JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Neil DUMMIGAN

On a conjecture of Watkins

Tome 18, n° 2 (2006), p. 345-355.

<http://jtnb.cedram.org/item?id=JTNB_2006__18_2_345_0>

Journal de Théorie des Nombres
de Bordeaux **18** (2006), 345-355

On a conjecture of Watkins

par Neil DUMMIGAN

Résumé. Watkins a conjecturé que si R est le rang du groupe des points rationnels d'une courbe elliptique E définie sur le corps des rationels, alors 2^R divise le degré du revêtement modulaire. Nous démontrons, pour une classe de courbes E choisie pour que ce soit le plus facile possible, que cette divisibilité découlerait de l'énoncé qu'un anneau de déformation 2-adique est isomorphe à un anneau de Hecke, et est un anneau d'intersection complète. Mais nous démontrons aussi que la méthode de Taylor, Wiles et autres pour démontrer de tels énoncés ne s'applique pas à notre situation. Il semble alors qu'on ait besoin d'une nouvelle méthode pour que cette approche de la conjecture de Watkins puisse marcher.

Abstract. Watkins has conjectured that if R is the rank of the group of rational points of an elliptic curve E over the rationals, then 2^R divides the modular parametrisation degree. We show, for a certain class of E, chosen to make things as easy as possible, that this divisibility would follow from the statement that a certain 2-adic deformation ring is isomorphic to a certain Hecke ring, and is a complete intersection. However, we show also that the method developed by Taylor, Wiles and others, to prove such statements, is necessarily inapplicable to our situation. It seems then that some new method is required if this approach to Watkins' conjecture is to work.

1. Introduction

For any elliptic curve E defined over $\mathbb{Q}$, of conductor N, there exists a finite morphism $\Phi : X_0(N) \to E$, defined over $\mathbb{Q}$, where $X_0(N)$ is the modular curve parametrising elliptic curves and cyclic subgroups of order N [BCDT]. In any isogeny class of elliptic curves over $\mathbb{Q}$, there is an optimal E with Φ of minimal degree, such that any other finite morphism from $X_0(N)$ to an elliptic curve in that isogeny class factors through this minimal one. This "modular degree" $\deg(\Phi)$ is an interesting invariant, and since the work of Zagier [Z] it has been computed by a variety of methods, summarised in the introduction to [Wa]. The modular degrees listed in

Manuscrit reçu le 24 mai 2005.

Cremona's tables [Cr] were obtained using modular symbols. Watkins has calculated many examples, using a method based on approximating the value of the symmetric square L-function at $s = 2$. On the basis of an examination of this numerical data, precipitated by an observation of Elkies on the first few rank 5 examples computed, Watkins made the following conjecture (Conjecture 4.1 of [Wa]).

Conjecture 1.1. *If* $R = \mathrm{rank}(E(\mathbb{Q}))$ *then* $2^R \mid \deg(\Phi)$.

He subsequently suggested that in fact the order of the 2-Selmer group should divide the modular degree, and this stronger assertion is certainly natural in view of the approach proposed in this note. (In fact Watkins has since suggested that something even stronger, involving also the size of the subgroup of Atkin-Lehner involutions through which Φ factors, may be true.) The idea is to use the $\mathbb{F}_2$-linear, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant "squaring" map from $E[2]$ to $\mathrm{Sym}^2 E[2]$ to induce a map from the 2-Selmer group of E to a certain subgroup of $H^1(\mathbb{Q}, \mathrm{Sym}^2 E[2])$, defined by local conditions. This is then identified with the (reduced) tangent space to a certain 2-adic deformation ring, parametrising strict equivalence classes of lifts of a certain type, of the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action on $E[2]$. This deformation ring ought to be isomorphic to a certain ring generated by Hecke operators, whose tangent space can be related to the modular degree, at least if we assume that it is a complete intersection. More precise details of this approach are described in subsequent sections.

The method of choice for identifying deformation rings with Hecke rings is that developed by Taylor and Wiles, simplified and extended by Faltings and Diamond [Wi],[TW],[D]. Other useful references describing the application to the semi-stable case of the Shimura-Taniyama-Weil conjecture are [DDT] and [dS]. In the application to the Shimura-Taniyama-Weil conjecture, one is dealing with ℓ-adic representations for odd prime ℓ, whereas here $\ell = 2$.

Dickinson [Di] has successfully applied the Taylor-Wiles method with $\ell = 2$, in order to help prove the modularity of certain icosahedral Galois representations [BDST]. He imposes certain conditions on a Galois representation with coefficients in an extension of $\mathbb{F}_2$, including the distinctness of the two characters arising from the semi-simplification of the restriction to a decomposition group at 2. This condition is not satisfied in our situation, where the coefficient field is $\mathbb{F}_2$.

Any application of the Taylor-Wiles method divides naturally into a "Galois theory" part and a "Hecke algebras" part. In our situation (under the conditions imposed in §2), it seems that the Hecke algebras part of the proof can be made to work, using ideas from [CDT] and [Di]. However, the Galois theory part cannot work, due ironically to the presence of the classes in $H^1(\mathbb{Q}, \mathrm{Sym}^2 E[2])$ whose construction was hinted at above. One might

say that the heart of the difficulty is the reducibility of $\mathrm{Sym}^2 E[2]$, which has the image of the squaring map as a non-trivial proper submodule.

A connection between hypothetical "$\mathcal{R} = \mathbb{T}$" results (with $\ell = 2$) and evenness of the modular degree also arises in recent work of Calegari and Emerton [CE]. They also encountered a problem in trying to apply the Taylor-Wiles method, but managed to bypass $\mathcal{R} = \mathbb{T}$ in proving their results, by a direct construction of a non-trivial element in the tangent space of a Hecke ring.

2. Local conditions

Let $E/\mathbb{Q}$ be an elliptic curve, of conductor N. We assume:

(1) N is even and squarefree;
(2) the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module $V := E[2]$ of 2-torsion points is ramified at all primes $p \mid N$ (equivalently, given (1), $\mathrm{ord}_p(\Delta)$ is odd for such p, where Δ is the minimal discriminant);
(3) E has no rational point of order 2;
(4) the action of complex conjugation on V is non-trivial (equivalently $E(\mathbb{R})$ is connected).

Let $\rho_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(T_2(E))$ be the 2-adic representation attached to E, where $T_2(E) = \varprojlim E[2^n]$ is the 2-adic Tate module, and let $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(V)$ be its reduction modulo 2. It follows from (3) and (4) above that $\overline{\rho}$ is surjective. Note that $\mathrm{Aut}(V) \simeq \mathrm{GL}_2(\mathbb{F}_2) \simeq D_6$, the dihedral group of order 6. The consequent absolute irreducibility of $\overline{\rho}$ is important for the construction of the universal deformation ring in §5, and the conditions (1) and (2) make the local deformation conditions easier. The conditions (1), (2) and (4) help in the proof of Lemma 4.1, and all four conditions help to make the calculation in §3 work out easily. (See also p.3 of [CE] for comments on the difficulty of getting such calculations to work without (4).) Though neither (3) nor (4) is, on its own, invariant under 2-isogeny, the irreducibility of $\overline{\rho}$, implied by the conditions (3) and (4) together, prevents the existence of 2-isogenies. Hence, if the conditions (1)-(4) hold for E, then they also hold for any elliptic curve in the same isogeny class as E.

Let $W := \mathrm{Sym}^2 V = \langle x \otimes x, y \otimes y, x \otimes y + y \otimes x \rangle$, where $\{x, y\}$ is any basis for V. Via the Weil pairing we have an isomorphism of $\mathbb{F}_2[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-modules $V \simeq V^*$. Under this isomorphism, $x \mapsto (y \mapsto 1, x \mapsto 0)$ and $y \mapsto (x \mapsto 1, y \mapsto 0)$. Hence W is isomorphic to the module attached to the representation $\mathrm{Ad}^0\overline{\rho}$, and elements of W may be identified with trace-zero 2-by-2 matrices over $\mathbb{F}_2$. Thus

$$x \otimes x \mapsto \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix},\ y \otimes y \mapsto \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},\ x \otimes y + y \otimes x \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

W^* is the $\mathbb{F}_2$-vector space of polynomial functions of degree 2 on V, thus $W^* = \langle x^2, y^2, xy\rangle$, where x and y are considered as elements of V^*, as above. We have, for example,

$$x^2 : x\otimes x \mapsto 0\times 0 = 0,\ y\otimes y \mapsto 1\times 1 = 1,\ x\otimes y + y\otimes x \mapsto 0\times 1 + 1\times 0 = 0.$$

$H^0(\mathbb{Q}, W) = \langle x\otimes y + y\otimes x\rangle$ and $H^0(\mathbb{Q}, W^*) = \langle x^2 + xy + y^2\rangle$. In fact $W \simeq W^*$ via

$$x\otimes x \mapsto y^2 + xy,\ y\otimes y \mapsto x^2 + xy,\ x\otimes y + y\otimes x \mapsto x^2 + xy + y^2.$$

Let $G_\infty := \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ and, for each prime number p, $G_p := \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. All of these are considered as subgroups of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, though this depends on choices of embeddings of $\overline{\mathbb{Q}}$ in $\mathbb{C}$ and the $\overline{\mathbb{Q}}_p$. Let I_p be the inertia subgroup at p.

Let Q be any finite set of primes, none dividing N. We define a Selmer group $H^1_Q(\mathbb{Q}, W) := \{c \in H^1(\mathbb{Q}, W) |\, \mathrm{res}_p(c) \in L_p\ \forall \text{ primes } p \le \infty\}$, where the subspaces $L_p \subset H^1(G_p, W)$ are defined as follows.

(1) $L_\infty := H^1(G_\infty, W)$. Its annihilator in $H^1(G_\infty, W^*)$ with respect to the local Tate duality pairing is $L_\infty^\perp = \{0\}$.
(2) Choose a basis $\{x, y\}$ for V such that G_2 and I_2 act on V via $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$. E has multiplicative reduction at 2, and consideration of the Tate parametrisation, and the fact that V is ramified at 2, shows that such a basis exists. Let $W^0 := \langle x\otimes x\rangle$ and
$$L_2 := \ker(H^1(G_2, W) \to H^1(G_2, W/W^0)).$$
(3) At $q \in Q$ let $L_q := H^1(G_q, W)$, so $L_q^\perp = \{0\}$.
(4) At all other finite primes p let $L_p = H^1(G_p/I_p, W^{I_p})$, and note that $L_p^\perp = H^1(G_p/I_p, (W^*)^{I_p})$.

Lemma 2.1. *$L_2 \simeq H^1(G_2, W^0)$, $\dim_{\mathbb{F}_2}(L_2) = 3$.*

Proof. Let $\{x, y\}$ be a basis as above for V. Take the cohomology, for G_2, of the exact sequence $0 \to W^0 \to W \to W/W^0 \to 0$. The H^0-part is exact:

$$0 \to \langle x\otimes x\rangle \to \langle x\otimes x, x\otimes y + y\otimes x\rangle \to \langle [x\otimes y + y\otimes x]\rangle \to 0,$$

so

$$L_2 \simeq H^1(G_2, W^0) \simeq \mathrm{Hom}(G_2, \mathbb{F}_2) \simeq \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2,$$

which is 3-dimensional over $\mathbb{F}_2$. □

Define filtrations $\{0\} \subset W^0 \subset W^1 \subset W$ and $\{0\} \subset (W^*)^0 \subset (W^*)^1 \subset W^*$ to be respectively $\{0\} \subset \langle x\otimes x\rangle \subset \langle x\otimes x, x\otimes y + y\otimes x\rangle \subset W$ and $\{0\} \subset \langle x^2\rangle \subset \langle x^2, xy\rangle \subset W^*$. Note that W^0 and $(W^*)^1$ form an annihilator pair, as do W^1 and $(W^*)^0$. We do not need the full strength of the following lemma, but include it for completeness.

Lemma 2.2. $L_2^\perp \simeq H^1(G_2, (W^*)^1)$, $\dim L_2^\perp = 4$.

Proof. By Tate's local duality and local Euler characteristic formula,

$$\frac{\#H^1(G_2, W)}{\#H^0(G_2, W)\#H^0(G_2, W^*)} = \#W,$$

so $\#H^1(G_2, W) = 2^7$. By Lemma 2.1, $L_2 = H^1(G_2, W^0)$ and is 3-dimensional. Since $H^1(G_2, (W^*)^1)$ annihilates $H^1(G_2, W^0)$, to prove part (1) it suffices to show that $\dim H^1(G_2, (W^*)^1) = 4$. (It is easy to prove that it injects into $H^1(G_2, W^*)$.)

Consider the cohomology for G_2 of the exact sequence $0 \to (W^*)^0 \to (W^*)^1 \to (W^*)^1/(W^*)^0 \to 0$. The H^i vanish for $i > 2$. The H^0 terms are all 1-dimensional, as are the H^2 terms (using Tate's local duality). The outer H^1 terms are both 3-dimensional, isomorphic to $\mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2$ as in the proof of Lemma 2.1. Since the alternating sum of the dimensions in the long exact sequence has to be zero, we find that indeed $\dim H^1(G_2, (W^*)^1) = 4$. □

3. A Selmer group calculation

Given a finite set of primes Q, none of which divides N, we have defined a Selmer group $H^1_Q(\mathbb{Q}, W)$. We may similarly define a dual Selmer group $H^1_{Q^*}(\mathbb{Q}, W^*)$ using the dual local conditions $L_v^\perp$, for all places v of $\mathbb{Q}$.

Proposition 3.1. *Let Q be a set of primes as above. Suppose that for each $q \in Q$ the arithmetic Frobenius element $\mathrm{Frob}_q \in G_q$ acts on V via an element $\overline{\rho}(\mathrm{Frob}_q)$ of order 3 (hence with eigenvalues $\alpha, \alpha+1$, where $\alpha^2+\alpha+1=0$). Then*

$$\frac{\#H^1_Q(\mathbb{Q}, W)}{\#H^1_{Q^*}(\mathbb{Q}, W^*)} = 2^r,$$

where $r = \#Q$.

Proof. By Theorem 2.18 of [DDT] (based on Proposition 1.6 of [Wi]),

$$\frac{\#H^1_Q(\mathbb{Q}, W)}{\#H^1_{Q^*}(\mathbb{Q}, W^*)} = \frac{\#H^0(\mathbb{Q}, W)}{\#H^0(\mathbb{Q}, W^*)} \prod_{\text{places of } \mathbb{Q}} \frac{\#L_v}{\#H^0(G_v, W)}.$$

Now $\#H^0(\mathbb{Q}, W) = \#H^0(\mathbb{Q}, W^*) = 2$. In the product we shall show that each $q \in Q$ contributes a factor of 2 (this is the reason for the condition on Frob_q), that the contributions from 2 and ∞ cancel out, and that the contributions from all other places are trivial.

(1) For $p \nmid 2Q\infty$, $\#L_p = \#H^1(G_p/I_p, W^{I_p}) = \#H^0(G_p, W)$.
(2) For $q \in Q$, Frob_q has eigenvalues $\alpha^2 = \alpha+1, (\alpha+1)^2 = \alpha$ and $\alpha(\alpha+1) = 1$ on $W \simeq W^*$, so $\#H^0(G_q, W^*) = 2$. By Tate's local

duality and Euler characteristic formula (noting that $\mathrm{ord}_q(\#W) = 0$), this is equal to $\frac{\#H^1(G_q,W)}{\#H^0(G_q,W)}$. In other words, $\frac{\#L_q}{\#H^0(G_q,W)} = 2$.

(3) $\#L_2 = 2^3$, by Lemma 2.1, and $\#H^0(G_2, W) = \#\langle x \otimes x, x \otimes y + y \otimes x\rangle = 2^2$, so $\frac{\#L_2}{\#H^0(G_2,W)} = 2$.

(4) Let $G_\infty = \langle\sigma\rangle$. Choose a basis $\{x, y\}$ for V such that σ acts as $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. (Recall that we assumed the action of σ on V to be non-trivial.) Then $\#H^0(G_\infty, W) = \#\langle x \otimes x + y \otimes y, x \otimes y + y \otimes x\rangle = 2^2$. If $f \in Z^1(G_\infty, W)$ (the group of 1-cocycles) then $f(\sigma^2) = 0$ so $f(\sigma)+f(\sigma)^\sigma = 0$, so $f(\sigma) \in H^0(G_\infty, W) = \langle x\otimes x+y\otimes y, x\otimes y+y\otimes x\rangle$. Modding out by the coboundaries $(\sigma - 1)W = \langle x \otimes x + y \otimes y\rangle$, we find that $\#H^1(G_\infty, W) = 2$ and $\frac{\#L_\infty}{\#H^0(G_\infty,W)} = \frac{1}{2}$.

□

4. Application of the squaring map

There is the usual descent map $\psi : E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow H^1(\mathbb{Q}, E[2]) \simeq H^1(\mathbb{Q}, V^*)$. Then there is the squaring map $s : V^* \to W^*$. This simply squares linear functions on V to produce quadratic functions on V. It is linear, because the characteristic is 2, and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-equivariant, because squaring fixes the coefficient field $\mathbb{F}_2$. There is an induced map $s_* : H^1(\mathbb{Q}, V^*) \to H^1(\mathbb{Q}, W^*)$, which is injective because $H^0(\mathbb{Q}, W^*)$ and $H^0(\mathbb{Q}, W^*/V^*)$ are both one-dimensional, and $H^0(\mathbb{Q}, V^*)$ is trivial by assumption.

Lemma 4.1. *If $P \in E(\mathbb{Q})$ then $s_*\psi(P) \in H^1_{\phi^*}(\mathbb{Q}, W^*)$.*

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

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

(2) Suppose that $p \mid N$ and $p \neq 2$. The point $P \in E(\mathbb{Q})$ is represented by some $v \in \overline{\mathbb{Q}}_p^\times$ on the Tate curve $\overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}$. This v lies at worst in the unramified quadratic extension of $\mathbb{Q}_p$, so is certainly fixed by the inertia subgroup I_p of G_p. We may choose $Q \in E(\overline{\mathbb{Q}}_p)$ with $2Q = P$ in such a way that Q is represented by $u \in \overline{\mathbb{Q}}_p^\times$ with $u^2 = v$. For any $\sigma \in I_p$, $\psi(P)(\sigma) = Q^\sigma - Q$ is represented by u^σ/u, whose square is $v^\sigma/v = 1$, so $\psi(P)(\sigma) \in \langle x\rangle$, where $\{x, y\} = \{-1, q^{1/2}\}$ is a basis for $V \simeq V^*$ with respect to which G_p and I_p act via $\left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$.

Since $p \neq 2$, I_p has a unique cyclic quotient of order 2. Let σ be a generator of this quotient. We have seen that the restriction of $\psi(P)$

to I_p is in the image of $H^1(I_p, \langle x\rangle) = \mathrm{Hom}(I_p, \langle x\rangle)$. But $x = y^\sigma - y$, so in fact $\psi(P)$ restricts to zero in $H^1(I_p, V^*)$, hence $\mathrm{res}_p(s_*\psi(P)) \in L_p^\perp$.

(3) For $p = 2$, if the reduction is split then we may prove as above that $\psi(P)(\sigma) \in \langle x\rangle$, where now σ may be anything in G_2. (It is still true to say that σ fixes v.) In the case of non-split reduction, it may be the case that $v^\sigma = v^{-1}$, then $u^\sigma = \pm u^{-1}$, and, taking into account the twist by the quadratic character, $Q^\sigma - Q$ is represented by $(u^\sigma)^{-1}/u = \pm 1 \in \langle x\rangle$. In either case, $\mathrm{res}_2(s_*\psi(P))$ is in the image of $H^1(G_2, (W^*)^0)$, which is contained in $L_2^\perp$ by (the easy part of) Lemma 2.2.

(4) Let $G_\infty = \langle\sigma\rangle$, acting by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with respect to a chosen basis $\{x, y\}$ of V^*. If $f \in Z^1(G_\infty, V^*)$ is a cocycle then, as in the proof of Proposition 3.1, $f(\sigma) \in (V^*)^{G_\infty} = \langle x + y\rangle$. But $x + y = x^\sigma - x$, so $H^1(G_\infty, V^*) = \{0\}$. Necessarily then $\mathrm{res}_\infty(\psi(P)) = 0$, so $\mathrm{res}_\infty(s_*\psi(P)) \in L_\infty^\perp = \{0\}$.

□

Proposition 4.2. *Let $R = \mathrm{rank}(E(\mathbb{Q}))$. Then $2^R \mid \#H^1_\phi(\mathbb{Q}, W)$.*

Proof. By Proposition 3.1 with $Q = \phi$, $\#H^1_\phi(\mathbb{Q}, W) = \#H^1_{\phi^*}(\mathbb{Q}, W^*)$, and Lemma 4.1 shows that 2^R divides the latter. □

5. Deformation rings and Hecke rings

Let $f = \sum_{n=1}^\infty a_n q^n$ be the newform attached to E. Let $\mathcal{C}$ be the category whose objects are complete noetherian local $\mathbb{Z}_2$-algebras with residue field $\mathbb{F}_2$ and whose morphisms are local $\mathbb{Z}_2$-algebra homomorphisms. Let $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_2)$ be as above. If $\mathcal{R} \in \mathcal{C}$, a lifting $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathcal{R})$ is said to be of type ϕ if and only if the following conditions hold.

(1) ρ is unramified outside N.

(2) $\rho|_{G_2} \sim \begin{pmatrix} \epsilon\lambda(a_2) & * \\ 0 & \lambda(a_2) \end{pmatrix}$, where ϵ is the restriction of the 2-adic cyclotomic character, and $\lambda(a_2)$ is the unramified character mapping Frob_2 to a_2.

(3) For any odd prime $p \mid N$, $\rho|_{G_p} \sim \begin{pmatrix} \epsilon\chi^{-1} & * \\ 0 & \chi \end{pmatrix}$, where χ is an unramified character.

(4) $\det\rho = \epsilon$.

Note that $a_2 = \pm 1$, according as the multiplicative reduction at 2 is split or non-split.

Lemma 5.1. (1) *There is a universal coefficient ring $\mathcal{R}_\phi$ and a universal deformation of $\overline{\rho}$ of type ϕ:*

$$\rho_\phi^{\mathrm{univ}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathcal{R}_\phi)$$

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

(2) *Let $\mathcal{P}_\mathcal{R}$ be the kernel of the homomorphism $\mathcal{R}_\phi \to \mathbb{Z}_2$ corresponding to the lifting ρ_E (associated to the 2-adic Tate module of E). There is a canonical isomorphism of $\mathbb{F}_2$-vector spaces*

$$\mathrm{Hom}_{\mathbb{F}_2}(\mathcal{P}_\mathcal{R}/\mathcal{P}_\mathcal{R}^2, \mathbb{F}_2) \simeq H^1_\phi(\mathbb{Q}, W).$$

Proof. The existence of a universal ring for deformations of $\overline{\rho}$ subject only to the condition (1) above follows from Proposition 2 in §20 of [M]. Note that $\overline{\rho}$ is absolutely irreducible, thanks to our assumptions about E. The determinant condition (4) is handled by §24 of [M], and (3) by §29 of [M]. The effects of these conditions on the description of $\mathrm{Hom}_{\mathbb{F}_2}(\mathcal{P}_\mathcal{R}/\mathcal{P}_\mathcal{R}^2, \mathbb{F}_2)$ are also dealt with in the aforementioned sections of [M]. That the condition (2) is a "deformation condition" may be proved by a similar argument to that used for (3), using its equivalence to $(\rho(h) - \epsilon(h))(\rho(h) - 1) = 0$ and $(\rho(h) - \epsilon(h))(\rho(g) - \lambda(a_2)(g)) = 0$ for all $h \in I_2$ and all $g \in G_2$. Its effect on the description of $\mathrm{Hom}_{\mathbb{F}_2}(\mathcal{P}_\mathcal{R}/\mathcal{P}_\mathcal{R}^2, \mathbb{F}_2)$ (matching the local condition L_2) is easy to prove. Note that we would not get the correct local subspace L_2 (with which the calculation in §3 works) without fixing the unramified character $\lambda(a_2)$. □

Let J be the largest abelian subvariety of $J_0(N)$ on which $U_2 = a_2$, where $J_0(N)$ is the Jacobian of the modular curve $X_0(N)$. Let $\mathbb{T}'$ be the commutative $\mathbb{Z}$-algebra generated by the Hecke operators T_p (for $p \nmid N$) and U_p (for $p \mid N$) acting as endomorphisms of J (via Picard functoriality). Let $\mathbb{T} = \mathbb{T}' \otimes_\mathbb{Z} \mathbb{Z}_2$. Let $\mathfrak{m}$ be that maximal ideal of $\mathbb{T}$ which is the kernel of the homomorphism from $\mathbb{T}$ to $\mathbb{F}_2$ such that $T_p \mapsto \overline{a_p}$ (for $p \nmid N$) and $U_p \mapsto \overline{a_p}$ (for $p \mid N$). Let $\mathbb{T}_\mathfrak{m}$ be the localisation of $\mathbb{T}$ at $\mathfrak{m}$. The following is a consequence of Proposition 2.4 of [Bz]. (Recall that $2 \,||\, N$ and $\overline{\rho}$ is ramified at 2, so the image of $\overline{\rho}|_{G_2}$ is not contained in the scalar matrices.)

Lemma 5.2. $\mathrm{Ta}_2(J)_\mathfrak{m}$ *is a free $\mathbb{T}_\mathfrak{m}$-module of rank* 2.

Since the Hecke operators commute with the Galois action on $\mathrm{Ta}_2(J)_\mathfrak{m}$, we have a representation $\rho_T : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{T}_\mathfrak{m})$. This is a lifting of $\overline{\rho}$, and is of type ϕ (see Theorem 13 and Proposition 14 of [Di] for a summary of what is needed for this). Hence it arises (up to strict equivalence) from $\rho_\phi^{\mathrm{univ}}$ via a homomorphism $\theta : \mathcal{R}_\phi \to \mathbb{T}_\mathfrak{m}$.

Conjecture 5.3. *θ is an isomorphism and $\mathcal{R}_\phi \simeq \mathbb{T}_\mathfrak{m}$ is a complete intersection.*

I am grateful to F. Calegari for pointing out that this is not a simple consequence of the conjectures of Fontaine-Mazur and Langlands, and we do not even know that $\mathcal{R}_\phi$ is torsion-free. We shall see next how to deduce Watkins' conjecture for E, from Conjecture 5.3. Let $\mathcal{P}_T$ be the kernel of the homomorphism $\theta_E : \mathbb{T}_\mathfrak{m} \to \mathbb{Z}_2$ such that $T_p \mapsto a_p$ (for $p \nmid N$) and $U_p \mapsto a_p$ (for $p \mid N$). Let $I = \mathrm{Ann}_{\mathbb{T}_\mathfrak{m}}(\mathcal{P}_T)$ and $\eta = \theta_E(I)$. As in Proposition 4.7 of [DDT], $\mathbb{T}_\mathfrak{m}$ may be identified with a manifestly reduced ring, then as in §4.4 of [DDT], η is non-zero and $\mathbb{Z}_2/\eta \simeq \mathbb{T}_\mathfrak{m}/(\mathcal{P}_T + I)$.

Proposition 5.4. *Let $E/\mathbb{Q}$ be an elliptic curve satisfying the conditions listed at the beginning of §2. Let $R = \mathrm{rank}(E(\mathbb{Q}))$ and let $\deg(\Phi)$ be the degree of an optimal modular parametrisation for the isogeny class of E. Conjecture 5.3 implies that $2^R \mid \deg(\Phi)$.*

Proof. We may take E to be optimal, with $\Phi : X_0(N) \to E$ of minimal degree. The morphism Φ factors through $\pi : J_0(N) \to E$, and we have also $\hat{\pi} : E \to J_0(N)$. The latter is an injection, and $\pi \cdot \hat{\pi}$ on E is multiplication by $\deg(\Phi)$. Let $\mathcal{P}'_T$ be the kernel of the homomorphism $\theta'_E : \mathbb{T}' \to \mathbb{Z}$ such that $T_p \mapsto a_p$ (for $p \nmid N$) and $U_p \mapsto a_p$ (for $p \mid N$). Then the image of $\mathcal{P}'_T$ is dense in $\mathcal{P}_T$, and $\hat{\pi}(E)$ is the connected part of the kernel of $\mathcal{P}'_T$ on J. Let $\mathbb{T}''$ be the commutative $\mathbb{Z}$-algebra generated by the Hecke operators T_p (for $p \nmid N$) and U_p (for $p \mid N$) acting as endomorphisms of $J_0(N)$. Let $\mathcal{P}''_T$ be the kernel of the homomorphism $\theta''_E : \mathbb{T}'' \to \mathbb{Z}$ such that $T_p \mapsto a_p$ (for $p \nmid N$) and $U_p \mapsto a_p$ (for $p \mid N$). By restriction from $J_0(N)$ to J, $\mathbb{T}''$ surjects onto $\mathbb{T}'$ and $\mathcal{P}''_T$ surjects onto $\mathcal{P}'_T$. Hence $\mathcal{P}'_T(J) \subset \mathcal{P}''_T(J_0(N))$, the kernel of the projection $\pi : J_0(N) \to E$.

According to Theorem 5.3 of [DDT], Conjecture 5.3 is equivalent to $\#(\mathcal{P}_\mathcal{R}/\mathcal{P}_\mathcal{R}^2) = \#(\mathbb{Z}_2/\eta)$. Combining this with Proposition 4.2 and Lemma 5.1 (2), we find that $2^R \mid \#(\mathbb{Z}_2/\eta) =: 2^S$, say. Since $\mathbb{Z}_2/\eta \simeq \mathbb{T}_\mathfrak{m}/(\mathcal{P}_T + I)$ we can write $2^S = p + i$ for some $p \in \mathcal{P}_T$ and $i \in I$, with $2 \nmid i$ in $\mathbb{T}_\mathfrak{m}$. Choose $S' \geq S$ such that $2^{S'-S}$ kills any 2-power torsion in the quotient of the kernel of $\mathcal{P}'_T$ on J by its connected part $\hat{\pi}(E)$.

By Lemma 5.2 we may choose $g' \in J[2^{S'}]$ such that $i(g')$ has exact order $2^{S'}$. Choose an element $p' \in \mathbb{T}'$, 2-adically approximating $p \in \mathbb{T}$ sufficiently closely that p and p' act the same way on $J[2^{S'}]$. In particular $p'(g') = p(g')$ (and therefore also $i'(g') = i(g')$, where $i' := 2^S - p'$). Since $\mathcal{P}_T$ annihilates I, $i'(g') = i(g')$ is in the kernel of $\mathcal{P}'_T$. Hence if $g := 2^{S'-S}g'$ then $i'(g)$ lies in $\hat{\pi}(E)$, say $i'(g) = \hat{\pi}(h)$, and has exact order 2^S. Also $i'(g) = i(g) = (2^S - p)(g) = -p(g) = -p'(g) \in \mathcal{P}'_T(J) \subset \ker(\pi)$. Hence h is a point of order 2^S on E, killed by $\pi \cdot \hat{\pi} = [\deg(\Phi)]$. This shows that $2^S \mid \deg(\phi)$, so $2^R \mid \deg(\Phi)$. □

6. A problem

Proposition 6.1. *Fix $n \geq 2$ and let $R = \mathrm{rank}(E(\mathbb{Q}))$. Let Q be a set of r primes such that, for each $q \in Q$, $q \nmid N$, $q \equiv 1 \pmod{2^n}$ and Frob_q acts non-trivially on V. Then $\#H^1_Q(\mathbb{Q}, W) \geq 2^{R+r}$.*

Proof. $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^n})/\mathbb{Q})$ contains a complex conjugation, which by assumption acts non-trivially on V, so $\mathrm{Frob}_q \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_{2^n}))$ must act on V through an element of order 3. Therefore Proposition 3.1 applies, and shows that it suffices to prove $2^R \mid \#H^1_{Q^*}(\mathbb{Q}, W^*)$. Lemma 4.1 shows that if $P \in E(\mathbb{Q})$ then $s_*\psi(P) \in H^1_{\phi^*}(\mathbb{Q}, W^*)$, where $\psi : E(\mathbb{Q})/2E(\mathbb{Q}) \to H^1(\mathbb{Q}, V^*)$ is the 2-descent map and $s : V^* \to W^*$ is the squaring map, hence that $2^R \mid \#H^1_{\phi^*}(\mathbb{Q}, W^*)$. We shall prove that $2^R \mid H^1_{Q^*}(\mathbb{Q}, W^*)$ by extending this to show that $s_*\psi(P) \in H^1_{Q^*}(\mathbb{Q}, W^*)$. It remains to show that, for all all $q \in Q$, $\mathrm{res}_q(s_*\psi(P)) = 0$.

Since $q \nmid N$, we know that $\mathrm{res}_q(\psi(P)) \in H^1(G_q/I_q, V^*)$, hence that $\mathrm{res}_q(s_*\psi(P)) \in H^1(G_q/I_q, W^*)$, so it suffices to prove that if f is a cocycle representing $s_*\psi(P)$ then $f(\mathrm{Frob}_q) \in (\mathrm{Frob}_q - 1)W^*$. But since Frob_q acts on V^* via an element of order 3, which may be represented by the matrix $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ with respect to some choice of basis, it is easy to check that $(\mathrm{Frob}_q - 1)W^* = s(V^*)$, which is exactly where $f(\mathrm{Frob}_q)$ must lie, since $s_*\psi(P) \in H^1(\mathbb{Q}, s(V^*)) \subset H^1(\mathbb{Q}, W^*)$. □

This proposition shows that, no matter how we try to choose the set Q of auxiliary primes, the dimension of the tangent space $H^1_Q(\mathbb{Q}, W)$ is greater than the r required for the Taylor-Wiles method (unless $R = 0$, a case which is not of any interest for our intended application).

Khare [K] has an alternative method for proving $\mathcal{R} = \mathbb{T}$ results, when N is square-free. He has applied it for $\ell > 5$. Again, one needs to show that a certain Selmer group $H^1_Q(\mathbb{Q}, W^*)$ (not quite his notation) is trivial. If we were to try to extend his method to $\ell = 2$, the set Q would comprise auxiliary primes q such that $\overline{\rho}(\mathrm{Frob}_q)$ has order 2 (c.f. [Bz]), the local conditions at primes in Q would be different, and the problem described above would not necessarily arise. But the reducibility of $\mathrm{Sym}^2 E[2]$, which lay behind the problem, appears nonetheless to cause a fundamental difficulty for this method too. In the papers [KR] and [R], on which [K] depends, the absolute irreducibility of $\mathrm{Ad}^0\overline{\rho}$ appears to be an important condition.

References

[BCDT] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*. J. Amer. Math. Soc. **14** (2001), 843–939.

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

[BDST] K. Buzzard, M. Dickinson, N. Shepherd-Barron, R. Taylor, *On icosahedral Artin representations*. Duke Math. J. **109** (2001), 283–318.

[CE] F. Calegari, M. Emerton, *Elliptic curves of odd modular degree*, preprint. `http://www.abel.math.harvard.edu/~fcale/`

[CDT] B. Conrad, F. Diamond, R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*. J. Amer. Math. Soc. **12** (1999), 521–567.

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

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

[dS] E. de Shalit, *Hecke rings and universal deformation rings*. Modular Forms and Fermat's Last Theorem, (G. Cornell, J. H. Silverman, G. Stevens, eds.), 421–445, Springer-Verlag, New York, 1997.

[D] F. Diamond, *The Taylor-Wiles construction and multiplicity one*. Invent. Math. **128** (1997), 379–391.

[Di] M. Dickinson, *On the modularity of certain 2-adic Galois representations*. Duke Math. J. **109** (2001), 319–382.

[K] C. Khare, *On isomorphisms between deformation rings and Hecke rings*. Invent. Math. **154** (2003), 199–222.

[KR] C. Khare, R. Ramakrishna, *Finiteness of Selmer groups and deformation rings*. Invent. Math. **154** (2003), 179–198.

[M] B. Mazur, *An introduction to the deformation theory of Galois representations*. Modular Forms and Fermat's Last Theorem, (G. Cornell, J. H. Silverman, G. Stevens, eds.), 243–311, Springer-Verlag, New York, 1997.

[R] R. Ramakrishna, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur*. Ann. Math. **156** (2002), 115–154.

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

[Wa] M. Watkins, *Computing the modular degree of an elliptic curve*. Experiment. Math. **11** (2002), 487–502.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*. Ann. Math. **141** (1995), 443–551.

[Z] D. Zagier, *Modular parametrizations of elliptic curves*. Canad. Math. Bull. **28** (1985), 372–384.

Neil Dummigan
University of Sheffield
Department of Pure Mathematics
Hicks Building
Hounsfield Road
Sheffield, S3 7RH, U.K.
E-mail: n.p.dummigan@shef.ac.uk
URL: `http://www.neil-dummigan.staff.shef.ac.uk/`