,S} \geqslant 1$ by Theorem 4.1, this forces $\overline{R}^{\psi}_{F,\Sigma,S}[\frac{1}{2}] \neq 0$. The residue fields at each maximal ideal of this ring are finite extensions of E, whose points give rise to the desired characteristic 0 deformations ρ. Furthermore, the argument above shows that after restriction to F', any such ρ comes from the specialization at weight 2 of a Hida Hecke algebra and hence $\rho|_{G_{F'}}$ is modular. By solvable base change, ρ is also modular. □

We now apply this to prove Theorem 2.9 when E is ordinary at 2. We choose our deformation problem as follows.

– $\overline{\rho} = \overline{\rho}_{E,2} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_2)$ is the mod 2 representation of the elliptic curve E.

– $\psi = \psi_2$ is the 2-adic cyclotomic character.

– Σ consists of the finite primes dividing $Nq_1 \cdots q_m$ as well as ∞.

– For $p\|N$ and $p \neq 2$, the deformation condition $\overline{D}^{\psi}_p$ is given by the Steinberg component (respectively the twisted Steinberg component) if $\epsilon_p = +1$ (respectively $\epsilon_p = -1$).

– For $p^2|N$, the deformation condition $\overline{D}^{\psi}_p$ is given by the unique component of $R^{\psi,\square}_v[\frac{1}{2}]$ that contains $\rho_{E,2}|_{G_{\mathbb{Q}_p}}$.

– At $v|2\infty$, the deformation conditions are chosen to be $\overline{D}^{\psi}_v$ as below Theorem 4.1. Note that we are in the situation dealt there because E was assumed to be ordinary at 2. For $v|2$, we choose the crystalline ordinary component if E has good reduction at 2. If E has multiplicative reduction at 2, we choose the component that either contains $\rho_{E,2}|_{G_{\mathbb{Q}_2}}$ or contains its unramified quadratic twist depending on the chosen sign ϵ_2.

– At q_i, the deformation condition is given by either the Steinberg component or the twisted Steinberg component, depending on the sign of ε_i.

– $S = \Sigma \cup \{q_0\}$, where q_0 is an auxiliary prime as in Definition 3.1.

By Remark 2.5, we know that 2 does not split in $K = \mathbb{Q}(\sqrt{\Delta})$. This, together with Lemma 3.4, shows that the hypotheses of Theorem 4.2 hold. Thus, we get a modular deformation of $\overline{\rho}$ which

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

corresponds to a weight 2 newform $g = \sum b_n q^n$ (with associated automorphic representation $\pi = \bigotimes \pi_p$) such that:

- π has trivial central character;
- for $p|2N$, the conductor of π_p is equal to ord $_p(N)$. If $p\|N$, π_p is Steinberg or the unramified quadratic twist of Steinberg depending on $a_p = 1$ or -1: thus, $b_p = a_p$ for such p;
- for $i > 0$, π_{q_i} is Steinberg or the unramified quadratic twist of Steinberg depending on $\varepsilon_i = 1$ or -1. Thus, $b_{q_i} = \varepsilon_i$.

4.3 Proof of Theorem 2.9 in the ordinary case

By construction, $q_0 \equiv 3 \bmod 4$ and $\overline{\rho}(\mathrm{Frob}_{q_0})$ has order 3 (hence has distinct eigenvalues). Applying Corollary 3.6, it follows that our level raised form g is either unramified at q_0 or its twist $g \otimes \chi_{q_0}$ is unramified at q_0, where χ_{q_0} is the unique quadratic character that is ramified at q_0 and unramified everywhere else. In the former case, the form g satisfies the conclusion of Theorem 2.9. In the latter case, $g \otimes \chi_{q_0}$ has the desired conductor, so we only need to check the matching of the signs at primes p where the conductor is 1. But such a prime p satisfies either $p\|N$ or $p = q_i$ $(i > 0)$. Since twisting by χ_{q_0} changes the sign of ε at p to $\varepsilon\chi_{q_0}(\mathrm{Frob}_p) = \varepsilon(p/q_0) = \varepsilon$ if $p \neq p_1$, we see that $g \otimes \chi_{q_0}$ satisfies the conclusion of Theorem 2.9. This finishes the proof in the ordinary case.

5. Simultaneous level raising: supersingular case

Let D be a quaternion algebra over $\mathbb{Q}$. We denote by G_D the $\mathbb{Q}$-algebraic group $D^\times$, $Z \cong \mathbb{G}_m$ its center and $\Sigma(D)$ the set of primes where D is ramified. Assume that $2 \notin \Sigma(D)$. Let $\nu_D : G_D \to \mathbb{G}_m$ be the reduced norm map. Fix a maximal order $\mathcal{O}_D$ of D, and fix once and for all an isomorphism between $\mathcal{O}_D \otimes \mathbb{Z}_p \cong M_2(\mathbb{Z}_p)$ for each place $p \notin \Sigma(D)$. This determines an isomorphism $G_D(\mathbb{Q}_p) \cong \mathrm{GL}_2(\mathbb{Q}_p)$.

Given an open subgroup U of $G_D(\mathbb{A})$ of the form $\prod U_p$, such that the set S of primes such that $U_p \neq \mathrm{GL}_2(\mathbb{Z}_p)$ is finite, we have the abstract Hecke algebra $\mathbb{T} = \mathbb{Z}[\{T_p, S_p\}_{p \notin S}]$ (this depends on U through the set S, though this dependence is not in the notation). A maximal ideal $\mathfrak{m} \subset \mathbb{T}$ is called *Eisenstein* if there exists some positive integer d such that $T_p - 2 \in \mathfrak{m}$ for all but finitely many primes $p = 1 \bmod d$.

Let $\mathrm{Iw}_1(p^n)$ (respectively, $\mathrm{Iw}(p^n)$) be the subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$ consisting of matrices which are upper triangular unipotent (respectively, upper triangular) mod p^n. If $U = \prod U_p$ is an open subgroup, and p is a prime such that $U_p = \mathrm{GL}_2(\mathbb{Z}_p)$, we denote by $U_0(p)$ the open subgroup of U which agrees with U away from p, and $U_0(p)_p = \mathrm{Iw}(p) \subset U_p$.

5.1 Quaternionic forms: definite case

Throughout this section, we assume that D is definite. As in [All14], for each $\Sigma' \subset \Sigma(D)$, a $(\Sigma' \subset \Sigma(D))$-open subgroup $U \subset G_D(\mathbb{A}^\infty)$ is a subgroup of the form $U = \prod_p U_p$ such that:

- $U_p \subseteq \mathrm{GL}_2(\mathbb{Z}_p)$ for $v \notin \Sigma(D)$, via our chosen identification. Equality holds for almost all p;
- $U_p = G_D(\mathbb{Q}_p) = D_p^\times$ for $p \in \Sigma'$;
- $U_p = (\mathcal{O}_D \otimes \mathbb{Z}_p)^\times$ for $p \in \Sigma(D) \backslash \Sigma'$.

Note that an $(\emptyset \subset \Sigma(D))$-open subgroup is an open compact subgroup.

Let $\gamma = (\gamma_p)_{p \in \Sigma'}$ be a tuple of unramified characters $\gamma_p : \mathbb{Q}_p^\times \to \mu_2$. This determines a character of $\gamma : G_D(\mathbb{A}^\infty) \to \mu_2$ given by composing the projection to $\prod_{p \in \Sigma'} G_D(\mathbb{Q}_p)$ and

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

$\prod_{p\in\Sigma'}\gamma_p\circ\nu_D$. If A is a topological $\mathbb{Z}_2$-module, define $S_\gamma(U,A)$ to be the space of functions

$$f : G_D(\mathbb{Q})\backslash G_D(\mathbb{A}^\infty)/UZ(\mathbb{A}^\infty)\to A$$

such that $f(gu)=\gamma(u)f(g)$. Because D is definite, there exist $t_1,\dots,t_n\in G_D(\mathbb{A}^\infty)$ such that $G_D(\mathbb{Q})\backslash G_D(\mathbb{A}^\infty)/UZ(\mathbb{A}^\infty)=\coprod G_D(\mathbb{Q})t_iUZ(\mathbb{A}^\infty)$, and this gives the identification

$$S_\gamma(U,A)\cong\bigoplus_{i=1}^{n}A^{\gamma((UZ(\mathbb{A}^\infty)\cap t_i^{-1}G_D(\mathbb{Q})t_i)/Z(\mathbb{Q}))}.$$

Here we view A as a μ_2-module via its $\mathbb{Z}_2$-module structure, and the superscript means taking invariants. In particular, if $(UZ(\mathbb{A}^\infty)\cap t_i^{-1}G_D(\mathbb{Q})t_i)/Z(\mathbb{Q})=1$ (or if γ is trivial), then $S_\gamma(U,A)=S_\gamma(U,\mathbb{Z}_2)\otimes_{\mathbb{Z}_2}A$. Without any assumption on U, this holds if A is $\mathbb{Z}_2$-flat.

Lemma 5.2. *Fix a prime $p\notin\Sigma(D)$. Let U be a $(\Sigma'\subset\Sigma(D))$-open subgroup. If $U_p\subset\mathrm{Iw}_1(p^n)$ for n large enough (depending only on p), then $UZ((\mathbb{A}^\infty)\cap t^{-1}G_D(\mathbb{Q})t)/Z(\mathbb{Q})=1$ for any $t\in G_D(\mathbb{A}^\infty)$.*

Proof. This is [All14, Lemma 2.1.5]. □

Definition 5.3. We call a subgroup U satisfying the conclusion of the lemma *sufficiently small*.

Let S be the set of primes such that $U_p\neq\mathrm{GL}_2(\mathbb{Z}_p)$. The abstract Hecke algebra $\mathbb{T}=\mathbb{Z}[\{T_p,S_p\}_{p\notin S}]$ acts on $S_\gamma(U,A)$ through the usual double coset operators T_p, S_p. Denote by $\mathbb{T}(\gamma,U,A)$ the quotient of $\mathbb{T}$ that acts faithfully on $S_\gamma(U,A)$. The subspace $S_\gamma(U,A)^{\mathrm{triv}}$ consisting of functions that factor through ν_D is stable under $\mathbb{T}$. Fix an embedding $\mathbb{Q}_2\hookrightarrow\mathbb{C}$. The Jacquet–Langlands correspondence gives a $\mathbb{T}$-equivariant isomorphism

$$(S_\gamma(U,\mathbb{Z}_2)/S_\gamma(U,\mathbb{Z}_2)^{\mathrm{triv}})\otimes_{\mathbb{Z}_2}\mathbb{C}\cong\bigoplus\pi^V.$$

Here $V\subseteq\mathrm{GL}_2(\mathbb{A}^\infty)$ is the open compact subgroup such that $V_p=U_p$ if $p\notin\Sigma(D)$, and $V_p=\mathrm{Iw}(p)$ if $p\in\Sigma(D)$. The sum runs over π such that:

– π is an algebraic automorphic representation of $\mathrm{GL}_2(\mathbb{A})$ such that π_∞ is a discrete series with trivial infinitesimal character (i.e. π corresponds to a modular form of weight 2) and trivial central character;

– for $p\in\Sigma(D)$, the local representation π_p is an unramified twist of the Steinberg representation St. If $p\in\Sigma'$, then $\pi_p\cong\gamma_p\otimes\mathrm{St}$.

It follows that $\mathbb{T}(\gamma,U,\mathbb{Z}_2)\otimes\overline{\mathbb{Q}}_2$ is a product of fields, and each homomorphism

$$\mathbb{T}\twoheadrightarrow\mathbb{T}(\gamma,U,\mathbb{Z}_2)\to\overline{\mathbb{Z}}_2$$

corresponds to the system of Hecke eigenvalues of a modular form of weight 2 whose automorphic representation satisfies the above condition. We say that such a system of Hecke eigenvalues *occurs in* $S_\gamma(U,\overline{\mathbb{Z}}_2)$. Given a maximal ideal $\mathfrak{m}$ of $\mathbb{T}$ corresponding to a homomorphism $\overline{\theta}:\mathbb{T}\to\overline{\mathbb{F}}_2$, there exists a modular form g whose system of Hecke eigenvalues congruent to $\overline{\theta}$ is equivalent to $\mathfrak{m}$ being in the support of $S_\gamma(U,\overline{\mathbb{Z}}_2)/S_\gamma(U,\overline{\mathbb{Z}}_2)^{\mathrm{triv}}$ or, equivalently, $(S_\gamma(U,\overline{\mathbb{Z}}_2)/S_\gamma(U,\overline{\mathbb{Z}}_2)^{\mathrm{triv}})_{\mathfrak{m}}\neq 0$. If $\mathfrak{m}$ corresponds to the mod 2 reduction of a system of Hecke eigenvalues of a modular form, then $\mathfrak{m}$ is Eisenstein if and only if the associated mod 2 representation $\rho_{\mathfrak{m}}:G_{\mathbb{Q}}\to\mathrm{GL}_2(\mathbb{F}_2)$ is

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

reducible [DT94b, Proposition 2]. One knows that the Hecke action on $S_\gamma(U,\overline{\mathbb{Z}}_2)^{\mathrm{triv}}$ is Eisenstein and hence, if $\mathfrak{m}$ is non-Eisenstein, $(S_\gamma(U,\overline{\mathbb{Z}}_2)/S_\gamma(U,\overline{\mathbb{Z}}_2)^{\mathrm{triv}})_{\mathfrak{m}} \neq 0$ is equivalent to $S_\gamma(U,\overline{\mathbb{Z}}_2)_{\mathfrak{m}} \neq 0$.

Now suppose that U is a $(\Sigma' \subset \Sigma(D))$-open subgroup and p is a prime such that $U_p = \mathrm{GL}_2(\mathbb{Z}_p)$. Recall that $U_0(p)$ is the $(\Sigma' \subset \Sigma(D))$-open subgroup of U which agrees with U away from p, and $U_0(p)_p = \mathrm{Iw}(p) \subset U_p$. We say that a system of Hecke eigenvalues in $\overline{\mathbb{Z}}_2$ that occurs in $S_\gamma(U_0(p),\overline{\mathbb{Z}}_2)$ but not in $S_\gamma(U,\overline{\mathbb{Z}}_2)$ is *p-new*. Under the Jacquet–Langlands correspondence, it corresponds to an automorphic representation whose component at p is an unramified twist of the Steinberg representation.

We have the following level raising result.

Lemma 5.4. *Let U be an $(\emptyset \subset \Sigma(D))$-open subgroup that is sufficiently small, and $U_p = \mathrm{GL}_2(\mathbb{Z}_p)$. Suppose that $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}$ in the support of $S(U,\mathbb{Z}_2)$, and that $T_p \in \mathfrak{m}$. Then there exists a p-new system of Hecke eigenvalues lifting $\mathfrak{m}$.*

Proof. This is a reformulation of [Kis09, Lemma 3.3.3]. □

5.5 Quaternionic forms: indefinite case

Throughout this section, D is assumed to be indefinite and not split. Let $U \subset G_D(\mathbb{A}^\infty)$ be an open compact subgroup. The double coset space

$$G_D(\mathbb{Q})\backslash \mathbb{H}^{\pm} \times G_D(\mathbb{A}^\infty)/U$$

is naturally the complex points of an algebraic curve X_U, which is in fact defined over $\mathbb{Q}$.

Following [DT94b], for N not divisible by any prime of $\Sigma(D)$, let $V_1(N)$ denote the open compact subgroup such that:

- for $p \in \Sigma(D)$, $V_1(N)_p = (\mathcal{O}_D \otimes \mathbb{Z}_p)^\times$;
- for $p|N$, $V_1(N)_p \subseteq \mathrm{GL}_2(\mathbb{Z}_p)$ consists of matrices whose mod p reduction is $\left(\begin{smallmatrix} * & * \\ 0 & 1 \end{smallmatrix}\right)$;
- $V_1(N)_p = \mathrm{GL}_2(\mathbb{Z}_p)$ otherwise.

Then we say that U is *sufficiently small* if $U \subset V_1(N)$ for some $N \geqslant 4$. If U is sufficiently small, then X_U is naturally the moduli space of false elliptic curves (A,i) with level structure (see [DT94b, §§ 3 and 4]).

For the rest of this section, we will let $U = V_1(q)$ for some suitable prime $q > 3$. In particular, such U is sufficiently small, and $\nu_D(U) = \hat{\mathbb{Z}}^\times$. Suppose that p is a prime away from $\Sigma(D) \cup \{q\}$. There are two natural étale projection maps $\pi_1, \pi_2 : X_{U_0(p)} \to X_U$, which give the Hecke correspondence T_p at p. The abstract Hecke algebra $\mathbb{T}$ consisting of Hecke operators T_l, S_l (for l such that $U_0(p)_l = \mathrm{GL}_2(\mathbb{Z}_l)$) acts on the whole situation by étale correspondences, and hence induces endomorphisms on étale cohomology groups. Because $U_0(p)$ has full level at 2, this picture makes sense over $\mathbb{Z}_2$. We have the following diagram:

$$H^1_{\text{ét}}(X_U,\mathbb{Z}_2)^2 \xrightarrow{i^*} H^1_{\text{ét}}(X_{U_0(p)},\mathbb{Z}_2) \xrightarrow{i_*} H^1_{\text{ét}}(X_U,\mathbb{Z}_2)^2$$

where $i^* = \pi_1^* + \pi_2^*$ and $i_* = \pi_{1*} + \pi_{2*}$. One computes that the composition $i_* i^*$ has the form

$$\begin{pmatrix} p+1 & T_p \\ S_p^{-1}T_p & p+1 \end{pmatrix}.$$

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

We have the following facts:

- $H^1_{\text{ét}}(X_U, \mathbb{Z}_2)$, $H^1_{\text{ét}}(X_{U_0(p)}, \mathbb{Z}_2)$ are torsion-free, and carry a perfect alternating pairing given by Poincaré duality;
- i_* is the adjoint of i^* with respect to the pairings;
- i^* is injective after inverting 2.

By the Jacquet–Langlands correspondence, the system of Hecke eigenvalues $\mathbb{T} \to \overline{\mathbb{Z}}_2$ that occurs in $H^1_{\text{ét}}(X_U, \mathbb{Z}_2)$ is exactly those of automorphic representations π of $\mathrm{GL}_2(\mathbb{A})$ such that:

- π_∞ is a discrete series with trivial infinitesimal character (i.e. π corresponds to a modular form of weight 2);
- for $l \in \Sigma(D)$, π_l is an unramified twist of the Steinberg representation;
- $\pi^U \neq 0$.

A system of Hecke eigenvalues that occurs in the cokernel of i^* will correspond exactly to an automorphic representation π as above which is furthermore *p-new*, i.e. that π_p is an unramified twist of the Steinberg representation. For a maximal ideal $\mathfrak{m}$, π contributes to $H^1_{\text{ét}}(X_U, \mathbb{Z}_2)_\mathfrak{m}$ if and only if the system of Hecke eigenvalues of π is congruent to the one given by $\mathfrak{m}$.

The following fact ('Ihara's lemma') is the key input to level raise in this setting.

Lemma 5.6. *Let $\mathfrak{m}$ be a non-Eisenstein maximal ideal of $\mathbb{T}$ which comes from a modular form g of level prime to 2. Assume that $\rho_\mathfrak{m}|_{G_{\mathbb{Q}_2}}$ is supersingular. Then the localization of i^* at $\mathfrak{m}$ is injective mod 2.*

Proof. In [DT94b, DT94a], this is proven for $\ell \geqslant 3$. This restriction comes from the fact that they used Fontaine–Laffaille theory. We show how to adapt their argument to our situation. If X is a smooth proper curve, we let $J(X)$ denote its Jacobian. The 2-divisible groups $J(X_U)[2^\infty]$ and $J(X_{U_0(p)})[2^\infty]$ admit direct summands $J(X_U)[2^\infty]_\mathfrak{m}$ and $J(X_{U_0(p)})[2^\infty]_\mathfrak{m}$, which are stable under $\mathbb{T}$. By the Eichler–Shimura relations, the Galois representations on $T_2J(X_U)[2]_\mathfrak{m}$ and $T_2J(X_{U_0(p)})[2]_\mathfrak{m}$ are successive extensions of $\rho_\mathfrak{m}$, and hence the summands are connected and unipotent 2-divisible groups. Consider the map $J(X_{U_0(p)})[2^\infty]_\mathfrak{m} \to J(X_U)[2^\infty]^2_\mathfrak{m}$, which on the Tate module is dual to i^*. Assume that i^* is not injective mod 2. Then the induced map $J(X_{U_0(p)})[2]_\mathfrak{m} \to J(X_U)[2]^2_\mathfrak{m}$ is not surjective, and hence has a cokernel that is a successive extension of $\rho_\mathfrak{m}$.

By Fontaine's theorem (see [BC, Theorem 7.2.10]), it follows that the induced map on the Honda systems attached to $J(X_U)[2^\infty]^2_\mathfrak{m}$ and $J(X_{U_0(p)})[2^\infty]_\mathfrak{m}$ is not injective mod 2. But this implies (since the 2-divisible groups involved are connected) that the induced map

$$H^0(J(X_U), \Omega^1)^2_\mathfrak{m} \cong \mathrm{Lie}(J(X_U)[2^\infty]^2_\mathfrak{m})^* \to \mathrm{Lie}(J(X_{U_0(p)})[2^\infty]_\mathfrak{m})^* \cong H^0(J(X_{U_0(p)}), \Omega^1)_\mathfrak{m}$$

is not injective mod 2. Thus,

$$\pi_1^* + \pi_2^* : H^0(X_U \otimes \mathbb{F}_2, \Omega^1)^2_\mathfrak{m} \to H^0(X_{U_0(p)} \otimes \mathbb{F}_2, \Omega^1)_\mathfrak{m}$$

has non-trivial kernel. Let (ω_1, ω_2) be a non-zero element in the kernel. Arguing as in [DT94b, Lemmas 8 and 9], we conclude that the divisor of ω_1 must be inside the supersingular locus of $X_U \otimes \mathbb{F}_2$, and in fact contains all supersingular points. Now, by [Kas99, § 5], there are a line bundle ω on $X_U \otimes \mathbb{F}_2$ and a section $\mathrm{Ha} \in H^0(X_U \otimes \mathbb{F}_2, \omega)$ which vanishes to order 1 at each supersingular point (note that even though the running assumption of [Kas99] is that $\ell > 3$, this

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

is not needed for [Kas99, § 5]). This property determines Ha up to a non-zero scalar. Using this characterization, we get that $\pi_1^*\mathrm{Ha}$ and $\pi_2^*\mathrm{Ha}$ coincide up to a non-zero scalar. It is known that $\mathbb{T}$ acts on Ha through an Eisenstein maximal ideal.

Now, we have an isomorphism $\Omega^1 \cong \omega^{\otimes 2}$, and hence we conclude that $\omega_1 = \mathrm{Ha} \cdot \omega_1'$ for some $\omega_1' \in H^0(X_U, \omega)$, and similarly for ω_2. But now in the equation $\pi_1^*\omega_1 = -\pi_2^*\omega_2$ we can cancel out $\pi_1^*\mathrm{Ha}$, and hence $\pi_1^*\omega_1'$ agrees with $\pi_2^*\omega_2'$ up to a non-zero scalar. Repeating the argument now forces $\omega_1' = c \cdot \mathrm{Ha}$, and hence $\omega_1 = c \cdot \mathrm{Ha}^2$. But then the action of $\mathbb{T}$ on ω_1 is Eisenstein, contradicting the fact that $\omega_1 \in H^0(X_U \otimes \mathbb{F}_2, \Omega^1)_{\mathfrak{m}}$ and $\mathfrak{m}$ is non-Eisenstein. □

The following is the main result of this section.

Lemma 5.7. *Suppose that $\mathfrak{m}$ is a maximal ideal of $\mathbb{T}$ that corresponds to the mod 2 reduction of a system of Hecke eigenvalues that contributes to $H^1_{\text{ét}}(X_U, \mathbb{Z}_2)$. Assume that $\mathfrak{m}$ is non-Eisenstein, that $\rho_{\mathfrak{m}}$ is supersingular at 2 and that p is a prime such that $T_p \in \mathfrak{m}$. Then there exists a p-new system of Hecke eigenvalues lifting $\mathfrak{m}$.*

Proof. By what we have said so far, we only need to show that $H^1_{\text{ét}}(X_{U_0(p)}, \mathbb{Z}_2)_{\mathfrak{m}}/\mathrm{Im}\, i^*$ is not torsion. Suppose that this is the case; then, because i^* is injective mod 2 (Lemma 5.6), this quotient is actually trivial and hence i^* is an isomorphism. By duality, i_* is also an isomorphism. But $T_p \in \mathfrak{m}$ implies that i_*i^* is 0 mod $\mathfrak{m}$ and hence cannot be surjective. This gives the desired contradiction. □

5.8 Proof of Theorem 2.9 in the supersingular case

In this section we prove Theorem 2.9 under the assumption that the modular mod 2 representation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_2)$ is supersingular at 2. We choose a prime $p_1|N$ such that $\mathrm{ord}_{p_1}(N) > 1$ and $\mathrm{ord}_{p_1}(\Delta)$ is odd if such a prime exists, otherwise choose any prime $p_1|N$. Choose an auxiliary prime $q > 7$ as in Definition 3.1. We choose $U_q \subset \mathrm{Iw}_1(q^n) \subset \mathrm{GL}_2(\mathbb{Z}_q)$, a sufficiently small open compact subgroup as in Definition 5.3.

We will first show that we can find a weight 2 modular form g with trivial central character, such that g is new at each prime q_i in our list (without specifying the signs).

Proposition 5.9. *Assume that we are in the situation of Theorem 2.9, with $\overline{\rho}$ supersingular. Then there is a modular form g of weight 2 with corresponding automorphic representation π of $\mathrm{GL}_2(\mathbb{A})$ such that:*

- *π has trivial central character;*
- *for $p \| N$ or $p = q_i$, π_p is an unramified twist of the Steinberg representation;*
- *for $p|N$, $\pi_p^{\mathrm{Iw}(p^{\mathrm{ord}_p(N)})} \neq 0$;*
- *$\pi_q^{U_q} \neq 0$;*
- *for all other primes p, π_p is unramified.*

Proof. This is done by induction on the number m of level raising primes. In the case $m = 1$ this follows from Ribet's theorem. Assume that we have found a level raising form g at m primes $q_1, \ldots, q_m$, and we wish to add in a prime q_{m+1}. The automorphic representation π_g is an unramified twist of the Steinberg representations at q_i and the primes $p \| N$. Let D be the quaternion algebra that ramifies at exactly these primes (it is definite or indefinite depending on the parity of the size of this set). Let $\mathfrak{m}$ be the maximal ideal of the abstract Hecke algebra that corresponds to $\overline{\rho}$. By assumption it is non-Eisenstein, and its associated mod 2 Galois representation is supersingular at 2. Let $U \subset G_D(\mathbb{A})$ be the open compact subgroup given by:

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

– $U_p = (\mathcal{O}_D \otimes \mathbb{Z}_p)^\times$ for $p \in \Sigma(D)$;
– $U_p = \mathrm{Iw}(p^{\mathrm{ord}_p(N)})$ for $p|N$, $p \notin \Sigma(D)$;
– U_q is chosen as above;
– $U_p = \mathrm{GL}_2(\mathbb{Z}_p)$ otherwise.

If D is definite, π_g contributes to the space $S(U, \overline{\mathbb{Z}}_2)$. By Lemma 5.4, we can find an automorphic representation π' corresponding to a weight 2 modular form g' congruent to g mod 2, such that $\pi'^{U_0(q_{m+1})} \neq 0$, that π' is new at q_{m+1} and that π' has trivial central character. This does the inductive step in this case.

If D is indefinite, π_g contributes to the space $H^1_{\text{ét}}(X_U \otimes \overline{\mathbb{Q}}_2, \overline{\mathbb{Z}}_2)$. By Lemma 5.7, we can find an automorphic representation π' corresponding to a weight 2 modular form g' congruent to g mod 2, such that $\pi'^{U_0(q_{m+1})} \neq 0$ and that π' is new at q_{m+1}. We claim that π' must have trivial central character or, equivalently, its associated Galois representation $\rho_{\pi'}$ has determinant ψ_2. The fact that π' has weight 2 and $\pi'^{U_0(q_{m+1})} \neq 0$ imply that $\det \rho_{\pi'} \psi_2^{-1}$ is a finite order character that is unramified at all $p \neq q$. By our choice of q and Remark 3.5, $\det \rho_{\pi'} \psi_2^{-1}|_{I_{\mathbb{Q}_q}}$ has order at most 2. But, since $\rho_{\pi'}$ is odd, we must have $\det \rho_{\pi'} \psi_2^{-1}(-1) = 1$, where we think of $-1 \in \mathbb{Z}_q^\times \cong I_{\mathbb{Q}_q^{\mathrm{ab}}}$ via local class field theory. But, since $q \equiv 3 \bmod 4$, -1 is a generator of $\mathbb{Z}_q^\times / (\mathbb{Z}_q^\times)^2$, and thus we conclude that $\det \rho_{\pi'} \psi_2^{-1}$ is unramified at q as well. But, since $\mathbb{Q}$ has class number 1, this forces this character to be trivial, so π' indeed has trivial central character. This finishes the inductive step in this case. □

Finally, we show how to modify the signs at level raising primes. Let π be the automorphic representation given by Proposition 5.9.

Now let $\Sigma(D)$ be the set of all primes where π_p is an unramified twist of the Steinberg representation. Let D be the quaternion algebra whose finite ramification places are exactly the places in $\Sigma(D)$.

Case 1: D is definite. Let U be the $(\Sigma(D) \subset \Sigma(D))$-open subgroup of $G_D(\mathbb{A}^\infty)$ such that:

– for $p|N$, $p \notin \Sigma(D)$, U_p is $\mathrm{Iw}(p^{\mathrm{ord}_p(N)})$;
– U_q is chosen as above;
– for $p \notin \Sigma(D)$ and $p \not| Nq$, $U_p = \mathrm{GL}_2(\mathbb{Z}_p)$.

Let $\gamma = (\gamma_v)_{v \in \Sigma(D)}$ be the collection of characters of $\mathbb{Q}_p^\times \to \mu_2$ such that $\gamma_p(p) = \epsilon_p$, an arbitrarily chosen sign at the prime $p \in \Sigma(D)$. The automorphic representation π determines a γ_π, which is the tuple of signs of π_p for $p \in \Sigma(D)$. Now, since U is sufficiently small, the reduction mod 2 maps

$$S_\gamma(U, \mathbb{Z}_2) \to S_\gamma(U, \mathbb{F}_2),$$
$$S_{\gamma_\pi}(U, \mathbb{Z}_2) \to S_{\gamma_\pi}(U, \mathbb{F}_2)$$

are both surjective. Note however that $S_{\gamma_\pi}(U, \mathbb{F}_2) = S_\gamma(U, \mathbb{F}_2)$, because any γ reduces to the trivial character mod 2. If $\mathfrak{m}$ is the ideal in $\mathbb{T}$ associated to the mod 2 reduction of the system of Hecke eigenvalues of π, we see that $S_{\gamma_\pi}(U, \mathbb{Z}_2)_\mathfrak{m} \neq 0$. Hence, $S_\gamma(U, \mathbb{F}_2)_\mathfrak{m} \neq 0$ and, because reduction mod 2 is surjective, $S_\gamma(U, \mathbb{Z}_2)_\mathfrak{m} \neq 0$. Note also that $S_\gamma(U, \mathbb{Z}_2)$ is torsion-free. Thus, there exists an automorphic representation π' satisfying the same properties as π listed above, but furthermore at each $p \in \Sigma(D)$, π' is the γ_p-twist of the Steinberg representation. This π' is almost what we want, except that π' might ramify at q. However, by Corollary 3.6, either π' is unramified, or the quadratic twist $\pi' \otimes \chi_q$ is unramified at q, where χ_q is the unique quadratic character that ramifies only at q. By the choice of q, we are done as in § 4.3.

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

Remark 5.10. The above argument shows also that if γ is trivial, then $S_{\gamma_\pi}(U, \mathbb{Z}_2)_{\mathfrak{m}} \neq 0$ implies that $S_\gamma(U, \mathbb{Z}_2)_{\mathfrak{m}} \neq 0$ even if U is not sufficiently small. It follows that there always exists a level raising form all of whose signs are $+1$ in this case.

Case 2: D is indefinite. Let V be the open (but not compact) subgroup of $G_D(\mathbb{A}^\infty)$ such that:

- for $p|N$, $p \notin \Sigma(D)$, V_p is $\mathrm{Iw}(p^{\mathrm{ord}_p(N)})$;
- $V_q = \mathrm{Iw}_1(q)Z(\mathbb{Z}_q)$;
- for $p \in \Sigma(D)$, $V_p = G_D(\mathbb{Q}_p) = (D \otimes \mathbb{Q}_p)^\times$;
- for all other p, $V_p = \mathrm{GL}_2(\mathbb{Z}_p)$.

Lemma 5.11. *For any $g \in G_D(\mathbb{A}^\infty)$, $gG_D(\mathbb{Q})g^{-1} \cap VZ(\mathbb{A}^\infty)/Z(\mathbb{Q})$ has no non-trivial element of order $< q$.*

Proof. Suppose that γ is a non-trivial element of order $h < q$. Writing the q-component of γ as kz with $z \in Z(\mathbb{Q}_q)$, $k \in \mathrm{Iw}_1(q)$, we have $k^h z^h$ is central and hence k^h is central. But then k^h is an element in $\mathbb{Z}_q^\times$ which is 1 mod q; hence, we can extract an hth root z' of it which is also 1 mod q. Then $(kz'^{-1})^h = 1$ but $kz'^{-1} \in \mathrm{Iw}_1(q)$ is an element of a pro-q group, so $k = z'$. Hence, γ is central. □

Let $U \subset G_D(\mathbb{A}^\infty)$ be the open compact subgroup of V such that $U_p = V_p$ for all $p \notin \Sigma(D)$, and $U_p = (\mathcal{O}_D \otimes \mathbb{Z}_p)^\times$ otherwise. As in the previous section, we define

$$X_V = G_D(\mathbb{Q})\backslash \mathbb{H}^\pm \times G_D(\mathbb{A}^\infty)/V$$

and similarly for X_U. Note that neither double coset will change if we replace U, V by $UZ(\mathbb{A}^\infty)$, $VZ(\mathbb{A}^\infty)$, because $U_p \supset Z(\mathbb{Z}_p)$ and $Z(\mathbb{A}^\infty) = Z(\mathbb{Q}) \prod_p Z(\mathbb{Z}_p)$.

Lemma 5.12. *X_U, X_V are compact Riemann surfaces. The natural projection map $X_U \to X_V$ is unramified everywhere, and is a Galois covering with Galois group*

$$VZ(\mathbb{A}^\infty)/UZ(A^\infty) \cong \prod_{p \in \Sigma(D)} \mathbb{Z}/2.$$

Proof. By strong approximation, we have a finite decomposition $G_D(\mathbb{A}^\infty) = \coprod G_D(\mathbb{Q}) t_i V$. This gives

$$X_V = \coprod \Gamma_i \backslash \mathbb{H}^\pm,$$

where $\Gamma_i = t_i V t_i^{-1} \cap G_D(\mathbb{Q})$ is a discrete group acting on $\mathbb{H}^\pm$ through its infinite component (which is in $\mathrm{GL}_2(\mathbb{R})$). This gives X_V the structure of a compact Riemann surface in the usual way.

The group $VZ(\mathbb{A}^\infty)/UZ(A^\infty)$ acts on X_U by right translation. Notice that for each $p \in \Sigma(D)$, $V_p Z(\mathbb{Q}_p)/U_p Z(\mathbb{Q}_p) \cong \mathbb{Z}/2$. We claim that the action is faithful and free. Suppose that $vz \in VZ(\mathbb{A}^\infty)$ fixes a point represented by (τ, g) with $\tau \in \mathbb{H}^\pm$, $g \in G_D(\mathbb{A})$. This means that there exist $\gamma \in G_D(\mathbb{Q})$, $u \in U$ such that

$$(\tau, gvz) = (\gamma\tau, \gamma g u).$$

The element $\gamma \in G_D(\mathbb{Q}) \cap gVZ(\mathbb{A}^\infty)g^{-1}$ thus has a fixed point in $\mathbb{H}^\pm$. Because $\gamma \in G_D(\mathbb{Q})$ acts discretely on $\mathbb{H}^\pm$, it acts as a finite order automorphism on $\mathbb{H}^\pm$, and there exists $h \leqslant 6$ such that γ^h acts trivially on $\mathbb{H}^\pm$. By Lemma 5.11 (and the fact that q is chosen to be large), γ is central. But then $gvz = \gamma g u$ implies that $vz \in UZ(\mathbb{A}^\infty)$. □

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

Given the above lemmas, we proceed similar to the previous case. For $\gamma = (\gamma_p)_{p\in\Sigma(D)}$, a tuple of unramified characters $\gamma_p : \mathbb{Q}_p^\times \to \mu_2$, we have the local system $\mathbb{Z}_2(\gamma)$ on X_V, given by twisting the trivial local system along the covering map $X_U \to X_V$. We have a short exact sequence

$$0 \to H^1(X_V, \mathbb{Z}_2(\gamma))/2 \to H^1(X_V, \mathbb{F}_2(\gamma)) \to H^2(X_V, \mathbb{Z}_2(\gamma))[2].$$

The Hecke algebra $\mathbb{T} = \mathbb{Z}[T_p, S_p]_{p\notin\Sigma(D)\cup\{q\}}$ acts on each term of the sequence, and the sequence is equivariant with respect to the $\mathbb{T}$-action. Since the $\mathbb{T}$-action on the H^2 is Eisenstein, for $\mathfrak{m}$ the non-Eisenstein maximal ideal corresponding to the mod 2 representation $\bar{\rho}$, we have that

$$H^1(X_V, \mathbb{Z}_2(\gamma))_\mathfrak{m} \to H^1(X_V, \mathbb{F}_2(\gamma))_\mathfrak{m}$$

is a surjection of Hecke modules. If γ_π denotes the tuple giving the signs of π, we have $H^1(X_V, \mathbb{Z}_2(\gamma_\pi))_\mathfrak{m} \neq 0$ and hence $H^1(X_V, \mathbb{F}_2(\gamma_\pi))_\mathfrak{m} = H^1(X_V, \mathbb{F}_2)_\mathfrak{m} \neq 0$. Because the Hecke action on H^0 is also Eisenstein, $H^1(X_V, \mathbb{Z}_2(\gamma))_\mathfrak{m}$ is torsion-free. Thus, for any γ, $H^1(X_V, \mathbb{Z}_2(\gamma))_\mathfrak{m} \neq 0$. The Jacquet–Langlands correspondence gives an automorphic representation π' contributing to this space, and we are done by the same argument as in the definite case. This finishes the proof of Theorem 2.9 in the supersingular case.

6. Preliminaries on local conditions

So far we have only used items (1)–(4) of Assumption 2.1. Henceforth we will assume that all items in Assumption 2.1 hold for the elliptic curve E. Suppose that A is obtained from E via level raising at $m \geqslant 0$ primes (Definition 2.11). Fix an isomorphism between $A[\lambda] \cong E[2] \otimes k$ and denote it by V.

Definition 6.1. Let v be a place of $\mathbb{Q}$. We define $H^1_{\mathrm{ur}}(\mathbb{Q}_v, V) := H^1(\mathbb{Q}_v^{\mathrm{ur}}/\mathbb{Q}_v, V^I) \subseteq H^1(\mathbb{Q}_v, V)$, consisting of classes which are split over an unramified extension of $\mathbb{Q}_v$.

Definition 6.2. Let $\mathcal{L} = \{\mathcal{L}_v\}$ be the collection of k-subspaces $\mathcal{L}_v \subseteq H^1(\mathbb{Q}_v, V)$, where v runs over every place of $\mathbb{Q}$. We say that $\mathcal{L}$ is a collection of *local conditions* if $\mathcal{L}_v = H^1_{\mathrm{ur}}(\mathbb{Q}_v, V)$ for almost all v. We define the *Selmer group* cut out by the local conditions $\mathcal{L}$ to be

$$H^1_\mathcal{L}(V) := \{x \in H^1(\mathbb{Q}, V) : \mathrm{res}_v(x) \in \mathcal{L}_v, \text{for all } v\}.$$

Definition 6.3. We define $\mathcal{L}_v(A)$ to be the image of the local Kummer map

$$A(\mathbb{Q}_v) \otimes_{\mathcal{O}_F} \mathcal{O}_F/\lambda \to H^1(\mathbb{Q}_v, A[\lambda]) = H^1(\mathbb{Q}_v, V).$$

The λ-*Selmer group* of A is defined to be the Selmer group cut out by $\mathcal{L}(A) := \{\mathcal{L}_v(A)\}$, denoted by $\mathrm{Sel}_\lambda(A/\mathbb{Q})$, or $\mathrm{Sel}(A)$ for short (if that causes no confusion). Its dimension as a k-space is called the λ-*Selmer rank* of A, denoted by $\dim \mathrm{Sel}(A)$ for short. For details on descent with endomorphisms, see the [GP12, Appendix].

Definition 6.4. The Weil pairing $E[2] \times E[2] \to \mu_2$ induces a perfect pairing $V \times V \to k(1)$. We identify $V \cong V^* = \mathrm{Hom}\,(V, k(1))$ using this pairing. For each place v of $\mathbb{Q}$, we define the cup product pairing

$$\langle\ ,\ \rangle_v : H^1(\mathbb{Q}_v, V) \times H^1(\mathbb{Q}_v, V) \to H^2(\mathbb{Q}_v, k(1)) \cong k.$$

This is a perfect pairing by the local Tate duality. We denote the annihilator of $\mathcal{L}_v$ by

$$\mathcal{L}_v^\perp := \{x \in H^1(\mathbb{Q}_v, V) : \langle x, y\rangle_v = 0, \text{for all } y \in \mathcal{L}_v\}.$$

Then $\dim_k \mathcal{L}_v + \dim \mathcal{L}_v^\perp = \dim H^1(\mathbb{Q}_v, V)$ by the non-degeneracy of $\langle\ ,\ \rangle_v$. By the local Tate duality for the elliptic curve E, $\mathcal{L}_v(E)$ is equal to its own annihilator $\mathcal{L}_v(E)^\perp$ and hence $\dim \mathcal{L}_v(E) = \frac{1}{2} \dim H^1(\mathbb{Q}_v, V)$.

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

Lemma 6.5. *Suppose that $v \nmid 2N\infty$. Then*

$$\dim H^1(\mathbb{Q}_v, V) = 2 \dim H^1_{\mathrm{ur}}(\mathbb{Q}_v, V) = 0, 2, 4,$$

if Frob_v *is of order* $3, 2, 1$ *acting on* V*, respectively.*

Proof. The map $c \mapsto c(\mathrm{Frob}_v)$ induces an isomorphism $H^1_{\mathrm{ur}}(\mathbb{Q}_v, V) \cong V^I/(\mathrm{Frob}_v - 1)V^I$, which has dimension $0, 1, 2$ if Frob_v has order $3, 2, 1$, respectively. It follows from [Mil86, I.2.6] that the annihilator of $H^1_{\mathrm{ur}}(\mathbb{Q}_v, V)$ is equal to itself and hence $\dim H^1(\mathbb{Q}_v, V) = 2 \dim H^1_{\mathrm{ur}}(\mathbb{Q}_v, V)$. □

Under our assumptions, the following lemma identifies the local conditions of the abelian variety A purely in terms of the Galois representation V, which is the key to control Selmer ranks in level raising families in the next two sections.

Lemma 6.6. *Suppose that A is obtained from E via level raising at primes $q_1, \dots, q_m$ $(m \geqslant 0)$. Let $\mathcal{L} = \mathcal{L}(A)$ be the local conditions defining* $\mathrm{Sel}(A)$*. Then:*

(1) *for $v \nmid 2q_1 \cdots q_m \infty$,*
$$\mathcal{L}_v = \mathcal{L}_v^\perp = H^1_{\mathrm{ur}}(\mathbb{Q}_v, V);$$

(2) *for $v = \infty$,*
$$\mathcal{L}_v = H^1(\mathbb{Q}_v, V) = 0;$$

(3) *for $v = q_i$, if Frob_{q_i} has order 2 acting on V and A has sign $\varepsilon_i = +1$, then $H^1(\mathbb{Q}_v, V)$ is 2-dimensional and*
$$\mathcal{L}_v = \mathcal{L}_v^\perp = \mathrm{im}(H^1(\mathbb{Q}_v, W) \to H^1(\mathbb{Q}_v, V))$$
is 1-dimensional. Here W is the unique $G_{\mathbb{Q}_v}$-stable line in V. Moreover, $\mathcal{L}_v$ and $H^1_{\mathrm{ur}}(\mathbb{Q}_v, V)$ are distinct lines;

(4) *if E is good at $v = 2$, then*
$$\mathcal{L}_2 = \mathcal{L}_2^\perp = H^1_{\mathrm{fl}}(\mathrm{Spec}\ \mathbb{Z}_2, \mathcal{E}[2]) \otimes k,$$
where $\mathcal{E}/\mathbb{Z}_2$ is the Neron model of $E/\mathbb{Q}_2$ and $H^1_{\mathrm{fl}}(\mathrm{Spec}\ \mathbb{Z}_2, \mathcal{E}[2])$ is the flat cohomology group, viewed as a subspace of $H^1_{\mathrm{fl}}(\mathrm{Spec}\ \mathbb{Q}_2, E[2]) = H^1(\mathbb{Q}_2, E[2])$;

(5) *if E is multiplicative at $v = 2$, then*
$$\mathcal{L}_2 = \mathcal{L}_2^\perp = \mathrm{im}(H^1(\mathbb{Q}_2, W) \to H^1(\mathbb{Q}_2, V)).$$
Here W is the unique $G_{\mathbb{Q}_2}$-stable line in V.

Proof. (1) The fact that $\mathcal{L}_v = H^1_{\mathrm{ur}}(\mathbb{Q}_v, V)$ follows from [GP12, Lemma 6] and Remark 2.4.

(2) By Remark 2.6, the complex conjugation c acts non-trivially on V, so $H^1(\mathbb{R}, V) = V^c/(1 + c)V = 0$.

(3) Write $q = q_i$ and $\varepsilon = \varepsilon_i$ for short. Our argument closely follows the proof of [GP12, Lemma 8]. Let $\mathcal{A}/\mathbb{Z}_q$ be the Neron model of $A/\mathbb{Q}_q$. Let $\mathcal{A}^0/\mathbb{F}_q$ be the identity component of the special fiber of $\mathcal{A}$. Since A is an isogeny factor of the new quotient of $J_0(Nq_1 \cdots q_m)$, it has purely toric reduction at q: $\mathcal{A}^0/\mathbb{F}_q$ is a torus that is split over $\mathbb{F}_{q^2}$ and it is split over $\mathbb{F}_q$ if and only if $\varepsilon = +1$. By the Neron mapping property, $\mathcal{O}_F$ acts on $\mathcal{A}^0$ and makes the character group $X^*(\mathcal{A}^0/\mathbb{F}_q) \otimes \mathbb{Q}$ a 1-dimensional F-vector space. Let $T/\mathbb{Q}_q$ be the split torus with character group $X^*(\mathcal{A}^0/\mathbb{F}_q)$. Then $\mathcal{O}_F$ naturally acts on T (dual to the action on the character group).

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

By the theory of q-adic uniformization, we have a $G_{\mathbb{Q}_q}$-equivariant exact sequence

$$0 \to \Lambda \to T(\overline{\mathbb{Q}_q}) \to A(\overline{\mathbb{Q}_q}) \to 0,$$

where Λ is a free $\mathbb{Z}$-module with trivial $G_{\mathbb{Q}_q}$-action. Since $\mathcal{O}_F$ is a maximal order, Λ is a locally free $\mathcal{O}_F$-module of rank one. Consider the following commutative diagram:

$$\begin{array}{ccc} T(\mathbb{Q}_q) \otimes \mathcal{O}_F/\lambda & \longrightarrow & H^1(\mathbb{Q}_q, T[\lambda]) \\ \downarrow & & \downarrow \\ A(\mathbb{Q}_q) \otimes \mathcal{O}_F/\lambda & \longrightarrow & H^1(\mathbb{Q}_q, A[\lambda]) \end{array}$$

Here the horizontal arrows are the local Kummer maps and the vertical maps are induced by the q-adic uniformization. The left vertical map is surjective since its cokernel lies in $H^1(\mathbb{Q}_q, \Lambda)$ $= \mathrm{Hom}\,(G_{\mathbb{Q}_q}, \Lambda)$, which is zero as Λ is torsion-free. The top horizontal map is also surjective since its cokernel maps into $H^1(\mathbb{Q}_q, T)$, which is zero by Hilbert 90 as T is a split torus. It follows that

$$\mathcal{L}_q = \mathrm{im}(H^1(\mathbb{Q}_q, T[\lambda]) \to H^1(\mathbb{Q}_q, A[\lambda])).$$

Also, because Λ has no λ-torsion, we see that $T[\lambda] \to A[\lambda]$ is a $G_{\mathbb{Q}_q}$-equivariant injection. But, since Frob_q is assumed to have order 2 acting on $V = A[\lambda]$, V has a unique $G_{\mathbb{Q}_q}$-stable line W. Therefore,

$$\mathcal{L}_q = \mathrm{im}(H^1(\mathbb{Q}_q, W) \to H^1(\mathbb{Q}_q, V)).$$

It follows from Lemma 6.5 that $H^1(\mathbb{Q}_q, V)$ is 2-dimensional and $H^1_{\mathrm{ur}}(\mathbb{Q}_q, V)$ is 1-dimensional. A class $c \in H^1(\mathbb{Q}_q, W) = \mathrm{Hom}\,(G_{\mathbb{Q}_q}, W)$ is determined by its image on σ (a lift of Frob_v) and a tame generator τ. Suppose that $E[2](\mathbb{Q}_q) = \langle P \rangle$; then the class $c(\tau) = 0$, $c(\sigma) = P$ is cohomologous to zero in $H^1(\mathbb{Q}_v, V)$ (equal to the coboundary of a non-$\mathbb{Q}_q$-rational point in $E[2]$). We see that $\mathcal{L}_q$ is generated by the class $c(\tau) = P$, $c(\sigma) = 0$. So, $\mathcal{L}_q$ is 1-dimensional and $\mathcal{L}_q \cap H^1_{\mathrm{ur}}(\mathbb{Q}_q, V) = 0$. This finishes the proof.

(4) Let $\mathcal{E}/\mathbb{Z}_2$ be the Neron model of $E/\mathbb{Q}_2$ and $\mathcal{A}/\mathbb{Z}_2$ be the Neron model of $A/\mathbb{Q}_2$. We claim that $\mathcal{E}[2] \otimes k = \mathcal{A}[\lambda]$ over $\mathbb{Z}_2$ (extending the isomorphism $E[2] \otimes k = A[\lambda]$).

First consider the case that E is supersingular at 2. Let W be the strict henselization of $\mathbb{Z}_2$. Let F be the fraction field of W and I be the absolute Galois group of F (i.e. the inertia subgroup at 2). Notice that $E[2]$ is an irreducible $\mathbb{F}_2[I]$-module (see [Ser72, p. 275, Proposition 12], see also [Con97, Theorem 1.1]); hence, by [Ray74, 3.3.2.3°], we know that $E[2]$ has a unique finite flat model over W. Since the descent datum from W to $\mathbb{Z}_2$ is determined by that of the generic fiber, $E[2]$ has a *unique* finite flat model over $\mathbb{Z}_2$ as well. Now $E[2] \otimes k$ is a direct sum of $[k : \mathbb{F}_2]$ copies of $E[2]$; by the standard five-lemma argument (see [Tat97, Proposition 4.2.1]), we know that $E[2] \otimes k$ also has a unique finite flat model over $\mathbb{Z}_2$. We conclude that this unique finite flat model of $E[2] \otimes k$ must be isomorphic to $\mathcal{E}[2] \otimes k = \mathcal{A}[\lambda]$.

Now consider the case that E is ordinary at 2. Then $\mathcal{E}[2]$ is an extension of $\mathbb{Z}/2\mathbb{Z}$ by μ_2 over $\mathbb{Z}_2$. Notice that $b_2 \equiv a_2 \not\equiv 0 \pmod{\lambda}$ by construction; we know that $\mathcal{A}[\lambda]$ is also ordinary, i.e. an extension of $\mathbb{Z}/2\mathbb{Z} \otimes k$ by $\mu_2 \otimes k$ over $\mathbb{Z}_2$. To show that $\mathcal{E}[2] \otimes k = \mathcal{A}[\lambda]$, it suffices to show that $E[2] \otimes k = A[\lambda]$ has a unique finite flat model over $\mathbb{Z}_2$ that is an extension of $\mathbb{Z}/2\mathbb{Z} \otimes k$ by $\mu_2 \otimes k$. This is true because of Assumption 2.1(4) that $G_{\mathbb{Q}_2}$ acts non-trivially on $E[2]$. In fact, the generic fiber map

$$\mathrm{Ext}_{\mathbb{Z}_2}(\mathbb{Z}/2\mathbb{Z}, \mu_2) \to \mathrm{Ext}_{\mathbb{Q}_2}(\mathbb{Z}/2\mathbb{Z}, \mu_2)$$

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

between the extension groups in the category of fppf sheaves of $\mathbb{Z}/2\mathbb{Z}$-modules can be identified with the natural map

$$H^1_{\mathrm{fppf}}(\mathbb{Z}_2, \mu_2) \cong \mathbb{Z}_2^\times/(\mathbb{Z}_2^\times)^2 \to H^1_{\mathrm{fppf}}(\mathbb{Q}_2, \mu_2) \cong \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2.$$

This map is injective. As a direct sum of $[k : \mathbb{F}_2]^2$ copies of this map, it follows that

$$\mathrm{Ext}_{\mathbb{Z}_2}(\mathbb{Z}/2\mathbb{Z} \otimes k, \mu_2 \otimes k) \to \mathrm{Ext}_{\mathbb{Q}_2}(\mathbb{Z}/2\mathbb{Z} \otimes k, \mu_2 \otimes k)$$

is also injective, which means that the extension class of such a finite flat model $\mathcal{V}$ of $E[2] \otimes k$ is determined by the extension class of the generic fiber of $\mathcal{V}$. But $G_{\mathbb{Q}_2}$ acts non-trivially on $E[2]$, there is a unique $\mathbb{F}_2$-subspace of dimension $[k : \mathbb{F}_2]$ in $E[2] \otimes k$ with trivial $G_{\mathbb{Q}_2}$-action, so the extension class of the generic fiber of $\mathcal{V}$ is uniquely determined by $E[2] \otimes k$, as desired.

In both cases, we have $\mathcal{E}[2] \otimes k = \mathcal{A}[\lambda]$. Now, by [GP12, Lemma 7], we know that

$$\mathcal{L}_v = H^1_{\mathrm{fl}}(\mathbb{Z}_2, \mathcal{A}[\lambda]) = H^1_{\mathrm{fl}}(\mathbb{Z}_2, \mathcal{E}[2]) \otimes k.$$

(5) By Assumption 2.1(3), there exists a unique $G_{\mathbb{Q}_2}$-stable line W in V. If A has split toric reduction at 2, the claim follows from the same argument as in (3) using the 2-adic uniformization of $A/\mathbb{Q}_2$. Now let us assume that A has non-split toric reduction. Since $G_{\mathbb{Q}_2}$ acts on V non-trivially and the image of $\bar{\rho}|_{\mathbb{Q}_2}$ has order 2, one easily sees that $\dim H^1(\mathbb{Q}_2, V) = 4$ by the Euler characteristic formula and

$$\dim \mathrm{im}(H^1(\mathbb{Q}_2, W) \to H^1(\mathbb{Q}_2, V)) = 2$$

by the long exact sequence in Galois cohomology associated to the short exact sequence

$$0 \to W \to V \to W/V \to 0.$$

Since $\mathcal{L}_2$ is a maximal isotropic subspace of $H^1(\mathbb{Q}_2, V)$ by the local Tate duality for A, we know that $\dim \mathcal{L}_2 = 2$, half of the dimension of $H^1(\mathbb{Q}_2, V)$. To prove the claim, it suffices to show that $\mathcal{L}_2$ contains $\mathrm{im}(H^1(\mathbb{Q}_2, W) \to H^1(\mathbb{Q}_2, V))$.

Let T be the split torus over $\mathbb{Q}_2$ with character group $X^*(\mathcal{A}^0/\mathbb{F}_2)$. Let χ be the unramified quadratic character $\chi : \mathrm{Gal}\,(\mathbb{Q}_4/\mathbb{Q}_2) \to \{\pm 1\}$ and $T(\chi)$ be the χ-twist of T. We have a $G_{\mathbb{Q}_2}$-equivariant exact sequence

$$0 \to \Lambda(\chi) \to T(\chi)(\overline{\mathbb{Q}_2}) \to A(\overline{\mathbb{Q}_2}) \to 0,$$

where Λ is a locally free $\mathcal{O}_F$-module of rank one with trivial $G_{\mathbb{Q}_2}$-action. As in (3), consider the following commutative diagram:

$$\begin{array}{ccc} T(\chi)(\mathbb{Q}_2) \otimes \mathcal{O}_F/\lambda & \longrightarrow & H^1(\mathbb{Q}_2, T(\chi)[\lambda]) \\ \downarrow & & \downarrow \\ A(\mathbb{Q}_2) \otimes \mathcal{O}_F/\lambda & \longrightarrow & H^1(\mathbb{Q}_2, A[\lambda]) \end{array}$$

Since the image of the right vertical arrow is $\mathrm{im}(H^1(\mathbb{Q}_2, W) \to H^1(\mathbb{Q}_2, V))$, we are done if the left vertical arrow is surjective or, equivalently,

$$\ker(H^1(\mathbb{Q}_2, \Lambda(\chi))_\lambda \to H^1(\mathbb{Q}_2, T(\chi))_\lambda) \otimes \mathcal{O}_F/\lambda \tag{6.6.0}$$

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

is zero. Since $H^1(\mathbb{Q}_4, \Lambda(\chi)) = 0$ (Λ is torsion-free) and $H^1(\mathbb{Q}_4, T(\chi)) = 0$ by Hilbert 90 ($T(\chi)$ splits over $\mathbb{Q}_4$), by inflation–restriction we know that

$$H^1(\mathbb{Q}_2, \Lambda(\chi)) = H^1(\mathbb{Q}_4/\mathbb{Q}_2, \Lambda(\chi)) = \Lambda/2\Lambda$$

and

$$H^1(\mathbb{Q}_2, T(\chi)) = H^1(\mathbb{Q}_4/\mathbb{Q}_2, T(\chi)(\mathbb{Q}_4)) = T(\mathbb{Q}_2)/\mathbb{N}(T(\mathbb{Q}_4)),$$

where $\mathbb{N} : T(\mathbb{Q}_4) \to T(\mathbb{Q}_2)$ is the norm map. The domain and target in (6.6.0) are finite $\mathcal{O}_{F,\lambda}$-modules of the same size because Λ is a locally free $\mathcal{O}_F$-module of rank one. Hence, it suffices to show that

$$H^1(\mathbb{Q}_2, \Lambda(\chi))_\lambda \to H^1(\mathbb{Q}_2, T(\chi))_\lambda$$

is surjective, which can be checked after tensoring with $\mathcal{O}_F/\lambda$, i.e.

$$\Lambda/\lambda\Lambda \to T(\mathbb{Q}_2)/\mathbb{N}(T(\mathbb{Q}_4)) \otimes \mathcal{O}_F/\lambda$$

is surjective. Since these are 1-dimensional k-vector spaces, it suffices to show that this last map is non-zero. We claim that for any $a \in \Lambda - \lambda\Lambda$, we have $a \notin \mathbb{N}(T(\mathbb{Q}_4))$. This is true because of Assumption 2.1(3) that $\bar{\rho}$ is ramified at 2. In fact, let $\lambda^{-1}\Lambda = \{t \in T(\chi) : \lambda t \subseteq \Lambda\}$; then $A[\lambda] \cong \lambda^{-1}\Lambda/\Lambda$ (notice that $\lambda^{-1}\Lambda/\Lambda$ is 2-dimensional over k: the torsion subgroup $T(\chi)[\lambda]$ gives a k-line in $\lambda^{-1}\Lambda/\Lambda$, whose quotient is isomorphic to $\Lambda/\lambda\Lambda$). We know that $\lambda^{-1}(a)$ generates a ramified extension of $\mathbb{Q}_2$. On the other hand, for any $b \in T(\mathbb{Q}_4)$, $\lambda^{-1}(\mathbb{N}(b)) = \lambda'(\sqrt{\mathbb{N}(b)})$, where λ' is an integral ideal of $\mathcal{O}$ such that $\lambda\lambda' = (2)$. Since $\mathbb{Q}_2(\sqrt{\mathbb{N}(b)})/\mathbb{Q}_2$ is unramified, we know that $\lambda^{-1}(\mathbb{N}(b))$ generates an unramified extension of $\mathbb{Q}_2$. Therefore, a is not of the form $\mathbb{N}(b)$, as desired.

Finally, in cases (1), (2), (4) and (5), we have $\mathcal{L}_v = \mathcal{L}_v(E)$ and the claim $\mathcal{L}_v = \mathcal{L}_v^\perp$ follows from the local Tate duality for E. In case (3), the claim $\mathcal{L}_v = \mathcal{L}_v^\perp$ is clear since $H^1(\mathbb{Q}_v, V)$ is 2-dimensional. □

Remark 6.7. When Assumption 2.1(4) is not satisfied, it is possible that $\mathcal{L}_2(E) \neq \mathcal{L}_2(A)$ (see Remark 7.3).

7. Rank lowering

Lemma 7.1. *Suppose that $\mathcal{L}$ and $\mathcal{L}'$ are two collections of local conditions. Let w be a place of $\mathbb{Q}$.*

(1) *Assume that $\mathcal{L}_v = \mathcal{L}'_v = \mathcal{L}_v^\perp$ for all $v \neq w$. Then* $\dim H^1_{\mathcal{L}}(V)$ *and* $\dim H^1_{\mathcal{L}'}(V)$ *differ by at most* $\frac{1}{2}\dim H^1(\mathbb{Q}_w, V)$.

(2) *If we further assume that:*

   (a) *$H^1(\mathbb{Q}_w, V)$ is 2-dimensional;*

   (b) *$\mathcal{L}_w$, $\mathcal{L}'_w$ are distinct lines;*

   (c) $\mathrm{res}_w(H^1_{\mathcal{L}}(V)) \neq 0$,

   then we have

$$\dim H^1_{\mathcal{L}'}(V) = \dim H^1_{\mathcal{L}}(V) - 1.$$

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

Proof. (1) Define the strict local conditions $\mathcal{S}$ by $\mathcal{S}_v = \mathcal{L}_v$ for $v \neq w$ and $\mathcal{S}_w = 0$. Similarly, define the relaxed local conditions $\mathcal{R}$ by $\mathcal{R}_v = \mathcal{L}_v$ for $v \neq w$ and $\mathcal{R}_w = H^1(\mathbb{Q}_w, V)$. Then we have

$$H^1_{\mathcal{S}}(V) \subseteq H^1_{\mathcal{L}}(V) \subseteq H^1_{\mathcal{R}}(V), \quad H^1_{\mathcal{S}}(V) \subseteq H^1_{\mathcal{L}'}(V) \subseteq H^1_{\mathcal{R}}(V).$$

The assumptions imply that $\mathcal{R}^\perp = \mathcal{S}$. By [DDT97, Theorem 2.18], we can compare the dual Selmer groups:

$$\frac{\#H^1_{\mathcal{S}}(V)}{\#H^1_{\mathcal{R}}(V)} = \prod_v \frac{\#\mathcal{S}_v}{\#H^0(\mathbb{Q}_v, V)}, \quad \frac{\#H^1_{\mathcal{R}}(V)}{\#H^1_{\mathcal{S}}(V)} = \prod_v \frac{\#\mathcal{R}_v}{\#H^0(\mathbb{Q}_v, V)}.$$

It follows that

$$\dim H^1_{\mathcal{R}}(V) - \dim H^1_{\mathcal{S}}(V) = \frac{1}{2}(\dim \mathcal{R}_w - \dim \mathcal{S}_w) = \frac{1}{2}\dim H^1(\mathbb{Q}_w, V).$$

So, the first claim is proved.

(2) Let $c_1, c_2 \in H^1_{\mathcal{L}}(V)$; then

$$\sum_v \langle \mathrm{res}_v(c_1), \mathrm{res}_v(c_2)\rangle_v = 0$$

by global class field theory. The assumption that $\mathcal{L}_v = \mathcal{L}_v^\perp$ implies that

$$\langle \mathrm{res}_v(c_1), \mathrm{res}_v(c_2)\rangle_v = 0, \quad v \neq w.$$

Hence, $\langle \mathrm{res}_w(c_1), \mathrm{res}_w(c_2)\rangle_w = 0$ as well. It follows that $\mathrm{res}_w(H^1_{\mathcal{L}}(V))$ is a totally isotropic subspace of $H^1(\mathbb{Q}_w, V)$ for the pairing $\langle\ ,\ \rangle_w$. The same argument shows that $\mathrm{res}_w(H^1_{\mathcal{L}'}(V))$ and $\mathrm{res}_w(H^1_{\mathcal{R}}(V))$ are also totally isotropic subspaces of $H^1(\mathbb{Q}_w, V)$. The isotropic subspaces are isotropic lines or zero by (a). Now (c) implies that $\mathrm{res}_w(H^1_{\mathcal{L}}(V))$ must be the line $\mathcal{L}_w \subseteq H^1(\mathbb{Q}_w, V)$. Thus, $\mathrm{res}_w(H^1_{\mathcal{R}}(V))$ must also be $\mathcal{L}_w$, as it contains $\mathrm{res}_w(H^1_{\mathcal{L}}(V))$. We thus know that $H^1_{\mathcal{L}}(V) = H^1_{\mathcal{R}}(V)$. Notice that

$$\mathrm{res}_w(H^1_{\mathcal{L}'}(V)) \subseteq \mathcal{L}'_w \cap \mathrm{res}_w(H^1_{\mathcal{R}}(V)) = \mathcal{L}'_w \cap \mathcal{L}_w,$$

which is zero by (b); we know that $H^1_{\mathcal{L}'}(V) = H^1_{\mathcal{S}}(V)$. The first part tells us that

$$\dim H^1_{\mathcal{R}}(V) - \dim H^1_{\mathcal{S}}(V) = 1.$$

So, the desired result is proved. □

Corollary 7.2. *Suppose that A is obtained from E via level raising at one prime q. Then* $\dim \mathrm{Sel}(A)$ *and* $\dim \mathrm{Sel}(E)$ *differ by at most* 1 *(respectively* 2*) when* Frob_q *is of order* 2 *(respectively* 1*) acting on* V*.*

Proof. This follows immediately from Lemmas 7.1(1), 6.6 and 6.5. □

Remark 7.3. The conclusion of Corollary 7.2 may fail when Assumption 2.1(4) is not satisfied due to the uncertainty of the local conditions at 2. For example, the elliptic curve $E = 2351a1 : y^2 + xy + y = x^3 - 5x - 5$ has trivial $\bar{\rho}|_{G_{\mathbb{Q}_2}}$. The elliptic curve $A = 25861i1 : y^2 + xy + y = x^3 + x^2 - 17x + 30$ is obtained from E via level raising at $q = 11$. One can compute that Frob_q has order 2 but $\dim \mathrm{Sel}(E) = 0$ and $\dim \mathrm{Sel}(A) = 2$ differ by 2.

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

Recall that $L = \mathbb{Q}(E[2])$. The inflation–restriction exact sequence gives us

$$0 \to H^1(L/\mathbb{Q}, V) \to H^1(\mathbb{Q}, V) \to H^1(L, V)^{\mathrm{Gal}\,(L/\mathbb{Q})} \to H^2(L/\mathbb{Q}, V).$$

Since V is the irreducible 2-dimensional representation of $\mathrm{Gal}\,(L/\mathbb{Q}) \cong S_3$, we have $H^1(L/\mathbb{Q}, V) = H^2(L/\mathbb{Q}, V) = 0$. Since G_L acts trivially on V, we know that $H^1(L, V) = \mathrm{Hom}(G_L, V)$. Therefore, we obtain an isomorphism

$$H^1(\mathbb{Q}, V) \cong \mathrm{Hom}\,(G_L, V)^{S_3}.$$

This allows us to view $c \in H^1(\mathbb{Q}, V)$ as a homomorphism $f : G_L \to V$ that is equivariant under the S_3-action. Namely, for any $g \in G_{\mathbb{Q}}$, $h \in G_L$, we have

$$f(ghg^{-1}) = \bar{g} \cdot f(h),$$

where $\bar{g}$ is the image of g in $\mathrm{Gal}\,(L/\mathbb{Q}) \cong S_3$.

LEMMA 7.4. *Let $c_1, \ldots, c_r \in H^1(\mathbb{Q}, V)$ be linearly independent elements. Let $f_1, \ldots, f_r : G_L \to V$ be the corresponding homomorphisms. Then the homomorphism*

$$f : G_L \to V^r, \quad g \mapsto (f_1(g), \ldots, f_r(g))$$

is surjective.

Proof. Since f_i is S_3-equivariant, we know that the image of f is a S_3-subrepresentation of V^r and hence must be isomorphic to V^s for some $s \leqslant r$. Therefore,

$$f_i \in \mathrm{Hom}\,(G_L/\ker f, V)^{S_3} \cong \mathrm{Hom}\,(V^s, V)^{S_3}$$

lies in an s-dimensional space. But, since $\{c_i\}$ are linearly independent, the homomorphisms $\{f_i\}$ are also linearly independent; we know that $s \geqslant r$. The surjectivity follows. □

LEMMA 7.5. *Suppose that A is obtained from E via level raising. Suppose that* $\mathrm{Sel}(A) \neq 0$. *Then there exists a positive density set of primes w satisfying the following:*

(1) *$H^1(\mathbb{Q}_w, V)$ is 2-dimensional;*
(2) $\mathrm{res}_w\,(\mathrm{Sel}(A)) \neq 0$.

Proof. By Lemma 6.5, the first condition that $H^1(\mathbb{Q}_w, V)$ is 2-dimensional is equivalent to that $\mathrm{Frob}_w \in \mathrm{Gal}\,(L/\mathbb{Q}) \cong S_3$ has order 2.

Let $c \in \mathrm{Sel}(A) \subseteq H^1(\mathbb{Q}, V)$ be a non-zero class. Let $f : G_L \to V$ be the corresponding homomorphism. We claim that there exists $g \in G_{\mathbb{Q}}$ such that $\bar{g}$ has order 2 and $f(g^2) \neq 0$. Take any transposition in S_3 and lift it to some $g \in G$. We are done if $f(g^2) \neq 0$. Otherwise, since V is a 2-dimensional irreducible representation of S_3, we know that there exists $v \in V$ such that $\bar{g} \cdot v + v \neq 0$. By Lemma 7.4, we can choose $h \in G_L$ such that $f(h) = v$. Let $g' = gh \in G_{\mathbb{Q}}$. Then $\bar{g}'$ has order 2 and

$$f(g'^2) = f(ghgh) = f(ghg^{-1} \cdot g^2 \cdot h) = \bar{g} \cdot f(h) + f(g^2) + f(h) = \bar{g} \cdot f(h) + f(h).$$

Therefore, $f(g'^2) = \bar{g} \cdot v + v \neq 0$ and the claim is proved.

It follows from the previous claim and the Chebotarev density theorem that there exists a positive density set of primes w such that Frob_w has order 2 in $\mathrm{Gal}\,(L/\mathbb{Q})$ and $f(\mathrm{Frob}_w^2) \neq 0$. Let u be a prime of L over w. Since

$$H^1(L_u/\mathbb{Q}_w, V) = H^2(L_u/\mathbb{Q}_w, V) = 0,$$

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

we know that

$$\mathrm{res}_w : H^1(\mathbb{Q}, V) \to H^1(\mathbb{Q}_w, V)$$

can be identified as

$$\mathrm{Hom}\,(G_L, V)^{S_3} \to \mathrm{Hom}\,(G_{L_u}, V)^{\mathrm{Gal}\,(L_u/\mathbb{Q}_w)}, \quad f \mapsto f|_{G_{L_u}}$$

by restricting f to the decomposition group G_{L_u}. Therefore, $\mathrm{res}_w(c) = f|_{G_{L_u}} \neq 0$, as $f(\mathrm{Frob}_w^2) \neq 0$. This completes the proof. □

Proposition 7.6. *Suppose that A is obtained from E via level raising at primes $q_1, \ldots, q_m$ $(m \geqslant 0)$ such that, for any $i \leqslant m$:*

(1) *$H^1(\mathbb{Q}_{q_i}, V)$ is 2-dimensional;*
(2) *$\varepsilon_i = \varepsilon_i(A) = +1$; and*
(3) *$\dim \mathrm{Sel}(A) \geqslant 1$.*

Then there exists a positive density set of primes q_{m+1} and A' obtained from E via level raising at primes $q_1, \ldots, q_m, q_{m+1}$ such that:

(1) *$H^1(\mathbb{Q}_{q_{m+1}}, V)$ is 2-dimensional;*
(2) *$\varepsilon_i' = \varepsilon_i(A') = +1$ for any $i \leqslant m+1$; and*
(3) *$\dim \mathrm{Sel}(A') = \dim \mathrm{Sel}(A) - 1$.*

Proof. Lemma 7.5 ensures the existence of a positive density set of primes $w = q_{m+1}$ such that $H^1(\mathbb{Q}_w, V)$ is 2-dimensional and $\mathrm{res}_w(\mathrm{Sel}(A)) \neq 0$. For such w, we choose A' using Theorem 2.9 with the prescribed signs $\varepsilon_i = +1$ $(i \leqslant m+1)$. Then the local conditions $\mathcal{L} = \mathcal{L}(A)$ and $\mathcal{L}' = \mathcal{L}(A')$ satisfy $\mathcal{L}_v = \mathcal{L}_v' = \mathcal{L}_v^\perp$ for $v \neq q_{m+1}$ by Lemma 6.6. For $w = q_{m+1}$, $\mathcal{L}_w$ and $\mathcal{L}_w'$ are distinct lines by Lemma 6.6 as well. Now we can apply Lemma 7.1 to conclude that $\dim \mathrm{Sel}(A') = \dim \mathrm{Sel}(A) - 1$. □

Theorem 7.7. *Suppose that $E/\mathbb{Q}$ satisfies Assumption 2.1. Then, for any given integer $0 \leqslant n < \dim \mathrm{Sel}(E)$, there exist infinitely many abelian varieties $A/\mathbb{Q}$ obtained from $E/\mathbb{Q}$ via level raising, such that*

$$\dim \mathrm{Sel}(A) = n.$$

Proof. It follows immediately from Proposition 7.6 by induction on the number of level raising primes m. □

8. Rank raising

To raise the rank, we need more refined control over the local conditions. For this purpose, we not only need the bilinear pairing $\langle\ ,\rangle_v$, but also a quadratic form Q_v giving rise to it. To define Q_v, first recall that the line bundle $\mathcal{L} = \mathcal{O}_E(2\infty)$ on E induces a degree 2 map

$$E \to \mathbb{P}^1 = \mathbb{P}(H^0(E, \mathcal{L})).$$

For $P \in E$, let τ_P be the translation by P on E. Since for $P \in E[2]$, $\tau_P^*\mathcal{L} \cong \mathcal{L}$, the translation by $E[2]$ induces an action of $E[2]$ on $\mathbb{P}^1$, i.e. a homomorphism $E[2] \to \mathrm{PGL}_2$. The short exact sequence

$$0 \to \mathbb{G}_m \to \mathrm{GL}_2 \to \mathrm{PGL}_2 \to 0$$

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

induces the connecting homomorphism in non-abelian Galois cohomology

$$H^1(\mathbb{Q}, \mathrm{PGL}_2) \to H^2(\mathbb{Q}, \mathbb{G}_m).$$

DEFINITION 8.1. We define Q to be the composition

$$Q : H^1(\mathbb{Q}, E[2]) \to H^1(\mathbb{Q}, \mathrm{PGL}_2) \to H^2(\mathbb{Q}, \mathbb{G}_m).$$

For a place v of $\mathbb{Q}$, we denote its restriction by

$$Q_v : H^1(\mathbb{Q}_v, E[2]) \to H^1(\mathbb{Q}_v, \mathrm{PGL}_2) \to H^2(\mathbb{Q}_v, \mathbb{G}_m).$$

By local class field theory, $H^2(\mathbb{Q}_v, \mathbb{G}_m) \cong \mathbb{Q}/\mathbb{Z}$ and so Q_v takes values in $H^2(\mathbb{Q}_v, \mathbb{G}_m)[2] \cong \mathbb{Z}/2\mathbb{Z}$. By [O'Ne02, § 4], Q_v is a quadratic form and extending scalars we obtain a quadratic form

$$Q_v : H^1(\mathbb{Q}_v, V) \to k,$$

whose associated bilinear form is given by $\langle\ ,\ \rangle_v$.

DEFINITION 8.2. We say that a subspace $W \subseteq H^1(\mathbb{Q}_v, V)$ is *totally isotropic for* Q_v if $Q_v|_W = 0$. We say that W is *maximal totally isotropic* if it is totally isotropic and $W = W^\perp$.

Remark 8.3. The local condition $\mathcal{L}_v = \mathcal{L}_v(E)$ is maximal totally isotropic for Q_v by [PR12, Proposition 4.11] (this is also implicit in [O'Ne02, Proposition 2.3]).

Remark 8.4. As $\mathrm{char}(k) = 2$, the requirement that $Q_v|_W = 0$ is stronger than $\langle\ ,\ \rangle_v|_W = 0$. For example, if $\dim H^1(\mathbb{Q}_v, V) = 2$, then all three lines in $H^1(\mathbb{Q}_v, V)$ are isotropic for $\langle\ ,\ \rangle_v$, but only two of them are isotropic for Q_v (since $(H^1(\mathbb{Q}_v, V), Q_v)$ is isomorphic to (k^2, xy) as quadratic spaces).

We replace the role of the bilinear form $\langle\ ,\ \rangle_v$ by the quadratic form Q_v and obtain the following more refined result analogous to Lemma 7.1.

LEMMA 8.5. *Suppose that $\mathcal{L}$ and $\mathcal{L}'$ are two collections of local conditions. Let w be a place of $\mathbb{Q}$. Assume that:*

(1) *$\mathcal{L}_v = \mathcal{L}'_v$ are maximal totally isotropic for Q_v (for any $v \neq w$);*
(2) *$H^1(\mathbb{Q}_w, V)$ is 2-dimensional;*
(3) *$\mathcal{L}_w$, $\mathcal{L}'_w$ are distinct lines and are both isotropic for Q_w.*

Then

$$\dim H^1_{\mathcal{L}'}(V) = \dim H^1_{\mathcal{L}}(V) \pm 1.$$

Moreover, $\mathrm{res}_w(H^1_{\mathcal{L}}(V)) = 0$ *if and only if*

$$\dim H^1_{\mathcal{L}'}(V) = \dim H^1_{\mathcal{L}}(V) + 1.$$

Proof. By the proof of Lemma 7.1(1), we obtain that

$$H^1_{\mathcal{S}}(V) \subseteq H^1_{\mathcal{L}}(V) \subseteq H^1_{\mathcal{R}}(V), \quad H^1_{\mathcal{S}}(V) \subseteq H^1_{\mathcal{L}'}(V) \subseteq H^1_{\mathcal{R}}(V)$$

and

$$\dim H^1_{\mathcal{R}}(V) = \dim H^1_{\mathcal{S}}(V) + 1,$$

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

since $\dim H^1(\mathbb{Q}_w, V) = 2$. By global class field theory, for any class $c \in H^1(\mathbb{Q}, V)$, we have

$$\sum_v Q_v(\mathrm{res}_v(c)) = 0.$$

The assumption that $\mathcal{L}_v$ is totally isotropic for Q_v (for any $v \neq w$) implies that $Q_w(\mathrm{res}_w(c)) = 0$ for any $c \in H^1_{\mathcal{L}}(V)$. In other words, the image $\mathrm{res}_w(H^1_{\mathcal{L}}(V))$ is a totally isotropic subspace for Q_w. Similarly, the images of $H^1_{\mathcal{L}'}(V)$, $H^1_{\mathcal{R}}(V)$ under res_w are all totally isotropic subspaces for Q_w. Since $H^1_{\mathcal{R}}(V) \neq H^1_{\mathcal{S}}(V)$ and $H^1(\mathbb{Q}_w, V)$ is 2-dimensional, we know that $\mathrm{res}_w(H^1_{\mathcal{R}}(V))$ must be an isotropic line for Q_w. But there are exactly two isotropic lines for Q_w (see Remark 8.4), which must be $\mathcal{L}_w$ and $\mathcal{L}'_w$, since they are assumed to be distinct. When $\mathrm{res}_w(H^1_{\mathcal{L}}(V)) = \mathcal{L}_w$, it follows that $\mathrm{res}_w(H^1_{\mathcal{R}}(V)) = \mathcal{L}_w$ and

$$H^1_{\mathcal{R}}(V) = H^1_{\mathcal{L}}(V), \quad H^1_{\mathcal{S}}(V) = H^1_{\mathcal{L}'}(V).$$

When $\mathrm{res}\,(H^1_{\mathcal{L}}(V)) = 0$, it follows that $\mathrm{res}_w(H^1_{\mathcal{R}}(V)) = \mathcal{L}'_w$ and

$$H^1_{\mathcal{R}}(V) = H^1_{\mathcal{L}'}(V), \quad H^1_{\mathcal{S}}(V) = H^1_{\mathcal{L}}(V).$$

This finishes the proof. □

Lemma 8.6. *Suppose that $w \nmid 2N\infty$ is a prime such that $H^1(\mathbb{Q}_w, V)$ is 2-dimensional. Let $\mathcal{L}'_w = \mathrm{im}(H^1(\mathbb{Q}_w, W) \to H^1(\mathbb{Q}_w, V))$, where W is the unique $G_{\mathbb{Q}_w}$-stable line in V. If Frob_w^2 is sufficiently close 1 (depending only on E), then $\mathcal{L}'_w$ is an isotropic line for Q_w.*

Proof. By the proof of Lemma 6.6(3), we know that the line $\mathcal{L}'_w$ is a generator by the class represented by the cocycle $c(\sigma) = 0$, $c(\tau) = P$, where σ is a lift of Frob_w, τ is a generator of the tame quotient $\mathrm{Gal}\,(\mathbb{Q}_w^t/\mathbb{Q}_w^{\mathrm{ur}})$ and P is a generator of $E[2](\mathbb{Q}_w)$.

We provide an explicit way to compute its image under $Q_w : H^1(\mathbb{Q}_w, E[2]) \to H^1(\mathbb{Q}_w, \mathrm{PGL}_2)$. Recall that $H^1(\mathbb{Q}_w, \mathrm{PGL}_2)$ classifies forms of $\mathbb{P}^1$, i.e. algebraic varieties $S/\mathbb{Q}_w$ which become isomorphic to $\mathbb{P}^1$ over $\overline{\mathbb{Q}}_w$. For any cocycle c, the corresponding form S can be described as follows. As a set, $S = \mathbb{P}^1(\overline{\mathbb{Q}}_w)$. The Galois action of $g \in G_{\mathbb{Q}_w}$ on $x \in S$ is given by $g \cdot x = c(g) \cdot g(x)$. The cocycle c is the trivial class in $H^1(\mathbb{Q}_w, \mathrm{PGL}_2)$ if and only if $S(\mathbb{Q}_w) \neq \emptyset$.

For our specific cocycle $c(\sigma) = 0$, $c(\tau) = P$, the corresponding form S has a $\mathbb{Q}_w$-rational point if and only if there exists $x \in \mathbb{P}^1(\mathbb{Q}_w^t)$ such that

$$\sigma(x) = x, \quad P \cdot \tau(x) = x.$$

Suppose that E has a Weierstrass equation $y^2 = F(x)$, where $F(x) \in \mathbb{Q}(x)$ is a monic irreducible cubic polynomial. Let $\alpha_1, \alpha_2, \alpha_3$ be the three roots of $F(x)$. We fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_w$ and view α_i as elements in $\overline{\mathbb{Q}}_w$. Without loss of generality, we may assume that $\alpha_1 \in \mathbb{Q}_w$ and thus $P = (\alpha_1, 0)$. Then the action of P on $\mathbb{P}^1$ is an involution that swaps $\alpha_1 \leftrightarrow \infty$, $\alpha_2 \leftrightarrow \alpha_3$. One can compute explicitly that this involution is given by the linear fractional transformation

$$x \mapsto \frac{\alpha_1 x + (\alpha_2\alpha_3 - \alpha_1\alpha_2 - \alpha_1\alpha_3)}{x - \alpha_1}.$$

Therefore, $Q_w(c) = 0$ if and only if there exists $x \in \mathbb{P}^1(\mathbb{Q}_w^t)$ such that

$$\sigma(x) = x, \quad (\tau(x) - \alpha_1)(x - \alpha_1) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3). \tag{8.6.0}$$

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

Let u be the prime of L over w induced by our fixed embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_w$. When Frob_w^2 is sufficiently close to 1 (depending only on E), u splits in the quadratic extension $L(\sqrt{\alpha_1 - \alpha_2})/L$. Therefore, $\alpha_1 - \alpha_2 \in (L_u^\times)^2$. The element $(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)$, as the norm of $\alpha_1 - \alpha_2$ from $L_u^\times$ to $\mathbb{Q}_w^\times$, must lie in $(\mathbb{Q}_w^\times)^2$. Let $\mathbb{Q}_w(\sqrt{\pi})$ be the tamely ramified quadratic extension fixed by σ. Then the image of the norm map

$$\mathbb{N} : \mathbb{Q}_w(\sqrt{\pi})^\times \to \mathbb{Q}_w^\times, \quad y \mapsto y \cdot \tau(y)$$

has index two in $\mathbb{Q}_w^\times$ by local class field theory and thus contains $(\mathbb{Q}_w^\times)^2$. So, we can find $y \in \mathbb{Q}_w(\sqrt{\pi})^\times$ such that $\mathbb{N}(y) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)$. Now $x = y + \alpha_1$ satisfies (8.6.0) and hence $Q_w(c) = 0$. It follows that $\mathcal{L}'_w$ is an isotropic line for Q_w, as desired. □

LEMMA 8.7. *Suppose that A is obtained from E via level raising. Then there exists a positive density set of primes w satisfying the following.*

(1) *$H^1(\mathbb{Q}_w, V)$ is 2-dimensional.*

(2) *Let $\mathcal{L}'_w = \mathrm{im}(H^1(\mathbb{Q}_w, W) \to H^1(\mathbb{Q}_w, V))$, where W is the unique $G_{\mathbb{Q}_w}$-stable line in V. Then $\mathcal{L}'_w$ is an isotropic line for Q_w.*

(3) $\mathrm{res}_w(\mathrm{Sel}(A)) = 0$.

Proof. Observe that for primes w such that Frob_w is sufficiently close to the class of the complex conjugation (depending only on A and E), we have:

(1) $\mathrm{Frob}_w \in \mathrm{Gal}\,(L/\mathbb{Q})$ has order 2 since we assumed that $\Delta < 0$ (Remark 2.6). So, $H^1(\mathbb{Q}_w, V)$ is 2-dimensional by Lemma 6.5;
(2) $\mathcal{L}'_w$ is an isotropic line for Q_w, by Lemma 8.6;
(3) let $c_1, \ldots, c_r$ be a k-basis of $\mathrm{Sel}(A)$. Let $f_i : G_L \to V$ be the homomorphisms corresponding to c_i. Then $f_i(\mathrm{Frob}_w^2) = 0$ and hence $\mathrm{res}_w(c_i) = 0$ for any $i \leqslant r$. This is satisfied if Frob_w^2 is trivial on the field cut out by the homomorphisms $f_1, \ldots, f_r$, which is a condition depending only on A.

The Chebotarev density theorem now finishes the proof. □

PROPOSITION 8.8. *Suppose that A is obtained from E via level raising at primes $q_1, \ldots, q_m$ ($m \geqslant 0$) satisfying that for any $i \leqslant m$:*

(1) *$H^1(\mathbb{Q}_{q_i}, V)$ is 2-dimensional;*
(2) *$\varepsilon_i = \varepsilon_i(A) = +1$; and*
(3) *$\mathcal{L}_{q_i} = \mathcal{L}_{q_i}(A)$ is an isotropic line for Q_{q_i}.*

Then there exists a positive density set of primes q_{m+1} and A' obtained from E via level raising at primes $q_1, \ldots, q_m, q_{m+1}$ satisfying that:

(1) *$H^1(\mathbb{Q}_{q_{m+1}}, V)$ is 2-dimensional;*
(2) *$\varepsilon'_i = \varepsilon_i(A') = +1$ for any $i \leqslant m+1$;*
(3) *$\mathcal{L}'_{q_i} = \mathcal{L}_{q_i}(A')$ is an isotropic line for Q_{q_i} for any $i \leqslant m+1$; and*
(4) $\dim \mathrm{Sel}(A') = \dim \mathrm{Sel}(A) + 1$.

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press

Proof. There exists a positive density of primes $w = q_{m+1}$ satisfying the conditions in Lemma 8.7. For such w, we choose A' using Theorem 2.9 such that $\varepsilon'_i = +1$ for any $i \leqslant m+1$. Let $\mathcal{L} = \mathcal{L}(A)$ and $\mathcal{L}' = \mathcal{L}(A')$. For $v = q_i$ $(i \leqslant m)$, we have $\dim H^1(\mathbb{Q}_v, V) = 2$ and $\mathcal{L}_v = \mathcal{L}'_v$ is an isotropic line for Q_v by the assumption and Lemma 6.6. Moreover, $\mathcal{L}_w$ and $\mathcal{L}'_w$ are distinct isotropic lines for Q_w by Lemmas 8.7 and 6.6. Then the conclusions (1)–(3) follow. Notice that $\mathcal{L}_v = \mathcal{L}'_v$ are maximal totally isotropic for $v \nmid q_1 \cdots q_{m+1}$ by Lemma 6.6 and Remark 8.3. We can apply Lemma 8.5 to obtain conclusion (4). □

Theorem 8.9. *Suppose that E satisfies Assumption 2.1. Then, for any given integer $n \geqslant \dim \mathrm{Sel}(E)$, there exist infinitely many abelian varieties A obtained from E via level raising, such that*

$$\dim \mathrm{Sel}(A) = n.$$

Proof. The statement for $n > \dim \mathrm{Sel}(E)$ follows immediately from Proposition 8.8 by induction on the number of level raising primes m. Applying Proposition 7.6 to A with $\dim \mathrm{Sel}(A) = \dim \mathrm{Sel}(E) + 1$ once, the statement for $n = \dim \mathrm{Sel}(E)$ also follows. □

Our main theorem (Theorem 1.4) then follows from Theorems 7.7 and 8.9.

Acknowledgements

We would like to thank Brian Conrad, Henri Darmon, Benedict Gross, Barry Mazur, Bjorn Poonen, Ken Ribet, Richard Taylor and Wei Zhang for helpful conversations or comments. We would also like to thank the referee for a careful reading and numerous suggestions. The examples in this article are computed using Sage [Ste13] and Magma [BCP97]. This material is also based upon work supported by the National Science Foundation under Grant No. 0932078000 while BVLH was in residence at the Mathematical Sciences Research Institute in Berkeley, California, during the Fall 2014 semester.

References

All14 P. B. Allen, *Modularity of nearly ordinary 2-adic residually dihedral Galois representations*, Compos. Math. **150** (2014), 1235–1346; MR 3252020.

BLGGT14 T. Barnet-Lamb, T. Gee, D. Geraghty and R. Taylor, *Potential automorphy and change of weight*, Ann. of Math. (2) **179** (2014), 501–609; MR 3152941.

BD99 M. Bertolini and H. Darmon, *Euler systems and Jochnowitz congruences*, Amer. J. Math. **121** (1999), 259–281; MR 1680333 (2001d:11060).

Boe G. Boeckle, *Deformations of Galois representations*, http://www.iwr.uni-heidelberg.de/groups/arith-geom/boeckle/Deformations-Barca.pdf.

BCP97 W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265; Computational algebra and number theory (London, 1993); MR 1484478.

BCDT01 C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* **Q***: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939, (electronic); MR 1839918 (2002d:11058).

BC O. Brinon and B. Conrad, *CMI summer school notes on p-adic Hodge theory*, http://math.stanford.edu/∼conrad/papers/notes.pdf.

Con97 B. Conrad, *The flat deformation functor*, in *Modular forms and Fermat's last theorem (Boston, MA, 1995)* (Springer, New York, 1997), 373–420; MR 1638486.

DDT97 H. Darmon, F. Diamond and R. Taylor, *Fermat's last theorem*, in *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)* (International Press, Cambridge, MA, 1997), 2–140; MR 1605752 (99d:11067b).

DT94a F. Diamond and R. Taylor, *Lifting modular mod l representations*, Duke Math. J. **74** (1994), 253–269; MR 1272977 (95e:11052).

DT94b F. Diamond and R. Taylor, *Nonoptimal levels of mod l modular representations*, Invent. Math. **115** (1994), 435–462; MR 1262939 (95c:11060).

Gee11 T. Gee, *Automorphic lifts of prescribed types*, Math. Ann. **350** (2011), 107–144; MR 2785764 (2012c:11118).

GP12 B. H. Gross and J. A. Parson, *On the local divisibility of Heegner points*, in *Number theory, analysis and geometry* (Springer, New York, 2012), 215–241; MR 2867919.

Kas99 P. L. Kassaei, *p-adic modular forms over Shimura curves over Q*, PhD thesis, Massachusetts Institute of Technology, ProQuest LLC, Ann Arbor, MI (1999); MR 2716881.

Kis09 M. Kisin, *Modularity of 2-adic Barsotti–Tate representations*, Invent. Math. **178** (2009), 587–634; MR 2551765 (2010k:11089).

Li15 C. Li, *2-Selmer groups and Heegner points on elliptic curves*, PhD thesis, Harvard University (2015).

MR10 B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), 541–575; MR 2660452 (2012a:11069).

Mil86 J. S. Milne, *Arithmetic duality theorems, vol. 1 of Perspectives in mathematics* (Academic Press, Boston, MA, 1986); MR 881804 (88e:14028).

O'Ne02 C. O'Neil, *The period-index obstruction for elliptic curves*, J. Number Theory **95** (2002), 329–339; MR 1924106 (2003f:11079).

Pil V. Pilloni, *The study of 2-dimensional p-adic Galois deformations in the ℓ not p case*, http://perso.ens-lyon.fr/vincent.pilloni/Defo.pdf.

PR12 B. Poonen and E. Rains, *Random maximal isotropic subspaces and Selmer groups*, J. Amer. Math. Soc. **25** (2012), 245–269; MR 2833483.

Ray74 M. Raynaud, *Schémas en groupes de type* $(p, \ldots, p)$, Bull. Soc. Math. France **102** (1974), 241–280; MR 0419467 (54 #7488).

Rib90 K. A. Ribet, *Raising the levels of modular representations*, in *Séminaire de théorie des nombres, Paris 1987–88*, Progress in Mathematics, vol. 81 (Birkhäuser, Boston, MA, 1990), 259–271; MR 1042773 (91g:11055).

Ser72 J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331; MR 0387283 (52 #8126).

SU14 C. Skinner and E. Urban, *The Iwasawa main conjectures for* GL_2, Invent. Math. **195** (2014), 1–277; MR 3148103.

Sno11 A. Snowden, *Singularities of ordinary deformation rings*, Preprint (2011), arXiv:1111.3654 [math.NT].

Ste13 W. A. Stein *et al.*, Sage mathematics software (ver. 5.11), The Sage Development Team, 2013, http://www.sagemath.org.

Tat97 J. Tate, *Finite flat group schemes*, in *Modular forms and Fermat's last theorem (Boston, MA, 1995)* (Springer, New York, 1997), 121–154; MR 1638478.

TW95 R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), 553–572; MR 1333036 (96d:11072).

Wil95 A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), 443–551; MR 1333035 (96d:11071).

Zar74 J. G. Zarhin, *Noncommutative cohomology and Mumford groups*, Math. Z. **15** (1974), 415–419; MR 0354612 (50 #7090).

Zha14 W. Zhang, *Selmer groups and the indivisibility of Heegner points*, Cambridge J. Math. **2** (2014), 191–253.

Bao V. Le Hung lhvietbao@googlemail.com
Department of Mathematics, University of Chicago, 5734 S. University Avenue, Chicago, IL 60637, USA

Chao Li chaoli@math.columbia.edu
Department of Mathematics, Columbia University, 2990 Broadway, New York, NY 10027, USA

https://doi.org/10.1112/S0010437X16007454 Published online by Cambridge University Press