Annals of Mathematics, **142** (1995), 443–551

Modular elliptic curves and Fermat's Last Theorem

By Andrew Wiles*

For Nada, Clare, Kate and Olivia

> *Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*
>
> *Pierre de Fermat*

Introduction

An elliptic curve over **Q** is said to be modular if it has a finite covering by a modular curve of the form $X_0(N)$. Any such elliptic curve has the property that its Hasse-Weil zeta function has an analytic continuation and satisfies a functional equation of the standard type. If an elliptic curve over **Q** with a given j-invariant is modular then it is easy to see that all elliptic curves with the same j-invariant are modular (in which case we say that the j-invariant is modular). A well-known conjecture which grew out of the work of Shimura and Taniyama in the 1950's and 1960's asserts that every elliptic curve over **Q** is modular. However, it only became widely known through its publication in a paper of Weil in 1967 [We] (as an exercise for the interested reader!), in which, moreover, Weil gave conceptual evidence for the conjecture. Although it had been numerically verified in many cases, prior to the results described in this paper it had only been known that finitely many j-invariants were modular.

In 1985 Frey made the remarkable observation that this conjecture should imply Fermat's Last Theorem. The precise mechanism relating the two was formulated by Serre as the ε-conjecture and this was then proved by Ribet in the summer of 1986. Ribet's result only requires one to prove the conjecture for semistable elliptic curves in order to deduce Fermat's Last Theorem.

*The work on this paper was supported by an NSF grant.

The same results hold if the image of the projective representation $\tilde{\rho}_0$ associated to ρ_0 is isomorphic to A_4, S_4 or A_5.

Proof. (i) Let $G = \operatorname{im}\rho_0$ and let Z denote the center of G. Then we have a surjection $G' \longrightarrow (G/Z)'$ where the $'$ denotes the derived group. By Dickson's classification of the subgroups of $\mathrm{GL}_2(k)$ containing an element of order p, (G/Z) is isomorphic to $\mathrm{PGL}_2(k')$ or $\mathrm{PSL}_2(k')$ for some finite field k' of characteristic p or possibly to A_5 when $p = 3$, cf. [Di, §260]. In each case we can find, and then lift to G', an element of order m with $(m, p) = 1$ and $m \geq 3$, except possibly in the case $p = 3$ and $\mathrm{PSL}_2(\mathbf{F}_3) \simeq A_4$ or $\mathrm{PGL}_2(\mathbf{F}_3) \simeq S_4$. However in these cases $(G/Z)'$ has order divisible by 4 so the 2-Sylow subgroup of G' has order greater than 2. Since it has at most one element of exact order 2 (the eigenvalues would both be -1 since it is in the kernel of the determinant and hence the element would be $-I$) it must also have an element of order 4.

The argument in the A_4, S_4 and A_5 cases is similar.

(ii) Since ρ_0 is assumed absolutely irreducible, $G = \operatorname{im}\rho_0$ has no fixed line. We claim that the same then holds for the derived group G'. For otherwise since $G' \triangleleft G$ we could obtain a second fixed line by taking $\langle gv \rangle$ where $\langle v \rangle$ is the original fixed line and g is a suitable element of G. Thus G' would be contained in the group of diagonal matrices for a suitable basis and either it would be central in which case G would be abelian or its normalizer in $\mathrm{GL}_2(k)$, and hence also G, would have order prime to p. Since neither of these possibilities is allowed, G' has no fixed line.

By Dickson's classification of the subgroups of $\mathrm{GL}_2(k)$ containing an element of order p the image of $\operatorname{im}\rho_0$ in $\mathrm{PGL}_2(k)$ is isomorphic to $\mathrm{PGL}_2(k')$ or $\mathrm{PSL}_2(k')$ for some finite field k' of characteristic p or possibly to A_5 when $p = 3$. The only one of these with a quotient group of order p is $\mathrm{PSL}_2(\mathbf{F}_3)$ when $p = 3$. It follows that $p \nmid [G : G']$ except in this one case which we treat separately. So assuming now that $p \nmid [G : G']$ we see that G' contains a nontrivial unipotent element u. Since G' has no fixed line there must be another noncommuting unipotent element v in G'. Pick a basis for $\rho_0|_{G'}$ consisting of their fixed vectors. Then let τ be an element of $\mathrm{Gal}(\mathbf{Q}_\Sigma/\mathbf{Q})$ for which the image of $\rho_0(\tau)$ in G/G' is prescribed and let $\rho_0(\tau) = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then

$$\delta = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & s\alpha \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & \\ r\beta & 1 \end{pmatrix}$$

has $\det(\delta) = \det\rho_0(\tau)$ and $\operatorname{trace}\delta = s\alpha(ra\beta + c) + br\beta + a + d$. Since $p \geq 3$ we can choose this trace to avoid any two given values (by varying s) unless $ra\beta + c = 0$ for all r. But $ra\beta + c$ cannot be zero for all r as otherwise $a = c = 0$. So we can find a δ for which the ratio of the eigenvalues is not $\omega(\tau)$, $\det(\delta)$ being, of course, fixed.

Now suppose that $\operatorname{im}\rho_0$ does not have order divisible by p but that the associated projective representation $\widetilde{\rho_0}$ has image isomorphic to S_4 or A_5, so necessarily $p \neq 3$. Pick an element τ such that the image of $\rho_0(\tau)$ in G/G' is any prescribed class. Since this fixes both $\det \rho_0(\tau)$ and $\omega(\tau)$ we have to show that we can avoid at most two particular values of the trace for τ. To achieve this we can adapt our first choice of τ by multiplying by any element of G'. So pick $\sigma \in G'$ as in (i) which we can assume in these two cases has order 3. Pick a basis for ρ_0, by extending scalars if necessary, so that $\sigma \mapsto \left(\begin{smallmatrix}\alpha & \\ & \alpha^{-1}\end{smallmatrix}\right)$. Then one checks easily that if $\rho_0(\tau) = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)$ we cannot have the traces of all of τ, $\sigma\tau$ and $\sigma^2\tau$ lying in a set of the form $\{\mp t\}$ unless $a = d = 0$. However we can ensure that $\rho_0(\tau)$ does not satisfy this by first multiplying τ by a suitable element of G' since G' is not contained in the diagonal matrices (it is not abelian).

In the A_4 case, and in the $\mathrm{PSL}_2(\mathbf{F}_3) \simeq A_4$ case when $p = 3$, we use a different argument. In both cases we find that the 2-Sylow subgroup of G/G' is generated by an element z in the centre of G. Either a power of z is a suitable candidate for $\rho_0(\sigma)$ or else we must multiply the power of z by an element of G', the ratio of whose eigenvalues is not equal to 1. Such an element exists because in G' the only possible elements without this property are $\{\mp I\}$ (such elements necessarily have determinant 1 and order prime to p) and we know that $\#G' > 2$ as was noted in the proof of part (i). □

Remark. By a well-known result on the finite subgroups of $\mathrm{PGL}_2(\overline{\mathbf{F}}_p)$ this lemma covers all ρ_0 whose images are absolutely irreducible and for which $\widetilde{\rho_0}$ is not dihedral.

Let K_1 be the splitting field of ρ_0. Then we can view W_λ and W_λ^* as $\mathrm{Gal}(K_1(\zeta_p)/\mathbf{Q})$-modules. We need to analyze their cohomology. Recall that we are assuming that ρ_0 is absolutely irreducible. Let $\widetilde{\rho_0}$ be the associated projective representation to $\mathrm{PGL}_2(k)$.

The following proposition is based on the computations in [CPS].

PROPOSITION 1.11. *Suppose that ρ_0 is absolutely irreducible. Then*

$$H^1(K_1(\zeta_p)/\mathbf{Q}, W_\lambda^*) = 0.$$

Proof. If the image of ρ_0 has order prime to p the lemma is trivial. The subgroups of $\mathrm{GL}_2(k)$ containing an element of order p which are not contained in a Borel subgroup have been classified by Dickson [Di, §260] or [Hu, II.8.27] Their images inside $\mathrm{PGL}_2(k')$ where k' is the quadratic extension of k are conjugate to $\mathrm{PGL}_2(F)$ or $\mathrm{PSL}_2(F)$ for some subfield F of k', or they are isomorphic to one of the exceptional groups A_4, S_4, A_5.

Assume then that the cohomology group $H^1(K_1(\zeta_p)/\mathbf{Q}, W_\lambda^*) \neq 0$. Then by considering the inflation-restriction sequence with respect to the normal subgroup $\mathrm{Gal}(K_1(\zeta_p)/K_1)$ we see that $\zeta_p \in K_1$. Next, since the representation is (absolutely) irreducible, the center Z of $\mathrm{Gal}(K_1/\mathbf{Q})$ is contained in the diagonal matrices and so acts trivially on W_λ. So by considering the inflation-restriction sequence with respect to Z we see that Z acts trivially on ζ_p (and on W_λ^*). So $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ is a quotient of $\mathrm{Gal}(K_1/\mathbf{Q})/Z$. This rules out all cases when $p \neq 3$, and when $p = 3$ we only have to consider the case where the image of the projective representation is isomorphic as a group to $\mathrm{PGL}_2(F)$ for some finite field of characteristic 3. (Note that $S_4 \simeq \mathrm{PGL}_2(\mathbf{F}_3)$.)

Extending scalars commutes with formation of duals and H^1, so we may assume without loss of generality $F \subseteq k$. If $p = 3$ and $\#F > 3$ then $H^1(\mathrm{PSL}_2(F), W_\lambda) = 0$ by results of [CPS]. Then if $\widetilde{\rho_0}$ is the projective representation associated to ρ_0 suppose that $g^{-1} \operatorname{im} \widetilde{\rho_0}\, g = \mathrm{PGL}_2(F)$ and let $H = g\ \mathrm{PSL}_2(F) g^{-1}$. Then $W_\lambda \simeq W_\lambda^*$ over H and

$$(1.18) \qquad H^1(H, W_\lambda) \underset{F}{\otimes} \bar{F} \simeq H^1(g^{-1}Hg, g^{-1}(W_\lambda \underset{F}{\otimes} \bar{F})) = 0.$$

We deduce also that $H^1(\operatorname{im} \rho_0, W_\lambda^*) = 0$.

Finally we consider the case where $F = \mathbf{F}_3$. I am grateful to Taylor for the following argument. First we consider the action of $\mathrm{PSL}_2(\mathbf{F}_3)$ on W_λ explicitly by considering the conjugation action on matrices $\{A \in M_2(\mathbf{F}_3) : \operatorname{trace} A = 0\}$. One sees that no such matrix is fixed by all the elements of order 2, whence

$$H^1(\mathrm{PSL}_2(\mathbf{F}_3), W_\lambda) \simeq H^1(\mathbf{Z}/3, (W_\lambda)^{C_2 \times C_2}) = 0$$

where $C_2 \times C_2$ denotes the normal subgroup of order 4 in $\mathrm{PSL}_2(\mathbf{F}_3) \simeq A_4$. Next we verify that there is a unique copy of A_4 in $\mathrm{PGL}_2(\bar{\mathbf{F}}_3)$ up to conjugation. For suppose that $A, B \in \mathrm{GL}_2(\bar{\mathbf{F}}_3)$ are such that $A^2 = B^2 = I$ with the images of A, B representing distinct nontrivial commuting elements of $\mathrm{PGL}_2(\bar{\mathbf{F}}_3)$. We can choose $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ by a suitable choice of basis, i.e., by a suitable conjugation. Then B is diagonal or antidiagonal as it commutes with A up to a scalar, and as B, A are distinct in $\mathrm{PGL}_2(\bar{\mathbf{F}}_3)$ we have $B = \left(\begin{smallmatrix} 0 & -a^{-1} \\ a & 0 \end{smallmatrix}\right)$ for some a. By conjugating by a diagonal matrix (which does not change A) we can assume that $a = 1$. The group generated by $\{A, B\}$ in $\mathrm{PGL}_2(\mathbf{F}_3)$ is its own centralizer so it has index at most 6 in its normalizer N. Since $N/\langle A, B\rangle \simeq S_3$ there is a unique subgroup of N in which $\langle A, B\rangle$ has index 3 whence the image of the embedding of A_4 in $\mathrm{PGL}_2(\bar{\mathbf{F}}_3)$ is indeed unique (up to conjugation). So arguing as in (1.18) by extending scalars we see that $H^1(\operatorname{im} \rho_0, W_\lambda^*) = 0$ when $F = \mathbf{F}_3$ also. □

The following lemma was pointed out to me by Taylor. It permits most dihedral cases to be covered by the methods of Chapter 3 and [TW].

LEMMA 1.12. *Suppose that ρ_0 is absolutely irreducible and that*

(a) *$\tilde{\rho}_0$ is dihedral (the case where the image is $\mathbf{Z}/2 \times \mathbf{Z}/2$ is allowed),*

(b) $\rho_0|_L$ *is absolutely irreducible where* $L = \mathbf{Q}\left(\sqrt{(-1)^{(p-1)/2}p}\right)$.

Then for any positive integer n and any irreducible Galois stable subspace X of $W_\lambda \otimes \bar{k}$ there exists an element $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ such that

(i) $\tilde{\rho}_0(\sigma) \neq 1$,

(ii) σ *fixes* $\mathbf{Q}(\zeta_{p^n})$,

(iii) σ *has an eigenvalue* 1 *on* X.

Proof. If $\tilde{\rho}_0$ is dihedral then $\rho_0 \otimes \bar{k} = \mathrm{Ind}_H^G \chi$ for some H of index 2 in G, where $G = \mathrm{Gal}(K_1/\mathbf{Q})$. (As before, K_1 is the splitting field of ρ_0.) Here H can be taken as the full inverse image of any of the normal subgroups of index 2 defining the dihedral group. Then $W_\lambda \otimes \bar{k} \simeq \delta \oplus \mathrm{Ind}_H^G(\chi/\chi')$ where δ is the quadratic character $G \to G/H$ and χ' is the conjugate of χ by any element of $G - H$. Note that $\chi \neq \chi'$ since H has nontrivial image in $\mathrm{PGL}_2(\bar{k})$.

To find a σ such that $\delta(\sigma) = 1$ and conditions (i) and (ii) hold, observe that $M(\zeta_{p^n})$ is abelian where M is the quadratic field associated to δ. So conditions (i) and (ii) can be satisfied if $\tilde{\rho}_0$ is non-abelian. If $\tilde{\rho}_0$ is abelian (i.e., the image has the form $\mathbf{Z}/2 \times \mathbf{Z}/2$), then we use hypothesis (b). If $\mathrm{Ind}_H^G(\chi/\chi')$ is reducible over $\bar{k}$ then $W_\lambda \otimes \bar{k}$ is a sum of three distinct quadratic characters, none of which is the quadratic character associated to L, and we can repeat the argument by changing the choice of H for the other two characters. If $X = \mathrm{Ind}_H^G(\chi/\chi') \otimes \bar{k}$ is absolutely irreducible then pick any $\sigma \in G - H$. This satisfies (i) and can be made to satisfy (ii) if (b) holds. Finally, since $\sigma \in G - H$ we see that σ has trace zero and $\sigma^2 = 1$ in its action on X. Thus it has an eigenvalue equal to 1. □

Chapter 2

In this chapter we study the Hecke rings. In the first section we recall some of the well-known properties of these rings and especially the Gorenstein property whose proof is rather technical, depending on a characteristic p version of the q-expansion principle. In the second section we compute the relations between the Hecke rings as the level is augmented. The purpose is to find the change in the η-invariant as the level increases.

In the third section we state the conjecture relating the deformation rings of Chapter 1 and the Hecke rings. Finally we end with the critical step of showing that if the conjecture is true at a minimal level then it is true at all levels. By the results of the appendix the conjecture is equivalent to the that $S \simeq T$, as otherwise $S \simeq \ker\alpha \oplus \operatorname{im}\hat{\alpha}$ is a nontrivial decomposition as S-modules, which contradicts S being local. □

Remark. Lenstra has made an important improvement to this proposition by showing that replacing $\tilde{\eta}_T$ by $\beta(\operatorname{ann}\mathfrak{p})$ gives a criterion valid for all local $\mathcal{O}$-algebras which are finite and free over $\mathcal{O}$, thus without the Gorenstein hypothesis.

PRINCETON UNIVERSITY, PRINCETON, NJ

REFERENCES

[AK] A. ALTMAN and S. KLEIMAN, *An Introduction to Grothendieck Duality Theory*, vol. 146, Springer Lecture Notes in Mathematics, 1970.

[BiKu] B. BIRCH and W. KUYK (eds.), *Modular Functions of One Variable* IV, vol. 476, Springer Lecture Notes in Mathematics, 1975.

[Bo] Boston, N., *Families of Galois representations—Increasing the ramification*, Duke Math. J. **66**, 357–367.

[BH] W. BRUNS and J. HERZOG, *Cohen-Macaulay Rings*, Cambridge University Press, 1993.

[BK] S. BLOCH and K. KATO, *L-Functions and Tamagawa Numbers of Motives*, The Grothendieck Festschrift, Vol. 1 (P. Cartier et al. eds.), Birkhäuser, 1990.

[BLR] N. BOSTON, H. LENSTRA, and K. RIBET, Quotients of group rings arising from two-dimensional representations, C. R. Acad. Sci. Paris **t312**, Ser. 1 (1991), 323–328.

[CF] J. W. S. CASSELS and A. FRÖLICH (eds.), *Algebraic Number Theory*, Academic Press, 1967.

[Ca1] H. CARAYOL, Sur les représentations p-adiques associées aux formes modulaires de Hilbert, Ann. Sci. Ec. Norm. Sup. **IV**, Ser. 19 (1986), 409–468.

[Ca2] ———, Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires, Duke Math. J. **59** (1989), 785–801.

[Ca3] ———, Formes modulaires et représentations Galoisiennes à valeurs dans un anneau local complet, in *p-Adic Monodromy and the Birch-Swinnerton-Dyer Conjecture* (eds. B. Mazur and G. Stevens), Contemp. Math., vol. 165, 1994.

[CPS] E. CLINE, B. PARSHALL, and L. SCOTT, Cohomology of finite groups of Lie type I, Publ. Math. IHES **45** (1975), 169–191.

[CS] J. COATES and C. G. SCHMIDT, Iwasawa theory for the symmetric square of an elliptic curve, J. reine und angew. Math. **375/376** (1987), 104–156.

[CW] J. COATES and A. WILES, On p-adic L-functions and elliptic units, Ser. A26, J. Aust. Math. Soc. (1978), 1–25.

[Co] R. COLEMAN, Division values in local fields, Invent. Math. **53** (1979), 91–116.

[DR] P. DELIGNE and M. RAPOPORT, *Schémas de modules de courbes elliptiques*, in Springer Lecture Notes in Mathematics, Vol. 349, 1973.

[DS] P. DELIGNE and J-P. SERRE, Formes modulaires de poids 1, Ann. Sci. Ec. Norm. Sup. **IV**, Ser. 7 (1974), 507–530.

[Dia] F. DIAMOND, The refined conjecture of Serre, to appear in Proc. 1993 Hong Kong Conf. on Modular Forms and Elliptic Curves.

[Di] L. E. DICKSON, *Linear Groups with an Exposition of the Galois Field Theory*, Teubner, Leipzig, 1901.

[Dr] V. Drinfeld, Two-dimensional ℓ-adic representations of the fundamental group of a curve over a finite field and automorphic forms on GL(2), Am. J. Math. **105** (1983), 85–114.

[E1] B. Edixhoven, The weight in Serre's conjecture on modular forms, Invent. Math. **109** (1992), 563–594.

[E2] ———, L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein", in *Courbes Modulaires et Courbes de Shimura*, Astérisque **196-197** (1991), 159–170.

[Fl] M. Flach, A finiteness theorem for the symmetric square of an elliptic curve, Invent. Math. **109** (1992), 307–327.

[Fo] J.-M. Fontaine, Sur certains types de représentations p-adiques du groupe de Galois d'un corps local; construction d'un anneau de Barsotti-Tate, Ann. of Math. **115** (1982), 529–577.

[Fr] G. Frey, Links between stable elliptic curves and certain diophantine equations, Annales Universitatis Saraviensis **1** (1986), 1–40.

[Gre1] R. Greenberg, Iwasawa theory for p-adic representations, Adv. St. Pure Math. **17** (1989), 97–137.

[Gre2] ———, On the structure of certain Galois groups, Invent. Math. **47** (1978), 85–99.

[Gro] B. H. Gross, A tameness criterion for Galois representations associated to modular forms mod p, Duke Math. J. **61** (1990), 445–517.

[Guo] L. Guo, General Selmer groups and critical values of Hecke L-functions, Math. Ann. **297** (1993), 221–233.

[He] Y. Hellegouarch, Points d'ordre $2p^h$ sur les courbes elliptiques, Acta Arith. **XXVI** (1975), 253–263.

[Hi1] H. Hida, Iwasawa modules attached to congruences of cusp forms, Ann. Sci. Ecole Norm. Sup. (4) **19** (1986), 231–273.

[Hi2] ———, Theory of p-adic Hecke algebras and Galois representations, Sugaku Expositions **2-3** (1989), 75–102.

[Hi3] ———, Congruences of cusp forms and special values of their zeta functions, Invent. Math. **63** (1981), 225–261.

[Hi4] ———, On p-adic Hecke algebras for GL$_2$ over totally real fields, Ann. of Math. **128** (1988), 295–384.

[Hu] B. Huppert, *Endliche Gruppen I*, Springer-Verlag, 1967.

[Ih] Y. Ihara, On modular curves over finite fields, in Proc. Intern. Coll. on discrete subgroups of Lie groups and application to moduli, Bombay, 1973, pp. 161–202.

[Iw1] K. Iwasawa, *Local Class Field Theory*, Oxford University Press, Oxford, 1986.

[Iw2] ———, On $\mathbf{Z}_\ell$-extensions of algebraic number fields, Ann. of Math. **98** (1973), 246–326.

[Ka] N. Katz, A result on modular forms in characteristic p, in *Modular Functions of One Variable* V, Springer L. N. M. **601** (1976), 53–61.

[Ku1] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhaüser, 1985.

[Ku2] ———, Almost complete intersections are not Gorenstein, J. Alg. **28** (1974), 111–115.

[KM] N. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Ann. of Math. Studies **108**, Princeton University Press, 1985.

[La] R. Langlands, *Base Change for* GL (2), Ann. of Math. Studies, Princeton University Press **96**, 1980.

[Li] W. Li, Newforms and functional equations, Math. Ann. **212** (1975), 285–315.

[Liv] R. Livné, On the conductors of mod ℓ Galois representations coming from modular forms, J. of No. Th. **31** (1989), 133–141.

[Ma1] B. Mazur, Deforming Galois representations, in *Galois Groups over* **Q**, vol. 16, MSRI Publications, Springer, New York, 1989.

[Ma2] ———, Modular curves and the Eisensten ideal, Publ. Math. IHES **47** (1977), 133–186.

[Ma3] ———, Rational isogenies of prime degree, Invent. Math. **44** (1978), 129–162.

[M Ri] B. Mazur and K. Ribet, Two-dimensional representations in the arithmetic of modular curves, *Courbes Modulaires et Courbes de Shimura*, Astérisque **196-197** (1991), 215–255.

[M Ro] B. Mazur and L. Roberts, Local Euler characteristics, Invent. Math. **9** (1970), 201–234.

[MT] B. Mazur and J. Tilouine, Représentations galoisiennes, differentielles de Kähler et conjectures principales, Publ. Math. IHES **71** (1990), 65–103.

[MW1] B. Mazur and A. Wiles, Class fields of abelian extensions of **Q**. Invent. Math. **76** (1984), 179–330.

[MW2] ———, On p-adic analytic families of Galois representations, Comp. Math. **59** (1986), 231–264.

[Mi1] J. S. Milne, Jacobian varieties, in *Arithmetic Geometry* (Cornell and Silverman, eds.), Springer-Verlag, 1986.

[Mi2] ———, *Arithmetic Duality Theorems*, Academic Press, 1986.

[Ram] R. Ramakrishna, On a variation of Mazur's deformation functor, Comp. Math. **87** (1993), 269–286.

[Ray1] M. Raynaud, Schémas en groupes de type $(p, p, \dots, p)$, Bull. Soc. Math. France **102** (1974), 241–280.

[Ray2] ———, Spécialisation du foncteur de Picard, Publ. Math. IHES **38** (1970), 27–76.

[Ri1] K. A. Ribet, On modular representations of Gal($\bar{\mathbf{Q}}/\mathbf{Q}$) arising from modular forms, Invent. Math. **100** (1990), 431–476.

[Ri2] ———, Congruence relations between modular forms, Proc. Int. Cong. of Math. **17** (1983), 503–514.

[Ri3] ———, Report on mod l representations of Gal($\bar{\mathbf{Q}}/\mathbf{Q}$), Proc. of Symp. in Pure Math. **55** (1994), 639–676.

[Ri4] ———, Multiplicities of p-finite mod p Galois representations in $J_0(Np)$, Boletin da Sociedade Brasileira de Matematica, Nova Serie **21** (1991), 177–188.

[Ru1] K. Rubin, Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication, Invent. Math. **89** (1987), 527–560.

[Ru2] ———, The 'main conjectures' of Iwasawa theory for imaginary quadratic fields, Invent. Math. **103** (1991), 25–68.

[Ru3] ———, Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer, Invent. Math. **64** (1981), 455–470.

[Ru4] ———, More 'main conjectures' for imaginary quadratic fields, CRM Proceedings and Lecture Notes, 4, 1994.

[Sch] M. Schlessinger, Functors on Artin rings, Trans. A.M.S. **130** (1968), 208–222.

[Scho] R. Schoof, The structure of the minus class groups of abelian number fields, in Seminaire de Théorie des Nombres, Paris (1988–1989), Progress in Math. **91**, Birkhauser (1990), 185–204.

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

[de Sh] E. de Shalit, *Iwasawa Theory of Elliptic Curves with Complex Multiplication*, Persp. in Math., Vol. 3, Academic Press, 1987.

[Sh1] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Iwanami Shoten and Princeton University Press, 1971.

[Sh2] ———, On the holomorphy of certain Dirichlet series, Proc. London Math. Soc. (3) **31** (1975), 79–98.

[Sh3] ———, The special values of the zeta function associated with cusp forms, Comm. Pure and Appl. Math. **29** (1976), 783–804.

[Sh4] ———, On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields, Nagoya Math. J. **43** (1971), 199–208.

[Ta] J. Tate, *p*-divisible groups, Proc. Conf. on Local Fields, Driebergen, 1966, Springer-Verlag, 1967, pp. 158–183.

[Ti1] J. Tilouine, Un sous-groupe *p*-divisible de la jacobienne de $X_1(Np^r)$ comme module sur l'algebre de Hecke, Bull. Math. Soc. France **115** (1987), 329–360.

[Ti2] ———, Théorie d'Iwasawa classique et de l'algèbre de Hecke ordinaire, Comp. Math. **65** (1988), 265–320.

[Tu] J. Tunnell, Artin's conjecture for representations of octahedral type, Bull. A.M.S. **5** (1981), 173–175.

[TW] R. Taylor and A. Wiles, Ring theoretic properties of certain Hecke algebras, next paper, this issue.

[We] A. Weil, Uber die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen, Math. Ann. **168** (1967), 149–156.

[Wi1] A. Wiles, On ordinary λ-adic representations associated to modular forms, Invent. Math. **94** (1988), 529–573.

[Wi2] ———, On *p*-adic representations for totally real fields, Ann. of Math. **123** (1986), 407–456.

[Wi3] ———, Modular curves and the class group of $\mathbf{Q}(\zeta_p)$, Invent. Math. **58** (1980), 1–35.

[Wi4] ———, The Iwasawa conjecture for totally real fields, Ann. of Math. **131** (1990), 493–540.

[Win] J. P. Wintenberger, Structure galoisienne de limites projectives d'unitées locales, Comp. Math. **42** (1981), 89–103.

(Received October 14, 1994)