We shall explain how the following is a corollary of results of Wiles [W]:

**Theorem.** Suppose that $E$ is an elliptic curve over $\mathbb{Q}$ all of whose 2-division points are rational, i.e., an elliptic curve defined by

$$y^2 = (x - a)(x - b)(x - c)$$

for some distinct rational numbers $a$, $b$ and $c$. Then $E$ is modular.

Recall that Wiles proves that if $E$ is a semistable elliptic curve over $\mathbb{Q}$, then $E$ is modular [W, Thm. 0.4]. He begins by considering the Galois representations $\bar{\rho}_{E,3}$ (respectively, $\rho_{E,3}$) on the 3-division points (respectively, 3-adic Tate module) of $E$. If $\bar{\rho}_{E,3}$ is irreducible, then a theorem of Langlands and Tunnell is used to show that $\bar{\rho}_{E,3}$ arises from a modular form. Wiles deduces that $\rho_{E,3}$ also arises from a modular form by appealing to his results in [W, Ch. 3] and those with Taylor in [TW] to identify certain universal deformation rings as Hecke algebras. This suffices to prove that $E$ is modular if $\bar{\rho}_{E,3}$ is irreducible. When $\bar{\rho}_{E,3}$ is reducible, Wiles gives an argument which allows one to use $\rho_{E,5}$ instead.

In fact, Wiles’ results apply to a larger class of elliptic curves than those which are semistable [W, Thm. 0.3], and this was subsequently extended in [Di] to include all elliptic curves with semistable reduction at 3 and 5. Rubin and Silverberg noted that an elliptic curve as in the above theorem necessarily has a twist which is semistable outside 2, and hence, is modular by [Di, Thm. 1.2]. The purpose of this note is to explain how, by a refinement of their observation, the above theorem follows directly from Wiles’ work, without appealing to [Di].

**Lemma 1 (Rubin-Silverberg).** By at most a quadratic twist, an elliptic curve as in the theorem may be brought to the form

$$E : y^2 = x(x - A)(x + B)$$

for some nonzero integers $A$ and $B$ with $A$ and $B$ relatively prime, $B$ even and $A \equiv -1 \mod 4$. Let $C = A + B$. For odd primes $p$, the curve $E$ has
good reduction at $p$ if $p$ is prime to $ABC$ and multiplicative reduction at $p$ otherwise.

Proof. Note that a curve as in the theorem is isomorphic to one defined by equation (1) for some integers $A$ and $B$ with $AB(A + B) \neq 0$. Let $D = \gcd(A, B)$. Twisting by $\mathbb{Q}(\sqrt{D})$, we may assume that $A$ and $B$ are relatively prime. By translating $x$ or exchanging $A$ and $B$, we may assume that $B$ is even. Finally, if $A \equiv 1 \mod 4$, we twist again by $\mathbb{Q}(i)$.

The reduction type of $E$ for odd primes $p$ may be determined as in [Se2, §4] and [Si1, Ch. VII].

See [O, §I.1] for discussion of the reduction type and conductor of curves given by equation (1), but under certain restrictions in the case $p = 2$. See also [Da, Lemma 2.1] for a related case. We treat the reduction type at $p = 2$ in the following lemma.

Lemma 2. Suppose that $E$ is an elliptic curve over $\mathbb{Q}_2$ defined by the model (1), with $A \equiv -1 \mod 4$ and $B$ even. The reduction type, conductor exponent $f_2(E)$ and valuation of the minimal discriminant of $E$ are given by the following table:

<table>
<thead>
<tr>
<th>$\text{ord}_2(B)$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>$\nu \geq 5$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\text{Kodaira Symbol}$</td>
<td>$I_{III}$</td>
<td>$I_7^*$</td>
<td>$I_{III}^*$</td>
<td>$I_0$</td>
<td>$I_{2\nu - 8}$</td>
</tr>
<tr>
<td>$f_2(E)$</td>
<td>5</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>$\text{ord}<em>2(\Delta</em>{\text{min}})$</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>0</td>
<td>$2\nu - 8$</td>
</tr>
</tbody>
</table>

Proof. A twist of $E$ by the unramified extension $\mathbb{Q}_2(\sqrt{-A})$ affects neither reduction type nor conductor exponent, and provides a model of the form

$$y^2 = x(x + 1)(x + s)$$

with $\text{ord}_2(s) = \text{ord}_2(B) \geq 1$ and discriminant $\Delta = 16s^2(1 - s)^2$. For the convenience of the reader, we indicate the appropriate translations of model, depending on $\text{ord}_2(s)$, so that the explicit criteria of Tate’s algorithm [T] may be used.

If $\text{ord}_2(s) = 1$, then $\text{ord}_2(\Delta) = 6$. Put $y + x$ for $y$ in (2) to get

$$y^2 + 2xy = x^2 + sx^2 + s.$$ 

If $\text{ord}_2(s) = 2$, then $\text{ord}_2(\Delta) = 8$. Put $x + 2$ for $x$ in (3), to get

$$y^2 + 2xy + 4y = x^3 + (s + 6)x^2 + (5s + 12)x + (6s + 8).$$

If $\text{ord}_2(s) = 3$, use the model (3) with $\text{ord}_2(\Delta) = 10$. If $\text{ord}_2(s) \geq 4$, the model (3) is not minimal and may be reduced to

$$y^2 + xy = x^3 + \frac{s}{4}x^2 + \frac{s}{16}x.$$
with discriminant \( s^2(1-s)^2/256 \). Thus, (4) has good reduction if \( \text{ord}_2(s) = 4 \) and multiplicative reduction if \( \text{ord}_2(s) \geq 5 \). \( \square \)

To show that an elliptic curve over \( \mathbb{Q} \) is modular, we may replace it with one to which it is isomorphic over \( \overline{\mathbb{Q}} \). We may therefore assume that \( E \) is defined by equation (1) with \( A \) and \( B \) as in Lemma 1. If \( E \) has good or multiplicative reduction at \( p = 2 \), then \( E \) is semistable and we can conclude from [W, Thm. 0.4] that \( E \) is modular. In view of Lemma 2, we may therefore also assume, henceforth, that \( \text{ord}_2(B) = 1 \), 2 or 3.

Let \( \ell \) be an odd prime. Choose a basis for \( E[\ell] \), the kernel of multiplication by \( \ell \) on \( E \), and let \( \overline{\rho}_{E, \ell} \) denote the representation \( G_{\mathbb{Q}} \to \text{GL}_2(\mathbb{F}_\ell) \) defined by the action of \( G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) on \( E[\ell] \). For each prime \( p \), we fix an embedding \( \mathbb{Q} \leftrightarrow \mathbb{Q}_p \) and regard \( G_p = \text{Gal}(\mathbb{Q}_p/\mathbb{Q}_p) \) as a decomposition subgroup of \( G_{\mathbb{Q}} \) at a place over \( p \). Thus, \( \rho_{E, \ell}|_{G_p} \) is equivalent to the representation of \( G_p \) defined by its action on \( E[\ell](\mathbb{Q}_p) \). Let \( I_p \subset G_p \) denote the inertia group.

Recall the special role played by the prime \( \ell = 3 \) in Wiles’ approach. We simply write \( \rho \) for \( \rho_{E,3} \). If \( \rho \) is irreducible, then \( \rho \) is modular by the theorem of Langlands and Tunnell (see [W, Ch. 5]). Since \( E \) has good or multiplicative reduction at 3, we need only verify certain hypotheses on \( \rho \) in order to apply [W, Thm. 0.3] to conclude that \( E \) is modular. We shall see that if \( E \) has additive reduction at \( p = 2 \), then those hypotheses are satisfied, the crucial point being the verification of a local condition at \( p = 2 \). The irreducibility of \( \rho \) in this case is a byproduct of our verification. In fact, we have the following stronger result:

**Lemma 3.** If \( \text{ord}_2(B) = 1, 2 \) or 3 and \( \ell \) is an odd prime, then \( \overline{\rho}_{E, \ell}|_{I_2} \) is absolutely irreducible.

**Proof.** For the moment, consider the more general case of a representation \( \psi : I \to \text{SL}_2(\mathbb{F}_\ell) \), where \( I \) is the inertia group of a finite Galois extension of \( p \)-adic fields and \( \ell \neq p \) is a prime. Let \( b(\psi) \) denote the wild conductor exponent [Se2, §4.9]. If \( b(\psi) \) is odd, then \( \psi \) is irreducible. Indeed, were \( \psi \) to be reducible, it would be equivalent to a representation of the form

\[
\begin{pmatrix}
\chi & * \\
0 & \chi^{-1}
\end{pmatrix}
\]

But then, because \( b \) is integer-valued and additive on short exact sequences, \( b(\psi) = 2b(\chi) \) would be even.
Under the hypotheses of this lemma, the elliptic curve $E$ has additive reduction at 2 and odd conductor exponent $f_2(E) = 2 + b(\rho_{E, \ell}/I_2)$, independent of the choice of odd prime $\ell$. Since $\det \rho_{E, \ell}/G_2$ is an unramified character associated to $Q_2(\mu_\ell)$, the image of $I_2$ under $\rho_{E, \ell}$ is contained in $\text{SL}_2(\mathbb{F}_\ell)$. It follows that $\rho_{E, \ell}/I_2$ is absolutely irreducible.

Remark. When Lemma 3 applies, an analysis of the group structure of $\text{SL}_2(\mathbb{F}_3)$ shows that the image of wild ramification at $p = 2$ under $\rho$, and hence, $\rho_{E, \ell}$, for any odd $\ell$, is isomorphic to the quaternion group of order 8.

Under the hypotheses of Lemma 3, we see that even the restriction of $\rho = \rho_{E,3}$ to $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_3))$ is absolutely irreducible. Using Lemma 3, one can also easily check the local conditions on $\rho$ appearing as hypotheses in [W, Thm. 0.3]. Since it is left to the reader of [W] to verify that those local conditions are sufficient to apply the central result [W, Thm. 3.3], we shall explain directly how this is done in the case with which we are concerned. Again, we consider, more generally, $\rho_{E, \ell}$ for odd primes $\ell$.

First recall that $\rho_{E, \ell}$ is unramified at $p$ if $p \neq \ell$ is a prime of good reduction, i.e., if $p$ does not divide $\ell ABC$.

Next we recall how the Tate parametrization is used to describe $\rho_{E, \ell}/G_p$ for primes $p$ at which $E$ has multiplicative reduction (see [Se2, §2.9]). Let $F$ denote the unramified quadratic extension of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$. Then $E$ has split multiplicative reduction over $F$ and the Tate parametrization (see [Si2, §V.3]) provides an isomorphism

$$\mathbb{Q}_p^\times/q^2 \cong E(\mathbb{Q}_p)$$

of $\text{Gal}(\mathbb{Q}_p/F)$-modules for some $q \in \mathbb{Q}_p$ with $\text{ord}_p(q) > 0$. From this it follows that for each prime $\ell$, there is a filtration of $\text{Gal}(\mathbb{Q}_p/F)$-modules

$$0 \to \mathbb{Z}_\ell(1) \to T_\ell(E) \to \mathbb{Z}_\ell \to 0,$$

where $T_\ell(E)$ is the $\ell$-adic Tate module and $\mathbb{Z}_\ell(1) = \varprojlim \mu_{\ell^n}(\mathbb{Q}_p)$. One then checks that the representation of $G_p$ on $T_\ell(E)$ is equivalent to one of the form

$$\chi \otimes \begin{pmatrix} \epsilon & * \\ 0 & 1 \end{pmatrix}$$

where $\chi$ is either trivial or the unramified quadratic character of $G_p$, and $\epsilon$ is the cyclotomic character given by the action of $G_p$ on $\mathbb{Z}_\ell(1)$. It follows that the representation of $G_p$ on $E[\ell]$ is of this form as well, but with $\epsilon$ now defined by the action of $G_p$ on $\mu_\ell$.

Suppose now that $p \neq \ell$ is an odd prime dividing $ABC$. Then the above analysis of multiplicative reduction applies to $\rho_{E, \ell}/G_p$, and shows that $\rho_{E, \ell}$ is either unramified or type (A) at $p$ in the terminology of [W,
Suppose next that \( p = \ell \). If \( p \) divides \( ABC \), then the above analysis of multiplicative reduction shows that \( \bar{\rho}_{E, \ell} |_{G_p} \) is ordinary at \( p \) in the terminology of [W, Ch. 1]. If on the other hand \( p \) does not divide \( ABC \), then the elliptic curve \( E \) has good reduction at \( p \). In fact, the equation (1) defines an elliptic curve \( E \) over \( \mathbb{Z} \) such that \( E_{\mathbb{Q}} \) is isomorphic to \( E_{\mathbb{Q}} \) (see [Si2, §IV.5]). The kernel of multiplication by \( \ell \) on \( E \) is a finite flat group scheme \( E[\ell] \) over \( \mathbb{Z}_p \). The representation \( \bar{\rho}_{E, \ell} |_{G_p} \) is given by the action of \( G_p \) on \( E[\ell](\bar{\mathbb{Q}}_p) \), which we may identify with \( E[\ell](\bar{\mathbb{Q}}_p) \). In this sense, \( \bar{\rho}_{E, \ell} |_{G_p} \) arises from a finite flat group scheme over \( \mathbb{Z}_p \). Now \( \bar{\rho}_{E, \ell} |_{G_p} \) is reducible if and only if \( E \) has ordinary reduction at \( p \), i.e., if and only if \( E_{\mathbb{F}_p} \) is ordinary. In that case \( \bar{\rho}_{E, \ell} \) is ordinary at \( p \) in the sense of [W]. On the other hand, \( \bar{\rho}_{E, \ell} |_{G_p} \) is irreducible if and only if \( E_{\mathbb{F}_p} \) is supersingular, in which case \( \bar{\rho}_{E, \ell} \) is flat at \( p \) in the sense of [W, Ch. 1].

Finally, suppose that \( p = 2 \) and \( E \) has additive reduction at 2. Then \( \text{ord}_2(B) = 1, 2 \) or 3, and \( \bar{\rho}_{E, \ell} |_{I_2} \) is absolutely irreducible by Lemma 3. We claim that \( \bar{\rho}_{E, \ell} |_{G_2} \) is of type (C) at 2 in the terminology of Wiles [W, Ch. 1]. Recall that this means that \( H^1(G_2, W) = 0 \), where \( W \) is the \( G_2 \)-module of endomorphisms of \( E[\ell](\bar{\mathbb{Q}}_2) \) of trace zero. From the triviality of the local Euler characteristic ([Se1, Thm. II.5]), we have

\[
\#H^1(G_2, W) = \#H^0(G_2, W) \cdot \#H^2(G_2, W).
\]

By local Tate duality ([Se1, Thm. II.1]), we have

\[
\#H^2(G_2, W) = \#H^0(G_2, W^*)
\]

where \( W^* = \text{Hom}(W, \mu_\ell) \). Therefore, we wish to prove that \( H^0(G_2, W) \) and \( H^0(G_2, W^*) \) both vanish. But in fact \( H^0(I_2, W) \) and \( H^0(I_2, W^*) \) already vanish. Indeed, \( I_2 \) acts trivially on \( \mu_\ell \), from which we deduce that there is a (noncanonical) isomorphism \( W^* \cong W \) of \( I_2 \)-modules; hence, it suffices to show that \( H^0(I_2, W) = 0 \). Since \( I_2 \) acts absolutely irreducibly on \( \mathbb{F}_p^2 \), Schur’s lemma implies that the only \( I_2 \)-invariant endomorphisms of \( \mathbb{F}_p^2 \) are scalars. But the only scalar in \( W \) is zero.

Specializing to the case \( \ell = 3 \), we now conclude that the representation \( \rho_{E, 3} \) of \( G_\mathbb{Q} \) on \( T_3(E) \) arises from a modular form. Indeed, Wiles [W, Thm. 3.3] establishes an isomorphism between the universal deformation ring of type \( \mathcal{D} \) and the Hecke algebra \( T_{\mathcal{D}} \), where \( \mathcal{D} = (\cdot, \Sigma, \mathbb{Z}_3, \emptyset) \) with

- as flat or Selmer according to whether or not \( E \) has supersingular reduction at 3;
- \( \Sigma \) as the set of primes dividing \( 3ABC \).
Since $\rho_{E,3}$ defines a deformation of $\rho$ of type $D$, the universal property of the deformation ring thus provides a homomorphism $T_D \to \mathbb{Z}_3$ with the following property: for all $p$ not dividing $3ABC$, the Hecke operator $T_p$ is sent to $a_p = p + 1 - N_p$ where $N_p$ is the number of $\mathbb{F}_p$-points on the reduction of $E \mod p$.

The definition of $T_D$ ensures that this homomorphism arises from a normalized eigenform of weight two whose $p^{th}$ Fourier coefficient is $a_p$ for all such $p$. Hence $E$ is modular.

**Acknowledgements**

The authors are grateful to Kevin Buzzard, Ken Ribet and Karl Rubin for comments on an earlier version of this note.

**References**


D.P.M.M.S., 16 MILL LANE, UNIV. OF CAMBRIDGE, CAMBRIDGE, CB2 1SB, UK

E-mail address: f.diamond@pmms.cam.ac.uk

DEPARTMENT OF MATHEMATICS, QUEENS COLLEGE (CUNY), FLUSHING, NY 11367

E-mail address: kramer@qcvaxa.acc.qc.edu