CHAPTER 6

Appendix by Kevin Buzzard: A mod ℓ multiplicity one result

In this appendix, we explain how the ideas of [**45**] can be used to prove the following mild strengthening of the multiplicity one results in §9 of [**31**].

The setup is as follows. Let f be a normalised cuspidal eigenform of level N, and weight k, defined over $\overline{\mathbf{F}}_\ell$, with $\ell \nmid N$ and $2 \leq k \leq \ell+1$. Let N^* denote N if $k=2$, and $N\ell$ if $k>2$. Let $J_{\mathbf{Q}}$ be the Jacobian of the curve $X_1(N^*)_{\mathbf{Q}}$, and let H denote the Hecke algebra in $\mathrm{End}(J_{\mathbf{Q}})$ generated over $\mathbf{Z}$ by T_p for all primes p, and all the Diamond operators of level N^*. It is well-known (for example by Proposition 9.3 of [**45**]) that there is a characteristic 0 normalised eigenform F in $S_2(\Gamma_1(N^*))$ lifting f. Let $\mathfrak{m}$ denote the maximal ideal of H associated to F (note that $\mathfrak{m}$ depends only on f and not on the choice of F), and let $\mathbf{F} = H/\mathfrak{m}$, which embeds naturally into $\overline{\mathbf{F}}_\ell$. Suppose the representation $\rho_f : G_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ associated to f is absolutely irreducible, and furthermore assume that if $k=\ell+1$ then ρ_f is not isomorphic to a representation coming from a form of weight 2 and level N.

Theorem 6.1. *If ρ_f is ramified at ℓ, or if ρ_f is unramified at ℓ but $\rho_f(\mathrm{Frob}_\ell)$ is not a scalar matrix, then $J_{\mathbf{Q}}(\overline{\mathbf{Q}})[\mathfrak{m}]$ has $H/\mathfrak{m}$-dimension two, and hence is a model for (precisely one copy of) ρ_f.*

The motivation for putting ourselves in the setup above is that every absolutely irreducible modular mod ℓ representation has a twist coming from a modular form of level prime to ℓ and weight at most $\ell+1$. In particular, every modular mod ℓ representation has a twist coming from a form satisfying the conditions of our setup. Furthermore, if f is as in our setup, then Theorems 2.5 and 2.6 of [**31**] tell us the precise structure of the restriction of ρ_f to D_ℓ, a decomposition group at ℓ. These results are explained in Section 2.2. Using them, it is easy to deduce

Corollary 6.2. *Let ρ be an absolutely irreducible modular mod ℓ representation, such that $\rho_f(D_\ell)$ is not contained within the scalars. Then some twist of ρ comes from a modular form satisfying the conditions of the theorem, and hence ρ is a multiplicity one representation in the sense of Remark 3.4.2.*

The theorem, commonly referred to as a "multiplicity one theorem", is a mild extension of results of Mazur, Ribet, Gross and Edixhoven. It was announced for $\ell=2$ as Proposition 2.4 of [**9**] but the proof given there is not quite complete—in fact, the last line of the proof there is a little optimistic. I would hence like to thank Ribet and Stein for the opportunity to correct this oversight in [**9**].

Proof of Theorem. Firstly we observe that the only case not dealt with by Theorem 9.2 of [**31**] is the case when $k = \ell$ and ρ_f is unramified at ℓ, with $\rho_f(\mathrm{Frob}_\ell)$ a non-scalar matrix whose eigenvalues are equal. Moreover, using Theorems 2.5 and 2.6 of [**31**] we see that in this case f must be ordinary at ℓ. We are hence in a position to use the detailed construction of ρ_f given in §§11–12 of [**45**]. We will follow the conventions set up in the present paper for normalisations of Hecke operators, and so in particular the formulae below differ from the ones in [**45**] by a twist.

The maximal ideal $\mathfrak{m}$ of H associated to f gives rise as in (12.5) of [**45**] to an idempotent $e \in H_\ell := H \otimes_{\mathbf{Z}} \mathbf{Z}_l$, such that the completion $H_\mathfrak{m}$ of H at $\mathfrak{m}$ is just eH_ℓ. Let G denote $e(J_{\mathbf{Q}_\ell}[\ell^\infty])$, the part of the ℓ-divisible group of J which is associated to $\mathfrak{m}$. Then $H_\mathfrak{m}$ acts on G, and it is proved in Propositions 12.8 and 12.9 of [**45**] that there is an exact sequence of ℓ-divisible groups

$$0 \to G^0 \to G \to G^e \to 0$$

over $\mathbf{Q}_\ell$, which is $H_\mathfrak{m}$-stable. Let

$$0 \to T^0 \to T \to T^e \to 0$$

be the exact sequence of Tate modules of these groups. We now explain explicitly, following [**45**], how the group D_ℓ acts on these Tate modules.

If $k > 2$ then there is a Hecke operator U_ℓ in $H_\mathfrak{m}$, and we define $u = U_\ell$. If $k = 2$ then there is a Hecke operator T_ℓ in $H_\mathfrak{m}$ and because we are in the ordinary case we know that T_ℓ is a unit in $H_\mathfrak{m}$. We define u to be the unique root of the polynomial $X^2 - T_\ell X + \ell\langle\ell\rangle$ in $H_\mathfrak{m}$ which is a unit (u exists by an appropriate analogue of Hensel's lemma).

The calculations of Propositions 12.8 and 12.9 of [**45**] show that, under our conventions, the absolute Galois group D_ℓ of $\mathbf{Q}_\ell$ acts on T^e as $\lambda(u)$, where $\lambda(x)$ denotes the unramified character taking Frob_ℓ to x. Moreover, these propositions also tell us that D_ℓ acts on T^0 via the character $\chi_\ell\lambda(u^{-1}\langle\ell\rangle_N)\chi^{\ell-2}$, where χ_ℓ is the cyclotomic character and χ is the Teichmüller character. The key point is that this character takes values in $H^\times$.

The next key observation is that a standard argument on differentials, again contained in the proof of Propositions 12.8 and 12.9 of [**45**], shows that $G^e[\mathfrak{m}] = \mathfrak{m}^{-1}\ell T^e/\ell T^e$ has $H_\mathfrak{m}/\mathfrak{m}$-dimension 1 and that $G^0[\mathfrak{m}]$ has dimension $d^0 \geq 1$. (Note that the fact that $G^e[\mathfrak{m}]$ has dimension 1 implies, via some simple linear algebra, that the sequence $0 \to G^0[\mathfrak{m}] \to G[\mathfrak{m}] \to G^e[\mathfrak{m}] \to 0$ is exact, as asserted by Gross.) Furthermore, because we can identify $G^0[\mathfrak{m}]$ with $\mathfrak{m}^{-1}\ell T^0/\ell T^0$, we see that the action of D_ℓ on $G^0[\mathfrak{m}]$ is via a character which takes values in $(H/\mathfrak{m})^\times$. In particular, D_ℓ acts as scalars on $G^0[\mathfrak{m}]$.

Let us now assume that ρ_f is unramified at ℓ, and that $\rho_f(\mathrm{Frob}_\ell)$ is a non-diagonalisable matrix with eigenvalue $\alpha \in H/\mathfrak{m}$. Choose a model ρ for ρ_f defined over $\mathrm{GL}_2(H/\mathfrak{m})$. By the theorem of Boston, Lenstra and Ribet, we know that $G[\mathfrak{m}]$ is isomorphic to a direct sum of d copies of ρ, or more precisely, d copies of the restriction of ρ to D_ℓ. Here d is an integer satisfying $2d = d^0 + d^e$. Hence, if $G[\mathfrak{m}]^\alpha$ denotes the subspace of $G[\mathfrak{m}]$ where Frob_ℓ acts as α, then the $H/\mathfrak{m}$-dimension of $G[\mathfrak{m}]^\alpha$ is at most d. On the other hand, Frob_ℓ acts on $G[\mathfrak{m}]^0$ as a scalar, and hence this scalar must be α, and so we see $G[\mathfrak{m}]^0 \subseteq G[\mathfrak{m}]^\alpha$. Hence $d^0 \leq d = (d^0+1)/2$. We deduce that $d^0 \leq 1$ and hence $d^0 = d = 1$ and the theorem is proved. ☐

We remark that L. Kilford has found examples of mod 2 forms f of weight 2, such that ρ_f is unramified at 2 and $\rho_f(\mathrm{Frob}_2)$ is the identity, and where $J_{\mathbf{Q}}(\overline{\mathbf{Q}})[\mathfrak{m}]$ has $H/\mathfrak{m}$-dimension 4, and so one cannot hope to extend the theorem to this case. See Remark 3.6 for more details, or [**63**]. A detailed analysis of what is happening in this case, at least in the analogous setting of forms of weight 2 on $J_0(p)$, with p prime, has been undertaken by Emerton in [**38**]. In particular, Emerton proves that multiplicity one fails if and only if the analogue of the exact sequence $0 \to T^0 \to T \to T^e \to 0$ fails to split as a sequence of $H_{\mathfrak{m}}$-modules.

BIBLIOGRAPHY

1. A. Ash and G. Stevens, *Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues*, J. Reine Angew. Math. **365** (1986), 192–220.
2. A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.
3. B. J. Birch, *Cyclotomic fields and Kummer extensions*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 85–93.
4. B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable. IV*, Springer-Verlag, Berlin, 1975, Lecture Notes in Mathematics, Vol. 476.
5. S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990.
6. N. Boston, H. W. Lenstra, Jr., and K. A. Ribet, *Quotients of group rings arising from two-dimensional representations*, C. R. Acad. Sci. Paris Sér. I Math. **312** (1991), no. 4, 323–328.
7. C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*, or Wild* 3*-adic exercises*, http://www.math.harvard.edu/HTML/Individuals/Richard_Taylor.html
8. S. Brueggeman, *The non-existence of certain Galois extensions unramified outside 5*, Journal of Number Theory **75** (1999), 47–52.
9. K. Buzzard, *On level-lowering for mod 2 representations*, to appear in Mathematics Research Letters.
10. K. Buzzard, M. Dickinson, N. Shepherd-Barron, and R. Taylor, *On icosahedral Artin representations*, in preparation.
11. H. Carayol, *Sur les représentations* ℓ*-adiques associées aux formes modulaires de Hilbert*, Ann. scient. Éc. Norm. Sup., 4^{eb} série **19** (1986), 409–468.
12. ______, *Sur les représentations galoisiennes modulo* ℓ *attachées aux formes modulaires*, Duke Math. J. **59** (1989), 785–801.
13. W. Casselman, *On representations of* GL_2 *and the arithmetic of modular curves*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972) (Berlin), Springer, 1973, pp. 107–141. Lecture Notes in Math., Vol. 349.
14. I. V. Čerednik, *Uniformization of algebraic curves by discrete arithmetic subgroups of* $\mathrm{PGL}_2(k_w)$ *with compact quotient spaces*, Mat. Sb. (N.S.) **100(142)**

(1976), no. 1, 59–88, 165.

15. R. F. Coleman, *Serre's conjecture: The Jugentraum of the 20th century*, Mat. Contemp. **6** (1994), 13–18, XII School of Algebra, Part I (Portuguese) (Diamantina, 1992).
16. R. F. Coleman and B. Edixhoven, *On the semi-simplicity of the U_p-operator on modular forms*, Math. Ann. **310** (1998), no. 1, 119–127.
17. R. F. Coleman and J. F. Voloch, *Companion forms and Kodaira-Spencer theory*, Invent. Math. **110** (1992), no. 2, 263–281.
18. B. Conrad, F. Diamond, and R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*, J. Amer. Math. Soc. **12** (1999), no. 2, 521–567.
19. J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.
20. C. W. Curtis and I. Reiner, *Representation theory of finite groups and associative algebras*, Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962, Pure and Applied Mathematics, Vol. XI.
21. H. Darmon, *Serre's conjectures*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993–1994), Amer. Math. Soc., Providence, RI, 1995, pp. 135–153.
22. H. Darmon, F. Diamond, and R. Taylor, *Fermat's last theorem*, Current developments in mathematics, 1995 (Cambridge, MA), Internat. Press, Cambridge, MA, 1994, pp. 1–154.
23. P. Deligne, *Formes modulaires et représentations ℓ-adiques.*, Sém. Bourbaki no. 355, 1968/69 (Berlin and New York), Springer-Verlag, 1971, Lecture Notes in Mathematics, Vol. 179, pp. 139–172.
24. P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972) (Berlin), Springer, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349.
25. F. Diamond, *The refined conjecture of Serre*, Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993) (Cambridge, MA), Internat. Press, 1995, pp. 22–37.
26. F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Providence, RI), Amer. Math. Soc., 1995, pp. 39–133.
27. M. Dickinson, *On the modularity of certain 2-adic galois representations*, Harvard Ph.D. thesis (2000).
28. D. Doud, *S_4 and $\tilde{S}_4$ extensions of $\mathbf{Q}$ ramified at only one prime*, J. Number Theory **75** (1999), no. 2, 185–197.
29. V. G. Drinfeld, *Coverings of p-adic symmetric domains*, Funkcional. Anal. i Prilov zen. **10** (1976), no. 2, 29–40.
30. B. Edixhoven, *L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein"*, Astérisque (1991), no. 196–197, 7–8, 159–170 (1992), Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).
31. ———, *The weight in Serre's conjectures on modular forms*, Invent. Math. **109** (1992), no. 3, 563–594.
32. B. Edixhoven, *Le rôle de la conjecture de Serre dans la démonstration du théorème de Fermat*, Gaz. Math. (1995), no. 66, 25–41.
33. ———, *Erratum and addendum: "The role of Serre's conjecture in the proof of Fermat's theorem"*, Gaz. Math. (1996), no. 67, 19.

34. ———, *Serre's conjecture*, Modular forms and Fermat's last theorem (Boston, MA, 1995) (New York), Springer, 1997, pp. 209–242.
35. M. Eichler, *Quadratische Formen und Modulfunktionen*, Acta Arith. **4** (1958), 217–239.
36. D. Eisenbud, *Commutative algebra with a view toward algebraic geometry*, Springer-Verlag, New York, 1995.
37. D. Eisenbud and J. Harris, *Schemes, The language of modern algebraic geometry*, Springer-Verlag, Berlin, Graduate Texts in Mathematics, Vol. 197.
38. M. Emerton, *Supersingular elliptic curves, theta series and weight two modular forms*, preprint.
39. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), no. 3, 349–366.
40. G. Faltings and B.W. Jordan, *Crystalline cohomology and* $\mathrm{GL}(2,\mathbf{Q})$, Israel J. Math. **90** (1995), no. 1-3, 1–66.
41. G. Frey, *Links between stable elliptic curves and certain Diophantine equations*, Ann. Univ. Sarav. Ser. Math. **1** (1986), no. 1, iv+40.
42. ———, *Links between solutions of* $A-B=C$ *and elliptic curves*, Number theory (Ulm, 1987), Springer, New York, 1989, pp. 31–62.
43. A. Fröhlich, *Local fields*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 1–41.
44. K. Fujiwara, *Level optimization in the totally real case*, in preparation (1999).
45. B.H. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. J. **61** (1990), no. 2, 445–517.
46. R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.
47. Y. Hellegouarch, *Invitation aux mathématiques de Fermat-Wiles*, Masson, Paris, 1997.
48. H. Hida, *Galois representations into* $\mathrm{GL}_2(\mathbf{Z}_p[[X]])$ *attached to ordinary cusp forms*, Invent. Math. **85** (1986), no. 3, 545–613.
49. ———, *Iwasawa modules attached to congruences of cusp forms*, Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 2, 231–273.
50. H. Jacquet and R.P. Langlands, *Automorphic forms on* $\mathrm{GL}(2)$, Springer-Verlag, Berlin, 1970, Lecture Notes in Mathematics, Vol. 114.
51. F. Jarvis, *On Galois representations associated to Hilbert modular forms*, J. Reine Angew. Math. **491** (1997), 199–216.
52. ———, *Level lowering for modular mod* ℓ *representations over totally real fields*, Math. Ann. **313** (1999), no. 1, 141–160.
53. ———, *Mazur's principle for totally real fields of odd degree*, Compositio Math. **116** (1999), no. 1, 39–79.
54. N. Jochnowitz, *A study of the local components of the Hecke algebra mod* ℓ, Trans. Amer. Math. Soc. **270** (1982), no. 1, 253–267.
55. ———, *The index of the Hecke ring,* T_k*, in the ring of integers of* $T_k \otimes \mathbf{Q}$, Duke Math. J. **46** (1979), no. 4, 861–869.
56. B.W. Jordan and R. Livné, *Conjecture "epsilon" for weight* $k > 2$, Bull. Amer. Math. Soc. (N.S.) **21** (1989), no. 1, 51–56.
57. K. Joshi, *Remarks on methods of Fontaine and Faltings*, Internat. Math. Res. Notices **1999**, no. 22, 1199–1209.
58. N.M. Katz, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ.

Antwerp, Antwerp, 1972) (Berlin), Springer, 1973, pp. 69–190. Lecture Notes in Mathematics, Vol. 350.

59. ———, *Higher congruences between modular forms*, Ann. of Math. (2) **101** (1975), 332–367.

60. ———, *A result on modular forms in characteristic p*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976) (Berlin), Springer, 1977, pp. 53–61. Lecture Notes in Math., Vol. 601.

61. N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Princeton University Press, Princeton, N.J., 1985.

62. C. Khare, *Multiplicities of mod p Galois representations*, Manuscripta Math. **95** (1998), no. 2, 181–188.

63. L. J. P. Kilford, *Some examples of non-Gorenstein Hecke algebras associated to modular forms*, in preparation.

64. A. W. Knapp, *Elliptic curves*, Princeton University Press, Princeton, NJ, 1992.

65. S. Lang, *Introduction to modular forms*, Springer-Verlag, Berlin, 1995, With appendixes by D. Zagier and Walter Feit, Corrected reprint of the 1976 original.

66. R. P. Langlands, *Modular forms and ℓ-adic representations*, Proceedings of the International Summer School, University of Antwerp, RUCA, July 17–August 3, 1972 (Berlin) (P. Deligne and W. Kuyk, eds.), Springer, 1973, pp. 361–500. Lecture Notes in Math., Vol. 349.

67. ———, *Base change for* GL(2), Princeton University Press, Princeton, N.J., 1980.

68. W-C. Li, *Newforms and functional equations*, Math. Ann. **212** (1975), 285–315.

69. R. Livné, *On the conductors of mod ℓ Galois representations coming from modular forms*, J. Number Theory **31** (1989), no. 2, 133–141.

70. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

71. B. Mazur and K. A. Ribet, *Two-dimensional representations in the arithmetic of modular curves*, Astérisque (1991), no. 196-197, 6, 215–255 (1992), Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

72. L. Merel, *Universal Fourier expansions of modular forms*, On Artin's conjecture for odd 2-dimensional representations (Berlin), Springer, 1994, pp. 59–94.

73. J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

74. T. Miyake, *Modular forms*, Springer-Verlag, Berlin, 1989, Translated from the Japanese by Yoshitaka Maeda.

75. H. Moon, *Finiteness results on certain mod p Galois representations*, to appear in J. Number Theory.

76. D. Mumford, *Abelian varieties*, Published for the Tata Institute of Fundamental Research, Bombay, 1970, Tata Institute of Fundamental Research Studies in Mathematics, No. 5.

77. C. Queen, *The existence of p-adic Abelian L-functions*, Number theory and algebra (New York), Academic Press, 1977, pp. 263–288.

78. A. Raji, *On the levels of modular mod ℓ Galois representations of totally real fields*, Princeton University Ph.D. thesis, 1998.

79. R. Ramakrishna, *Lifting Galois representations*, Invent. Math. **138** (1999), no. 3, 537–562.
80. ———, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur*, preprint, ftp://math.cornell.edu/pub/ravi (2000).
81. M. Raynaud, *Spécialisation du foncteur de Picard*, Inst. Hautes Études Sci. Publ. Math. No. **38** (1970), 27–76.
82. K. A. Ribet, *From the Taniyama-Shimura conjecture to Fermat's last theorem*, Ann. Fac. Sci. Toulouse Math. (5) **11** (1990), no. 1, 116–139.
83. ———, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.
84. ———, *Raising the levels of modular representations*, Séminaire de Théorie des Nombres, Paris 1987–88, Birkhäuser Boston, Boston, MA, 1990, pp. 259–271.
85. ———, *Lowering the levels of modular representations without multiplicity one*, International Mathematics Research Notices (1991), 15–19.
86. ———, *Report on mod ℓ representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Motives (Seattle, WA, 1991), Amer. Math. Soc., Providence, RI, 1994, pp. 639–676.
87. A. Robert, *Elliptic curves*, Springer-Verlag, Berlin, 1973, Notes from postgraduate lectures given in Lausanne 1971/72, Lecture Notes in Mathematics, Vol. 326.
88. T. Saito, *Modular forms and p-adic Hodge theory*, Invent. Math. **129** (1997), 607–620.
89. I. Schur, *Arithmetische Untersuchungen über endliche Gruppen linearer Substitutionen*, Sitz. Pr. Akad. Wiss. (1906), 164–184, Gesam. Abhl., **I**, 177–197, Springer-Verlag, Berlin-Heidelberg-New York-Tokyo, 1973.
90. J-P. Serre, *Groupes de Lie l-adiques attachés aux courbes elliptiques*, Les Tendances Géom. en Algébre et Théorie des Nombres, Éditions du Centre National de la Recherche Scientifique, Paris, 1966, pp. 239–256 (= Collected Papers **70**).
91. ———, *Une interprétation des congruences relatives à la fonction τ de Ramanujan*, Séminaire Delange-Pisot-Poitou n^o **14** (1967–68) (= C.P. **80**).
92. ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331 (= C.P. **94**).
93. ———, *Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]*, Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416 (Berlin), Springer, 1973, pp. 319–338. Lecture Notes in Math., Vol. 317 (= C.P. **95**).
94. ———, *Formes modulaires et fonctions zêta p-adiques*, Proceedings of the International Summer School, University of Antwerp, RUCA, July 17–August 3, 1972 (Berlin), Springer, 1973, pp. 191–268. Lecture Notes in Math., Vol. 350 (= C.P. **97**).
95. ———, *A Course in Arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7.
96. ———, *Valeurs propres des opérateurs de Hecke modulo ℓ*, Astérisque **24–25** (1975), 109–117 (= C.P. **104**).
97. ———, *Divisibilité de certaines fonctions arithmétiques*, Enseign. Math. (2) **22** (1976), no. 3-4, 227–260 (= C.P. **108**).

98. ———, *Linear representations of finite groups*, Springer-Verlag, New York, 1977, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.
99. ———, *Local fields*, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.
100. ———, *Lettre à J.-F. Mestre*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), Amer. Math. Soc., Providence, RI, 1987, pp. 263–268 (= C.P. **142**).
101. ———, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230 (= C.P. **143**).
102. ———, *Travaux de Wiles (et Taylor, ...)*, Partie I, Séminaire Bourbaki, **803** (1995) (= C.P. **168**).
103. J-P. Serre and J. T. Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517 (= C.P. **79**).
104. N. I. Shepherd-Barron and R. Taylor, *Mod 2 and mod 5 icosahedral representations*, J. Amer. Math. Soc. **10** (1997), no. 2, 283–298.
105. H. Shimizu, *On zeta functions of quaternion algebras*, Ann. of Math. (2) **81** (1965), 166–193.
106. G. Shimura, *A reciprocity law in non-solvable extensions*, J. Reine Angew. Math. **221** (1966), 209–220.
107. ———, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.
108. J. H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1992, Corrected reprint of the 1986 original.
109. ———, *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.
110. C. M. Skinner and A. J. Wiles, *Ordinary representations and modular forms*, Proc. Nat. Acad. Sci. U.S.A. **94** (1997), no. 20, 10520–10527.
111. H. P. F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms*, Proceedings of the International Summer School, University of Antwerp, RUCA, July 17–August 3, 1972 (Berlin), Springer, 1973, pp. 1–55. Lecture Notes in Math., Vol. 350.
112. J. T. Tate, *The non-existence of certain Galois extensions of* $\mathbf{Q}$ *unramified outside* 2, Contemporary Math. **174** (1994), 153–156.
113. R. Taylor and A. J. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2) **141** (1995), no. 3, 553–572.
114. J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. Amer. Math. Soc. (N.S.) **5** (1981), no. 2, 173–175.
115. J.-L. Waldspurger, *Quelques propriétés arithmétiques de certaines formes automorphes sur* GL(2), Compositio Math. **54** (1985), no. 2, 121–171.
116. A. J. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.