Mathematical Research Letters **2**, 299–304 (1995)

MODULARITY OF A FAMILY OF ELLIPTIC CURVES

Fred Diamond and Kenneth Kramer

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

Theorem. *Suppose that E is an elliptic curve over $\mathbf{Q}$ 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 $\mathbf{Q}$, 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*

$$E:\ y^2 = x(x-A)(x+B) \tag{1}$$

for some nonzero integers A and B with A and B relatively prime, B even and $A \equiv -1 \bmod 4$. Let $C = A + B$. For odd primes p, the curve E has

Received March 24, 1995.

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 $\mathbf{Q}(\sqrt{D})$, 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 $A \equiv 1 \bmod 4$, we twist again by $\mathbf{Q}(i)$.

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 $\mathbf{Q}_2$ defined by the model (1), with $A \equiv -1 \bmod 4$ and B even. The reduction type, conductor exponent $\mathbf{f}_2(E)$ and valuation of the minimal discriminant of E are given by the following table:*

$\operatorname{ord}_2(B)$	1	2	3	4	$\nu \geq 5$
Kodaira Symbol	III	I_1^*	III^*	I_0	$I_{2\nu-8}$
$\mathbf{f}_2(E)$	5	3	3	0	1
$\operatorname{ord}_2(\Delta_{min})$	6	8	10	0	$2\nu - 8$

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

$$y^2 = x(x+1)(x+s) \tag{2}$$

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

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

$$y^2 + 2xy = x^3 + sx^2 + sx. \tag{3}$$

If $\operatorname{ord}_2(s) = 2$, then $\operatorname{ord}_2(\Delta) = 8$. 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 $\operatorname{ord}_2(s) = 3$, use the model (3) with $\operatorname{ord}_2(\Delta) = 10$. If $\operatorname{ord}_2(s) \geq 4$, the model (3) is not minimal and may be reduced to

$$y^2 + xy = x^3 + \frac{s}{4}x^2 + \frac{s}{16}x \tag{4}$$

with discriminant $s^2(1-s)^2/256$. Thus, (4) has good reduction if $\mathrm{ord}_2(s) = 4$ and multiplicative reduction if $\mathrm{ord}_2(s) \geq 5$. □

To show that an elliptic curve over $\mathbf{Q}$ is modular, we may replace it with one to which it is isomorphic over $\bar{\mathbf{Q}}$. 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 $\mathrm{ord}_2(B) = 1, 2$ or 3.

Let ℓ be an odd prime. Choose a basis for $E[\ell]$, the kernel of multiplication by ℓ on E, and let $\bar{\rho}_{E,\ell}$ denote the representation

$$G_{\mathbf{Q}} \to \mathrm{GL}_2(\mathbf{F}_\ell)$$

defined by the action of $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ on $E[\ell]$. For each prime p, we fix an embedding $\bar{\mathbf{Q}} \hookrightarrow \bar{\mathbf{Q}}_p$ and regard $G_p = \mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ as a decomposition subgroup of $G_{\mathbf{Q}}$ at a place over p. Thus, $\bar{\rho}_{E,\ell}|G_p$ is equivalent to the representation of G_p defined by its action on $E[\ell](\bar{\mathbf{Q}}_p)$. 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 ρ for $\bar{\rho}_{E,3}$. If ρ is irreducible, then ρ 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 ρ 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 ρ in this case is a byproduct of our verification. In fact, we have the following stronger result:

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

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

$$\begin{pmatrix} \chi & * \\ 0 & \chi^{-1} \end{pmatrix}.$$

But then, because $\mathbf{b}$ is integer-valued and additive on short exact sequences, $\mathbf{b}(\psi) = 2\mathbf{b}(\chi)$ would be even.

Under the hypotheses of this lemma, the elliptic curve E has additive reduction at 2 and odd conductor exponent $\mathbf{f}_2(E) = 2 + \mathbf{b}(\bar\rho_{E,\ell}|I_2)$, independent of the choice of odd prime ℓ. Since $\det\bar\rho_{E,\ell}|G_2$ is an unramified character associated to $\mathbf{Q}_2(\boldsymbol{\mu}_\ell)$, the image of I_2 under $\bar\rho_{E,\ell}$ is contained in $\mathrm{SL}_2(\mathbf{F}_\ell)$. It follows that $\bar\rho_{E,\ell}|I_2$ is absolutely irreducible. □

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

Under the hypotheses of Lemma 3, we see that even the restriction of $\rho = \bar\rho_{E,3}$ to $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}(\boldsymbol{\mu}_3))$ is absolutely irreducible. Using Lemma 3, one can also easily check the local conditions on ρ 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, $\bar\rho_{E,\ell}$ for odd primes ℓ.

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

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

$$\bar{\mathbf{Q}}_p^\times/q^{\mathbf{Z}} \cong E(\bar{\mathbf{Q}}_p)$$

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

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

where $T_\ell(E)$ is the ℓ-adic Tate module and $\mathbf{Z}_\ell(1) = \varprojlim \boldsymbol{\mu}_{\ell^n}(\bar{\mathbf{Q}}_p)$. 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 χ is either trivial or the unramified quadratic character of G_p and ϵ is the cyclotomic character given by the action of G_p on $\mathbf{Z}_\ell(1)$. It follows that the representation of G_p on $E[\ell]$ is of this form as well, but with ϵ now defined by the action of G_p on $\boldsymbol{\mu}_\ell$.

Suppose now that $p \neq \ell$ is an odd prime dividing ABC. Then the above analysis of multiplicative reduction applies to $\bar\rho_{E,\ell}|G_p$ and shows that $\bar\rho_{E,\ell}$ is either unramified or type (A) at p in the terminology of [W, Ch. 1]. (The first possibility occurs precisely when $\operatorname{ord}_p(ABC)$ is divisible by ℓ; see [Se2, §4].)

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 $\mathcal{E}$ over $\mathbf{Z}_p$ such that $\mathcal{E}_{\mathbf{Q}_p}$ is isomorphic to $E_{\mathbf{Q}_p}$ (see [Si2, §IV.5]). The kernel of multiplication by ℓ on $\mathcal{E}$ is a finite flat group scheme $\mathcal{E}[\ell]$ over $\mathbf{Z}_p$. The representation $\bar{\rho}_{E,\ell}|G_p$ is given by the action of G_p on $E[\ell](\bar{\mathbf{Q}}_p)$, which we may identify with $\mathcal{E}[\ell](\bar{\mathbf{Q}}_p)$. In this sense, $\bar{\rho}_{E,\ell}|G_p$ arises from a finite flat group scheme over $\mathbf{Z}_p$. 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 $\mathcal{E}_{\mathbf{F}_p}$ 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 $\mathcal{E}_{\mathbf{F}_p}$ 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 $\operatorname{ord}_2(B) = 1, 2$ 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 $E[\ell](\bar{\mathbf{Q}}_2)$ 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 $W^* = \operatorname{Hom}(W, \boldsymbol{\mu}_\ell)$. 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 $\boldsymbol{\mu}_\ell$, 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 $\bar{\mathbf{F}}_\ell^2$, Schur's lemma implies that the only I_2-invariant endomorphisms of $\bar{\mathbf{F}}_\ell^2$ 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 $G_{\mathbf{Q}}$ 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 $\mathbf{T}_{\mathcal{D}}$, where $\mathcal{D} = (\cdot, \Sigma, \mathbf{Z}_3, \emptyset)$ with

- $\cdot$ as flat or Selmer according to whether or not E has supersingular reduction at 3;
- Σ as the set of primes dividing $3ABC$.

Since $\rho_{E,3}$ defines a deformation of ρ of type $\mathcal{D}$, the universal property of the deformation ring thus provides a homomorphism $\mathbf{T}_{\mathcal{D}} \to \mathbf{Z}_3$ 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 $\mathbf{F}_p$-points on the reduction of E mod p.

The definition of $\mathbf{T}_{\mathcal{D}}$ 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

[Da] H. Darmon, *The equations* $x^n + y^n = z^2$ *and* $x^n + y^n = z^3$, Duke IMRN **10** (1993), 263–274.

[Di] F. Diamond, *On deformation rings and Hecke rings*, preprint.

[O] J. Oesterlé, *Nouvelles approches du "théorème" de Fermat*, Séminaire Bourbaki 694 (1987–88), Astérisque **161–162** (1988), 165–186.

[Se1] J. P. Serre, Cohomologie Galoisienne, 5^e éd, LNM **5**. Springer-Verlag, New York, 1994.

[Se2] ———, *Sur les représentations modulaires de degré* 2 *de* Gal $(\bar{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), 179–230.

[Si1] J. Silverman, The arithmetic of elliptic curves, GTM **106**, Springer-Verlag, New York, 1986.

[Si2] ———, Advanced topics in the arithmetic of elliptic curves, GTM **151**, Springer-Verlag, New York, 1994.

[T] J. T. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in Modular Functions of One Variable IV, LNM **476**, Springer-Verlag, New York, 1975.

[TW] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, to appear in Ann. Math.

[W] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, to appear in Ann. Math.

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