---

**MR2085902** 11G40 11G10

**Agashe, Amod** (1-TX);
**Stein, William [Stein, William A.]** (1-HRV)

**Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero. (English. English summary)**

With an appendix by J. Cremona and B. Mazur.

*Math. Comp.* **74** (2005), *no.* 249, 455–484 (*electronic*).

**[References]**

1. A. Agashe, *On invisible elements of the Tate-Shafarevich group*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), no. 5, 369–374. MR1678131 (2000e:11083)
2. A. Agashe and W. A. Stein, Appendix to Joan-C. Lario and René Schoof: Some compu- tations with Hecke rings and deformation rings, to appear in J. Exp. Math. MR1959271 (2004b:11072)
3. A. Agashe and W.A. Stein, *Visibility of Shafarevich-Tate Groups of Abelian Varieties*, to appear in J. of Number Theory (2002). MR1939144 (2003h:11070)
4. A. Agashe and W. A. Stein, *The Manin constant, congruence primes, and the modular degree*, preprint, (2004). http://modular.fas.harvard.edu/papers/manin-agashe/
5. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user lan- guage*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR1484478
6. B.J. Birch, *Elliptic curves over* **Q***: A progress report*, 1969 Number Theory Institute (Proc. Sympos. Pure Math., Vol. XX, State Univ. New York, Stony Brook, N.Y., 1969), Amer. Math. Soc., Providence, R.I., 1971, pp. 396–400. MR0314845 (47 #3395)
7. S. Bosch, W. L'́utkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)
8. J. W.S. Cassels, "*Arithmetic on curves of genus* 1*. III. The Tate-Šafarevič and Selmer groups*", Proc. London Math. Soc. (3) **12** (1962), 259–296. MR0163913 (29 #1212)
9. J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997. MR1628193 (99e:11068)
10. J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Ex- periment. Math. **9** (2000), no. 1, 13–28. MR1758797 (2001g:11083)

11. B. Conrad and W.A. Stein, *Component groups of purely toric quotients*, Math. Res. Lett. **8** (2001), no. 5–6, 745–766. MR1879817 (2003f:11087)
12. C. Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* **Q**, Experiment. Math. **10** (2001), no. 2, 191–196. MR1837670 (2003a:11065)
13. F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem, Providence, RI, 1995, pp. 39–133. MR1357209 (97g:11044)
14. B. Edixhoven, *On the Manin constants of modular elliptic curves*, Arithmetic algebraic geometry (Texel, 1989), Birkh́auser Boston, Boston, MA, 1991, pp. 25–39. MR1085254 (92a:11066)
15. M. Emerton, *Optimal quotients of modular Jacobians*. Preprint. MR2021024
16. E.V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll, and J. L. Wetherell, *Em- pirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp. **70** (2001), no. 236, 1675–1697. MR1836926 (2002d:11072)
17. J-M. Fontaine, *Groupes finis commutatifs sur les vecteurs de Witt*, C. R. Acad. Sci. Paris Sér. A-B **280** (1975), Ai, A1423–A1425. MR0374153 (51 #10353)
18. B.H. Gross, *L-functions at the central critical point*, Motives (Seattle, WA, 1991), Amer. Math. Soc., Providence, RI, 1994, pp. 527–535. MR1265543 (95a:11060)
19. A. Grothendieck, *Le groupe de Brauer. III. Exemples et compléments*, Dix Exposés sur la Cohomologie des Schémas, North-Holland, Amsterdam, 1968, pp. 88–188. MR0244271 (39 #5586c)
20. A. Grothendieck,*Mod'eles de Néron et monodromie* in *Groupes de monodromie en géométrie algébrique. I*, Springer-Verlag, Berlin, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Dirigé par A. Grothendieck. Vol. 288. MR0354656 (50 #7134)
21. B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320. MR0833192 (87j:11057)
22. N.M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), no. 3, 481–502. MR0604840 (82d:14025)
23. V.A. Kolyvagin and D.Y. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Algebra i Analiz **1** (1989), no. 5, 171–196. MR1036843 (91c:11032)

24. V.A. Kolyvagin and D.Y. Logachev, *Finiteness ofover totally real fields*, Math. USSR Izvestiya **39** (1992), no. 1, 829–853. MR1137589 (93d:11063)
25. D.R. Kohel and W. A. Stein, *Component Groups of Quotients of* $J0(N)$, Proceedings of the 4th International Symposium (ANTS-IV), Leiden, Netherlands, July 2–7, 2000 (Berlin), Springer, 2000. MR1850621 (2002h:11051)
26. S. Lang, *Number theory. III*, Springer-Verlag, Berlin, 1991, Diophantine geometry. MR1112552 (93a:11048)
27. H. W. Lenstra, Jr. and F. Oort, *Abelian varieties having purely additive reduction*, J. Pure Appl. Algebra **36** (1985), no. 3, 281–298. MR0790619 (86e:14020)
28. Joan-C. Lario and René Schoof, *Some computations with Hecke rings and deformation rings*, Experiment. Math. **11** (2002), no. 2, 303–311, with an appendix by Amod Agashe and William Stein. MR1959271 (2004b:11072)
29. B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266. MR0444670 (56 #3020)
30. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. HautesÉtudes Sci. Publ. Math. (1977), no. 47, 33–186 (1978). MR0488287 (80c:14015)
31. B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162. MR0482230 (80h:14022)
32. B. Mazur and J. Tate, *Points of order* 13 *on elliptic curves*, Invent. Math. **22** (1973/74), 41–49. MR0347826 (50 #327)
33. J. S. Milne, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150. MR0861974
34. A. P. Ogg, *Rational points on certain elliptic modular curves*, Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R.I., 1973, pp. 221–231. MR0337974 (49 #2743)
35. B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2) **150** (1999), no. 3, 1109–1149. MR1740984 (2000m:11048)
36. G. Shimura, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), no. 3, 523–544. MR0318162 (47 #6709)
37. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Prince- ton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.

MR1291394 (95e:11048)

38. G. Stevens, *Arithmetic on modular curves*, Birkh́auser Boston Inc., Boston, Mass., 1982. MR0670070 (87b:11050)
39. W. A. Stein, *Explicit approaches to modular abelian varieties*, Ph.D. thesis, University of California, Berkeley (2000).
40. W. A. Stein, *An introduction to computing modular forms using modular symbols*, to appear in an MSRI Proceedings (2002).
41. W. A. Stein, *Shafarevich-Tate groups of nonsquare order*, Proceedings of MCAV 2002, Progress of Mathematics (to appear). MR2058655
42. J. Sturm, *On the congruence of modular forms*, Number theory (New York, 1984–1985), Springer, Berlin, 1987, pp. 275–280. MR0894516 (88h:11031)
43. J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Inter- nat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295. MR0175892 (31 #168)
44. J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1966 (reprinted in 1995), Exp. No. 306, 415–440. MR1610977

**MR2023296** 11F33

**Coleman, Robert F.** (1-CA); **Stein, William A.** (1-HRV)

**Approximation of eigenforms of infinite slope by eigenforms of finite slope.**

*Geometric aspects of Dwork theory. Vol. I, II*, 437–449, *Walter de Gruyter GmbH & Co. KG*, *Berlin*, 2004.

**MR2058655 (2005c:11072)** 11G10

**Stein, William A.** (1-HRV)

**Shafarevich-Tate groups of nonsquare order. (English. English summary)**

*Modular curves and abelian varieties*, 277–289, *Progr. Math.*, 224, *Birkhäuser*, *Basel*, 2004.

In an unguarded moment, P. Swinnerton-Dyer [in *Proc. Conf. Local Fields (Driebergen, 1966)*, 132–157, Springer, Berlin, 1967; MR0230727 (37 #6287)] wrote that if the group Ш($A$) (of everywhere locally trivial $K$-torsors under an abelian variety $A$ over a number field $K$) is finite—as it is widely conjectured to be—then a theorem of Tate would imply that its order ш($A$) is a square, i.e. for every prime $p$, the exponent $v_p(\text{ш}(A))$ of $p$ in $\text{ш}(A)$ is even.

What the results of J. Tate [in *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, 288–295, Inst. Mittag-Leffler, Djursholm, 1963; MR0175892 (31 #168)] and M. Flach [J. Reine Angew. Math. **412** (1990), 113–127; MR1079004 (92b:11037)] do imply is that $v_p(\text{ш}(A))$ is even, if $A$ admits a suitable polarisation (cf. Theorem 1.2). Admitting a principal polarisation is sufficient for the odd part of $\text{ш}(A)$ to have square order.

And indeed, B. Poonen and M. Stoll [Ann. of Math. (2) **150** (1999), no. 3, 1109–1149; MR1740984 (2000m:11048)] came up with an explicit Jacobian surface $A$ over $\mathbf{Q}$ such that $\text{ш}(A) = 2$; they also gave a criterion for the Jacobian variety $A$ of a (smooth, projective, absolutely connected) curve $X$ of genus $g \geq 2$ over $K$ to have odd $v_2(\text{ш}(A))$: such is the case if the (finite) number of places of $K$ where $X$ fails to have a 0-cycle of degree $g-1$ is odd. Numerous further examples have been found by B. W. Jordan and R. A. Livné [Bull. London Math. Soc. **31** (1999), no. 6, 681–685; MR1711026 (2000j:11090)] and by S. Baba [J. Number Theory **87** (2001), no. 1, 96–108; MR1816038 (2002b:11085)].

The author gives the first examples of odd $v_p(\text{ш}(A))$ for an odd prime $p$. His main result implies that for every $p < 25000$ (with $p \neq 37$), there is a twist $A$ of the power $E^{p-1}$ of the abelian curve $E\colon y^2 + y = x^3 - x$ (the curve 37A) such that $v_p(\text{ш}(A))$ is odd (Theorem 3.1). To get an example where $v_{37}(\text{ш}(A))$ is odd, use the curve 43A instead.

The restriction $p < 25000$ (cf. Proposition 2.3) comes from the fact that for these primes his tireless computer has been able to find a certain auxiliary prime $l$ (cf. Conjecture 2.1) needed for constructing $A$. A sample of his instructions to the computer is included.

The main result (Theorem 2.14) establishes an exact sequence

$$0 \to E(\mathbf{Q})/pE(\mathbf{Q}) \to {}_{p^\infty}\text{Ш}(A) \to {}_{p^\infty}\text{Ш}(E_L) \to {}_{p^\infty}\text{Ш}(E) \to 0$$

for an abelian curve $E$ over $\mathbf{Q}$ and an odd prime $p$ which does not divide any of the Tamagawa numbers of $E$ and for which $\rho_{E,p}\colon \text{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \text{Aut}({}_pE(\overline{\mathbf{Q}}))$ is surjective. The auxiliary prime $l$ should be $\equiv 1 \pmod p$, it should not divide the conductor of $E$, the function $L(E,\chi,s)$ should not vanish at $s=1$ for some—and hence for all $p-1$—character(s) $\chi\colon (\mathbf{Z}/l\mathbf{Z})^\times \to {}_p\mathbf{C}^\times$ of level $l$ and order $p$, and, finally, $p$ should not divide $\text{Card}\, E(\mathbf{F}_l)$. The degree-$p$ cyclic extension $L$ is contained in the field of $l$th roots of 1, and $A$ is the kernel of the trace map $\text{Res}_{L|\mathbf{Q}} E_L \to E$; it turns out to be a twist of $E^{p-1}$ (Proposition 2.4).

If ${}_{p^\infty}\text{Ш}(E)$ is finite, then so are the other two Ш by a deep theorem of Kazuya Kato, applicable by the choice of $l$. In that case $\text{rk}\, E(\mathbf{Q})$

and $v_p(ш(A))$ have the same parity, in view of the surjectivity of $\rho_{E,p}$ and the fact that the last two groups in the displayed exact sequence are of square order. The author gets the desired examples of odd $v_p(ш(A))$ by choosing an $E$ for which $\mathrm{rk}\, E(\mathbf{Q})$ is odd—such as the rank-1 curve 37A. For this curve he also verifies, for good measure, that $Ш = \{0\}$, using the results of Kolyvagin and the programmes of Cremona.

However, $v_q(ш(A))$ is even for every prime $q \neq p$, if ${}_{q^\infty}Ш(E)$ is finite (Proposition 2.16).

REVISED (January, 2005)

*Chandan Singh Dalawat* (6-HCRI)

**MR2052021 (2005c:11070)** 11G05 11G18

**Stein, William [Stein, William A.]** (1-HRV)**;**
**Watkins, Mark [Watkins, Mark J.]** (1-PAS)

**Modular parametrizations of Neumann-Setzer elliptic curves.**

*Int. Math. Res. Not.* **2004,** *no.* 27, 1395–1405.

Let $E/\mathbf{Q}$ be an elliptic curve of conductor $N$. G. Stevens [Invent. Math. **98** (1989), no. 1, 75–106; MR1010156 (90m:11089)] conjectured that the optimal quotient of $X_1(N)$ in the isogeny class of $E$ is the curve in this isogeny class with minimal Faltings height. In this paper the authors verify Stevens' conjecture in the case where $N$ is prime. To do so, first recall that in [J.-F. Mestre and J. Oesterlé, J. Reine Angew. Math. **400** (1989), 173–184; MR1013729 (90g:11078)] the isogeny class of an elliptic curve $E/\mathbf{Q}$ of prime conductor $p > 37$ contains exactly one curve, unless $p = u^2 + 64$ and $E$ is one of the two Neumann-Setzer curves [O. Neumann, Math. Nachr. **49** (1971), 107–123; MR0337999 (49 #2767a); B. Setzer, J. London Math. Soc. (2) **10** (1975), 367–378; MR0371904 (51 #8121)]:

$$E_0\colon y^2 + xy = x^3 - \frac{u+1}{4}x^2 + 4x - u,$$

$$E_1\colon y^2 + xy = x^3 - \frac{u+1}{4}x^2 - u.$$

To study Stevens' conjecture it then suffices to consider the second case. The Faltings height of $E_1$ is smaller than that of $E_0$; this follows by exhibiting an isogeny $E_1 \to E_0$ that extends to an étale morphism of the respective Néron models. Analyze the kernel of this isogeny and of the natural map from the Jacobian of $X_0(p)$ to that of $X_1(p)$, coupled with the fact that $E_0$ is $X_0(p)$-optimal [J.-F. Mestre and J. Oesterlé, op. cit.], and it follows that $E_1$ is $X_1(p)$-optimal.

By an intricate analysis of the Eisenstein ideals [B. Mazur, Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33–186 (1978); MR0488287 (80c:14015)], the authors also show that the modular degree of $E_0$ is odd if and only if $u \equiv 3 \pmod 8$, and they post various conjectures concerning the parity of the modular degree of elliptic curves over **Q** (sample Conjecture 4.2: there are infinitely many elliptic curves over **Q** with odd modular degree). The paper ends with numerical data for the frequency of nontrivial $p$-Ш (presumably computed under the Birch-Swinnerton-Dyer conjecture) for the Neumann-Setzer curves. *Siman Wong* (1-MA-LMS)

**[References]**

1. A. Abbes and E. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires* [*The Manin conjecture for modular elliptic curves*], Compositio Math. **103** (1996), no. 3, 269–286 (French). MR1414591 (97f:11038)
2. A. Brumer and O. McGuinness, *The behavior of the Mordell-Weil group of elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 375–382, http://www.oisinmc.com/math/310716/. MR1044170 (91b:11076)
3. F. Calegari and W. Stein, *Conjectures about discriminants of Hecke algebras of prime level*, to appear in ANTS VI proceedings, Springer-Verlag Lecture Notes in Computer Science Series, http://web.ew.usna.edu/∼ants/.
4. J. E. Cremona, *Elliptic curves of conductor* $\leq 20000$, http://www.maths.nott.ac.uk/personal/jec/ftp/data.
5. C. Delaunay, *Heuristics on Tate-Shafarevitch groups of elliptic curves defined over* $\mathbb{Q}$ Experiment. Math. **10** (2001), no. 2, 191–196. MR1837670 (2003a:11065)
6. P. Deligne, *Preuve des conjectures de Tate et de Shafarevitch (d'après G. Faltings)* [*Proof of the Tate and Shafarevich conjectures (after G. Faltings)*], Astérisque (1985), no. 121–122, 25–41 (French), Seminaire Bourbaki, Vol. 1983/84. MR0768952 (87c:11026)
7. F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, Ontario, 1993–1994), CMS Conf. Proc., vol. 17, American Mathematical Society, Rhode Island, 1995, pp. 39–133. MR1357209 (97g:11044)
8. M. Emerton, *Optimal quotients of modular Jacobians*, preprint, 2001. MR2021024
9. G. Frey, *Links between solutions of* $\mathrm{A} - \mathrm{B} = \mathrm{C}$ *and elliptic curves*, Number Theory (Ulm, 1987) (H. P. Schlickewei and E. Wirsing,

eds.), Lecture Notes in Math., vol. 1380, Springer, New York, 1989, pp. 31–62. MR1009792 (90g:11069)
10. R. K. Guy, *Unsolved Problems in Number Theory*, Problem Books in Mathematics, Springer-Verlag, New York, 1994. MR1299330 (96e:11002)
11. G. H. Hardy and J. E. Littlewood, *Some problems of "Partitio numerorum": III. On the expression of a number as a sum of primes*, Acta Math. **44** (1922), 1–70.
12. S. Ling and J. Oesterlé, *The Shimura subgroup of* $J_0(N)$, Astérisque (1991), no. 196–197, 171–203 (1992). MR1141458 (93b:14038)
13. B. Mazur, *Three lectures about the arithmetic of elliptic curves*, http://swc.math.arizona.edu/notes/files/98MazurLN.pdf.
14. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186. MR0488287 (80c:14015)
15. L. Merel, *L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de* $J_0(p)$ [*Weil pairing of the Shimura subgroup and the cuspidal subgroup of* $J_0(p)$], J. reine angew. Math. **477** (1996), 71–115 (French). MR1405312 (97f:11045)
16. J.-F. Mestre and J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance* m*-ième* [*Semistable Weil curves with discriminant an* m*th power*], J. reine angew. Math. **400** (1989), 173–184 (French). MR1013729 (90g:11078)
17. D. Mumford, *Abelian Varieties*, Tata Institute of Fundamental Research Studies in Mathematics, no. 5, Oxford University Press, London, 1970. MR0282985 (44 #219)
18. O. Neumann, *Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. I*, Math. Nachr. **49** (1971), 107–123 (German). MR0337999 (49 #2767a)
19. O. Neumann, *Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. II*, Math. Nachr. **56** (1973), 269–280 (German). MR0338000 (49 #2767b)
20. A. P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462. MR0364259 (51 #514)
21. K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, Arithmetic Algebraic Geometry (Park City, Utah, 1999), IAS/Park City Math. Ser., vol. 9, American Mathematical Society, Rhode Island, 2001, pp. 143–232. MR1860042 (2002h:11047)
22. B. Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. (2) **10** (1975), 367–378. MR0371904 (51 #8121)
23. W. A. Stein and M. Watkins, *A database of elliptic curves—first*

*report*, Algorithmic Number Theory (Sydney 2002) (C. Fieker and D. Kohel, eds.), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 267–275. MR2041090

24. G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Invent. Math. **98** (1989), no. 1, 75–106. MR1010156 (90m:11089)
25. S.-L. Tang, *Congruences between modular forms, cyclic isogenies of modular elliptic curves and integrality of* p-*adic* L-*functions*, Trans. Amer. Math. Soc. **349** (1997), no. 2, 837–856. MR1376558 (98b:11056)
26. V. Vatsal, *Multiplicative subgroups of* $\mathrm{J}_0(\mathrm{N})$ *and applications to elliptic curves*, preprint, 2003, http://www.math.ubc.ca/∼vatsal/page.html.
27. M. Watkins, *Computing the modular degree of an elliptic curve*, Experiment. Math. **11** (2002), no. 4, 487–502. MR1969641 (2004c:11091)
28. A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551. MR1333035 (96d:11071)

**MR2053457** 11F33 11F67 11F80 11G18

**Dummigan, Neil** (4-SHEF-PM)**;**
**Stein, William [Stein, William A.]** (1-HRV)**;**
**Watkins, Mark [Watkins, Mark J.]** (1-PAS)

**Constructing elements in Shafarevich-Tate groups of modular motives. (English. English summary)**

*Number theory and algebraic geometry*, 91–118, *London Math. Soc. Lecture Note Ser.*, 303, *Cambridge Univ. Press*, *Cambridge*, 2003.

**MR2029169 (2004k:11094)** 11G18 11F11 14H40

**Conrad, Brian** (1-MI)**; Edixhoven, Bas** (NL-LEID-MI)**;**
**Stein, William [Stein, William A.]** (1-HRV)

$J_1(p)$ **has connected fibers. (English. English summary)**

*Doc. Math.* **8** (2003), 331–408 (*electronic*).

Let $p$ be a prime number and $J_1(p)$ the Jacobian of the moduli curve $X_1(p)$ over $\mathbf{Q}$ that parametrizes pairs $(E, P)$ where $E$ is an elliptic curve and $P$ is a point of $E$ of order $p$. One of the main results of the paper is that $J_1(p)$ has trivial component group at $p$.

The proof involves the study of the component groups at $p$ of Jacobians of intermediate curves between $X_1(p)$ and $X_0(p)$. (The case of $X_0(p)$ was treated by Mazur-Rapoport.) More precisely, for any subgroup $H$ of $(\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$ the authors consider the curve $X_H(p) =$

$X_1(p)/H$ and its Jacobian $J_H(p)$. They prove that the natural surjective map $J_H(p) \to J_0(p)$ induces an injection $\Phi(J_H(p)) \to \Phi(J_0(p))$ between the component groups of mod $p$ fibers and that $\Phi(J_H(p))$ is cyclic of order $|H|/\gcd(|H|, 6)$ over $\overline{\mathbf{F}}_p$. Furthermore, viewing $\Phi(J_0(p))$ as a quotient of $(\mathbf{Z}/p\mathbf{Z})^\times/\{\pm 1\}$, the image of $\Phi(J_H(p))$ coincides with the image of $H$. In particular, $\Phi(J_H(p))$ is always Eisenstein in the sense of Mazur and Ribet and $\Phi(J_1(p))$ is trivial. In order to reach these results they compute a regular proper model of $X_H(p)$ over $\mathbf{Z}_{(p)}$, adapting the classical Jung-Hirzebruch method for complex sufaces. This method enables them to resolve tame cyclic quotient singularities on curves over a discrete valuation ring.

The last part of the paper is devoted to computer computations concerning the arithmetic of $J_1(p)$. The authors give a conjectural formula for the order of the torsion subgroup of $J_1(p)(\mathbf{Q})$.

*Alessandra Bertapelle* (I-PADV-PM)

**[References]**


1. A. Agashé, *On invisible elements of the Tate-Shafarevich group*, C. R. Acad. Sci. Paris Sér. I Math. 328 (1999), no. 5, 369–374. MR1678131 (2000e:11083)
2. A. Agashe and W. Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory 97 (2002), no. 1, 171–185. MR1939144 (2003h:11070)
3. A. Agashe and W. Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank* 0, to appear in Math. Comp. MR2085902
4. A. Agashe and W. Stein, *The Manin constant, congruence primes, and the modular degree*, in progress.
5. M. Artin, *Algebraic approximation of structures over complete local rings*, Publ. Math. IHES, 36 (1969), 23–58. MR0268188 (42 #3087)
6. L. Bégueri, *Dualité sur un corps local à corps résiduel algébriquement clos*, Mém. Soc. Math. France (1980/81), no. 4. MR0615883 (82k:12019)
7. A. Bertapelle, *On perfectness of Grothendieck's pairing for the ℓ-parts of component groups*, J. Reine Angew. Math., 538 (2001), 223–236. MR1855757 (2002k:14072)
8. A. Bertapelle and S. Bosch, *Weil restriction and Grothendieck's duality conjecture*, Journal of algebraic geometry, 9 (2000), 155–164. MR1713523 (2000i:14065)
9. S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)

10. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), no. 3–4, 235–265, Computational algebra and number theory (London, 1993). MR1484478
11. J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus* 2, Cambridge University Press, Cambridge, 1996. MR1406090 (97i:11071)
12. J. W. S. Cassels, A. Fröhlich, *Algebraic Number Theory*, Academic Press, London, 1967. MR0215665 (35 #6500)
13. T. Chinburg "Minimal models of curves over Dedekind rings" in *Arithmetic Geometry* (Cornell/Silverman ed.), Springer-Verlag, Berlin, 1986. MR0861982
14. J. E. Cremona, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997. MR1628193 (99e:11068)
15. P. Deligne and M. Rapoport, "Les schémas de modules de courbes elliptiques" in *Modular Functions of One Variables II*, Lecture Notes in Mathematics 349, Springer-Verlag, Berlin, 1973. MR0337993 (49 #2762)
16. F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem, Providence, RI, 1995, pp. 39–133. MR1357209 (97g:11044)
17. A. Edelman, *The mathematics of the Pentium division bug*, SIAM Rev. 39 (1997), no. 1, 54–67. MR1439485 (98a:68009)
18. S. J. 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). MR1141457 (92k:11059)
19. S. J. Edixhoven, *On the Manin constants of modular elliptic curves*, Arithmetic algebraic geometry (Texel, 1989), Birkhäuser Boston, Boston, MA, 1991, pp. 25–39. MR1085254 (92a:11066)
20. S. J. Edixhoven, *Néron models and tame ramification*, Compositio Math., 81 (1992), 291–306. MR1149171 (93a:14041)
21. S. J. Edixhoven, *Modular parameterizations at primes of bad reduction*, in preparation.
22. S. J. Edixhoven, *Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod* 2 *of weight one*, preprint.
23. M. Emerton, *Optimal Quotients of Modular Jacobians*, to appear in Math. Ann. MR2021024
24. E. Freitag and R. Kiehl, *Étale cohomology and the Weil conjec-*

*tures*, Springer-Verlag, Berlin, 1988. MR0926276 (89f:14017)
25. W. Fulton, *Introduction to toric varieties*, Annals of Mathematics Studies 131, Princeton University Press, 1993. MR1234037 (94g:14028)
26. J. González and J.-C. Lario, **Q**-*curves and their Manin ideals*, Amer. J. Math. 123 (2001), no. 3, 475–503. MR1833149 (2002e:11070)
27. A. Grothendieck, *Éléments de géométrie algébrique.* $\mathrm{IV}_4$. Étude locale des schémas et des morphismes de schémas, Inst. Hautes Études Sci. Publ. Math. (1966), no. 28. MR0217086 (36 #178)
28. A. Grothendieck, *Groupes de monodromie en géométrie algébrique. I*, Springer-Verlag, Berlin, 1973, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I), Lecture Notes in Mathematics, Vol. 288. MR0354656 (50 #7134)
29. A. Grothendieck, *Groupes de monodromie en géométrie algébrique. II*, Springer-Verlag, Berlin, 1973, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II), Dirigé par P. Deligne et N. Katz, Lecture Notes in Mathematics, Vol. 340. MR0354657 (50 #7135)
30. B. H. Gross, *A tameness criterion for Galois representations associated to modular forms* (*mod $p$*), Duke Math. J. 61 (1990), no. 2, 445–517. MR1074305 (91i:11060)
31. A. Joyce, *The Manin Constant of an Optimal Quotient of* $J_0(431)$, preprint, 2003.
32. K. Kato, *$p$-adic Hodge theory and values of zeta functions of modular forms*, 244 page preprint.
33. N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. 62 (1981), no. 3, 481–502. MR0604840 (82d:14025)
34. N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Princeton University Press, Princeton, N. J., 1985. MR0772569 (86i:11024)
35. D. R. Kohel and W. A. Stein, *Component Groups of Quotients of* $J_0(N)$, Proceedings of the 4th International Symposium (ANTS-IV), Leiden, Netherlands, July 2–7, 2000 (Berlin), Springer, 2000. MR1850621 (2002h:11051)
36. V. A. Kolyvagin and D. Y. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Algebra i Analiz 1 (1989), no. 5, 171–196. MR1036843 (91c:11032)
37. D. S. Kubert and S. Lang, *Modular units*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science], vol. 244, Springer-Verlag, New York, 1981.

MR0648603 (84h:12009)

38. S. Lang, *Introduction to modular forms*, Springer-Verlag, Berlin, 1995, With appendixes by D. Zagier and W. Feit, Corrected reprint of the 1976 original. MR1363488 (96g:11037)
39. S. Lichtenbaum, *Curves over discrete valuation rings*, American Journal of Mathematics, 90 (1968), 380–405. MR0230724 (37 #6284)
40. J. Lipman, *Desingularization of two-dimensional schemes*, Annals of Mathematics, 107 (1978), 151–207. MR0491722 (58 #10924)
41. Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford University Press, Oxford, 2002. MR1917232 (2003g:14001)
42. Q. Liu and D. Lorenzini, *Models of curves and finite covers*, Compositio Math., 118 (1999), 61–102. MR1705977 (2000f:14033)
43. W. Lütkebohmert, *On compactification of schemes*, Manuscripta Mathematica, 80 (1993), 95–111. MR1226600 (94h:14004)
44. H. Matsumura, *Commutative ring theory*, Cambridge University Press, Cambridge, 1986, Translated from the Japanese by M. Reid. MR0879273 (88h:13001)
45. B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186. MR0488287 (80c:14015)
46. B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. 44 (1978), no. 2, 129–162. MR0482230 (80h:14022)
47. L. Merel, *L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de* $J_0(p)$, J. Reine Angew. Math. 477 (1996), 71–115. MR1405312 (97f:11045)
48. A. P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France 102 (1974), 449–462. MR0364259 (51 #514)
49. A. P. Ogg, *Rational points on certain elliptic modular curves*, Analytic number theory (Proc. Sympos. Pure Math., Vol XXIV, St. Louis Univ., St. Louis, Mo., 1972), Amer. Math. Soc., Providence, R.I., 1973, pp. 221–231. MR0337974 (49 #2743)
50. A. P. Ogg, *Rational points of finite order on elliptic curves*, Invent. Math. 12 (1971), 105–111. MR0291084 (45 #178)
51. B. Poonen and M. Stoll, *The Cassels–Tate pairing on polarized abelian varieties*, Ann. of Math. (2) 150 (1999), no. 3, 1109–1149. MR1740984 (2000m:11048)
52. D. Popescu, *General Néron desingularization and approximation*, Nagoya Math Journal, 104 (1986), pp. 85–115. MR0868439 (88a:14007)
53. Michel Raynaud, *Schémas en groupes de type* $(p,\dots,p)$, Bull. Soc.

Math. France 102 (1974), 241–280. MR0419467 (54 #7488)
54. K. Ribet, "On the component groups and the Shimura subgroup of $J_0(N)$", exposé 6, Sém. Th. Nombres, Université Bordeaux, 1987–88. MR0993107 (91b:11070)
55. K. Ribet, "Irreducible Galois representations arising from component groups of Jacobians" in *Elliptic curves, modular forms, and Fermat's Last Theorem*, International Press, 1995. MR1363499 (97h:11059)
56. M. Schlessinger, *Infinitesimal deformations of singularities*, 1964 Harvard Ph.D. thesis, unpublished.
57. J-P. Serre, *Groupes finis d'automorphismes d'anneaux locaux réguliers*, Colloque d'Algèbre (Paris, 1967), Exp. 8 (1968), 11. MR0234953 (38 #3267)
58. J-P. Serre, *Cohomologie des groupes discrets*, Prospects in mathematics (Proc. Sympos., Princeton Univ., Princeton, N.J., 1970), Princeton Univ. Press, Princeton, N.J., 1971, pp. 77–169. Ann. of Math. Studies, No. 70. MR0385006 (52 #5876)
59. J-P. Serre, *Lie algebras and Lie groups*, second ed., Lecture Notes in Mathematics, vol. 1500, Springer-Verlag, Berlin, 1992, 1964 lectures given at Harvard University. MR1176100 (93h:17001)
60. J-P. Serre, *Œuvres. Collected papers. IV*, Springer-Verlag, Berlin, 2000, 1985–1998. MR1730973 (2001e:01037)
61. I. Shafarevich, *Lectures on minimal models and birational transformations of two-dimensional schemes*, Tata Institute: Bombay, 1966. MR0217068 (36 #163)
62. G. Shimura, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan 25 (1973), no. 3, 523–544. MR0318162 (47 #6709)
63. G. Shimura, *An introduction to computing modular forms using modular symbols*, to appear in an MSRI proceedings.
64. G. Shimura, *Shafarevich-Tate groups of nonsquare order*, to appear in proceedings of MCAV 2002, Progress of Mathematics. MR2058655
65. G. Stevens, *Stickelberger elements and modular parametrizations of elliptic curves*, Invent. Math. 98 (1989), no. 1, 75–106. MR1010156 (90m:11089)
66. R. Swan, *Néron-Popescu desingularization*, Lectures in Algebra and Geometry 2, International Press, Cambridge (1998), pp. 135–192. MR1697953 (2000h:13006)
67. J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 288–295. MR0175892 (31

#168)
68. J. Watanabe, *Some remarks on Cohen-Macaulay rings with many zero divisors and an application*, J. Algebra 39 (1976), no. 1, 1–14. MR0399117 (53 #2968)

**MR2041090** 11G05 11Yxx

**Stein, William A.** (1-HRV)**;**
**Watkins, Mark [Watkins, Mark J.]** (1-PAS)

**A database of elliptic curves—first report.**

*Algorithmic number theory* (*Sydney*, 2002), 267–275, *Lecture Notes in Comput. Sci.*, 2369, *Springer*, *Berlin*, 2002.

**MR1959271 (2004b:11072)** 11F80 11F11 11F25

**Lario, Joan-C.** (E-UPBMS)**; Schoof, René** (I-ROME2)

**Some computations with Hecke rings and deformation rings. (English. English summary)**

With an appendix by Amod Agashe and William Stein.

*Experiment. Math.* **11** (2002), *no.* 2, 303–311.

Let $E$ be the elliptic curve over $\mathbf{Q}$ of conductor 142, having Weierstrass equation $Y^2+XY=X^3-X^2-X-3$. The representation $\overline{\rho}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})\to \mathrm{GL}_2(\mathbf{F}_3)$ provided by the 3-torsion points is unramified outside 3 and 71. For $N=71,142$ and 284 the authors determine explicitly the structure of the local Hecke algebra $\mathbf{T}_N$ generated over $\mathbf{Z}_3$ by the Hecke operators acting on the weight 2 and level $N$ cusp forms whose associated mod 3 representation is isomorphic to $\overline{\rho}$. More precisely, they show that $\mathbf{T}_N\simeq \mathbf{Z}_3[[X,Y]]/I_N$, where generators of the ideals $I_N$ are explicitly computed. By the results of A. J. Wiles [Ann. of Math. (2) **141** (1995), no. 3, 443–551; MR1333035 (96d:11071)] and R. L. Taylor and Wiles [Ann. of Math. (2) **141** (1995), no. 3, 553–572; MR1333036 (96d:11072)], in the case $N=71$ (resp. $N=284$) the algebra $T_N$ is the universal deformation ring of $\overline{\rho}$ for a deformation problem which is minimal (resp. non-minimal) at 71; it is a complete intersection, as we can directly see from the description given in this paper. For the case $N=142$ two natural Hecke algebras are considered, corresponding to the eigenvalues $\pm 1$ for the Hecke operator $T_2$. Both algebras turn out to be complete intersections. The main tool of the construction is the determination, in the appendix, of a bound (depending on the level $N$) on the greatest index $n$ such that the Hecke operators $T_r$ with $r\le n$ generate the whole Hecke algebra. This allows the authors to do computations by dealing with a finite number of vectors with entries in $\mathbf{Z}_3$. *Lea Terracini* (I-TRIN)

**[References]**

1. G. Cornell, J.H. Silverman and G. Stevens, Eds. *Modular forms and Fermat's Last Theorem*, Springer-Verlag, New York 1997. MR1638473 (99k:11004)
2. B. J. Birch and W. Kuyk. *Modular Functions of One Variable IV*, Lecture Notes in Mathematics **476**, Springer-Verlag, Berlin-Heidelberg, 1975. MR0376533 (51 #12708)
3. J. Cremona. *Algorithms for modular elliptic curves*, Cambridge University Press, Cambridge, UK, 1992. MR1201151 (93m:11053)
4. H. Darmon. "Serre's conjectures." in *Seminar on Fermat's Last Theorem 1993–1994*, Kumar Murty ed., pp. 135–153, Canadian Mathematical Society, CMS Conference Proceedings **17**, 1995. MR1357210 (96h:11048)
5. E. De Shalit. "Hecke rings and universal deformation rings." Chapter XIV in *Modular Forms and Fermat's Last Theorem*, G. Cornell, J.H. Silverman, and G. Stevens, eds., Springer-Verlag, New York 1997. MR1638487
6. B. De Smit, K. Rubin, and R. Schoof. "Criteria for Complete Intersections." Chapter XI in *Modular Forms and Fermat's Last Theorem*, G. Cornell, J.H. Silverman, and G. Stevens, eds., Springer-Verlag, New York 1997. MR1638484
7. F. Diamond. "The refined conjecture of Serre." in *Elliptic Curves, Modular Forms and Fermat's Last Theorem*, J. Coates, S. Yau, eds., pp. 22–37, International Press, Cambridge, 1995. MR1363493 (97b:11065)
8. F. Diamond, and K. Ribet. "$\ell$-adic Modular Deformations and Wiles's "Main Conjecture" ", Chapter XII in *Modular Forms and Fermat's Last Theorem*, G. Cornell, J.H. Silverman, and G. Stevens, eds., Springer-Verlag, New York 1997. MR1638485
9. S. J. Edixhoven. "Serre's conjecture." Chapter VII in *Modular Forms and Fermat's Last Theorem*, G. Cornell, J.H. Silverman, and G. Stevens, eds., Springer-Verlag, New York 1997. MR1638480
10. S. Gelbart. "Three lectures on the modularity of $\bar{\rho}_{E,3}$ and the Langlands reciprocity conjecture." Chapter VI in *Modular Forms and Fermat's Last Theorem*, G. Cornell, J.H. Silverman, and G. Stevens, eds., Springer-Verlag, New York 1997. MR1638479
11. B. Mazur. "Deformation theory of Galois representations in Galois groups over **Q**." Chapter VIII in *Modular Forms and Fermat's Last Theorem*, G. Cornell, J.H. Silverman, and G. Stevens, eds., Springer-Verlag, New York 1997. MR1638481
12. A. Rio. *Representacions de Galois octaèdriques*, Tesi Doctoral,

Universitat de Barcelona (1995).
13. J.-P. Serre. "Sur les représentations de degré 2 de Gal($\overline{\mathbf{Q}}/\mathbf{Q}$)." *Duke Math. Journal* **54** (1987), 179–230. MR0885783 (88g:11022)
14. J.-P. Serre. "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques." *Invent. Math.* **15** (1972), 259–331. MR0387283 (52 #8126)
15. W. A. Stein. HECKE package, Magma V2.7 or higher, 2000.
16. J. Sturm. "On the Congruence of Modular Forms." in *Number theory (New York, 1984–1985)*, 275–280, Lecture Notes in Math., 1240, Springer, Berlin-New York, 1987. MR0894516 (88h:11031)
17. R. Taylor and A. Wiles. "Ring-theoretic properties of certain Hecke algebras." *Ann. Math.* **141** (1995), 553–572. MR1333036 (96d:11072)
18. J. Tilouine. "Hecke algebras and the Gorenstein property." Chapter X in *Modular Forms and Fermat's Last Theorem*, G. Cornell, J.H. Silverman, and G. Stevens, eds., Springer-Verlag, New York 1997. MR1638483
19. A. Wiles. "Modular elliptic curves and Fermat's Last Theorem." *Ann. Math.* **141** (1995), 443–551. MR1333035 (96d:11071)

**MR1939144 (2003h:11070)** 11G40 11G10 14K15

**Agashe, Amod** (1-TX)**;**
**Stein, William [Stein, William A.]** (1-HRV)

**Visibility of Shafarevich-Tate groups of abelian varieties. (English. English summary)**

*J. Number Theory* **97** (2002), *no.* 1, 171–185.

To a short exact sequence $0 \to A \to J \to Q \to 0$ of abelian varieties over a field $K$ corresponds a long exact sequence

$$0 \to A(K) \to J(K) \to Q(K) \to H^1(K, A) \to H^1(K, J) \to \cdots$$

of cohomology groups. B. C. Mazur says that a class $c \in H^1(K, A)$ is visible in $J$ if it gets killed in $H^1(K, J)$. The authors show that every class $c$ is visible in some $J$ (Proposition 1.3)—indeed, one can take $J$ to have dimension less than $dn^{2d}$, where $d$ is the dimension of $A$ and $n$ is the order of $c$ in $H^1(K, A)$ (Proposition 2.3).

When $K$ is a number field, the notion of visibility in $J$ applies to elements of the subgroup $Ш(A) \subset H^1(K, A)$ of those classes whose restriction to every completion of $K$ is trivial. If $d = 1$, the upper bound $dn^{2d} = n^2$ can be improved to $n$ for elements of $Ш(A)$ (Proposition 2.4).

The main theorem (Theorem 3.1) provides a method for constructing elements of the kernel of $Ш(A) \to Ш(J)$, which is the $J$-visible subgroup of Ш$(A)$. Namely, if one can find an abelian subvariety $B \subset J$ and an integer $n$ satisfying a certain number of properties which are too technical to reproduce here, then there is a natural map $\varphi$ from $B(K)/nB(K)$ to the $J$-visible subgroup of Ш$(A)$; the order of the kernel of $\varphi$ is at most $n^r$, where $r$ is the rank of $A(K)$.

As an application, the authors give an example (Proposition 4.1) of a 20-dimensional abelian subvariety $A$ of $J_0(389)$ and an elliptic curve $B \subset J_0(389)$ such that by taking $J = A + B$ and $n = 5$ in the main theorem, one concludes that $\varphi$ embeds $(\mathbf{Z}/5\mathbf{Z})^2$ into the subgroup of $J$-visible elements of Ш$(A)$, thus providing evidence for the Birch and Swinnerton-Dyer conjecture in this case.

As another application (Proposition 4.2), the authors treat the elliptic curve $E$ of conductor 5389 considered by J. E. Cremona and B. C. Mazur [Experiment. Math. **9** (2000), no. 1, 13–28; MR1758797 (2001g:11083)] for which the conjectural order of Ш$(E)$ is 9 but no element of order 3 is visible in $J_0(5389)$. The authors produce 9 elements of Ш$(E)$ and show that they are all visible at the higher level of $J_0(7 \cdot 5389)$. *Chandan Singh Dalawat* (6-HCRI)

**[References]**

1. A. Agashe and W.A. Stein, Visible Evidence for the Birch and Swinnerton-Dyer Conjecture for Rank 0 Modular Abelian Varieties, preprint. MR2085902
2. S. Bosch, W. Lütkebohmert, and M. Raynaud, "Néron Models," Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)
3. W. Bosma, J. Cannon, and C. Playoust, The magma algebra system. I. The user language, *J. Symbolic Comput.* **24**, No. 3-4 (1997), 235–265; Computational Algebra and Number Theory, London, 1993. MR1484478
4. J.W.S. Cassels, Arithmetic on curves of genus 1. V. Two counterexamples, *J. London Math. Soc.* **38** (1963), 244–248. MR0148664 (26 #6171)
5. J.E. Cremona, *Elliptic curves of conductor* $\leqslant$ 12000, http://www.maths.nott.ac.uk/personal/jec/ftp/data/.
6. J.E. Cremona, "Algorithms for Modular Elliptic Curves," 2nd ed., Cambridge Univ. Press, Cambridge, UK, 1997. MR1628193 (99e:11068)
7. J.E. Cremona and B. Mazur, Visualizing elements in the Shafarevich-Tate group, *Exp. Math.* **9**, No. 1 (2000), 13–28. MR1758797 (2001g:11083)
8. B. Edixhoven, The weight in Serre's conjectures on modular forms, *Invent. Math.* **109**, No. 3 (1992), 563–594. MR1176206

(93h:11124)

9. A. Grothendieck, Éléments de géométric algébrique. IV. Étude locale des schémas et des morphismes de schémas. II, *Inst. Hautes Études Sci. Publ. Math.* No. 24 (1965), 231. MR0199181 (33 #7330)
10. A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas. III, *Inst. Hautes Études Sci. Publ. Math.* No. 28 (1966), 255. MR0217086 (36 #178)
11. A. Grothendieck, Éléments de géométrie algébrique. IV. Étude locale des schémas et des morphismes de schémas IV, *Inst. Hautes Études Sci. Publ. Math.* No. 32 (1967), 361. MR0238860 (39 #220)
12. A. Grothendieck, "Schémas en groupes. I: Propriétés générales des schémas en groupes," Springer-Verlag, Berlin, 1970. MR0274458 (43 #223a)
13. T. Klenke, "Modular Varieties and Visibility," Ph.D. thesis, Harvard University, 2001.
14. S. Lang and J. Tate, Principal homogeneous spaces over abelian varieties, *Amer. J. Math.* **80** (1958), 659–684. MR0106226 (21 #4960)
15. B. Mazur, Visualizing elements of order three in the Shafarevich-Tate group, *Asian J. Math.* **3**, No. 1 (1999), 221–232. MR1701928 (2000g:11048)
16. J.S. Milne, "Arithmetic Quality Theorems," Academic Press Inc., Boston, MA, 1986. MR0881804 (88e:14028)
17. C. O'Neil, The period-index obstruction for elliptic curves, *J. Number Theory*, to appear. MR1924106 (2003f:11079)
18. K.A. Ribet, Raising the levels of modular representations, *in* "Séminaire de Théorie des Nombres," Paris 1987–88, pp. 259–271, Birkhäuser, Boston, MA, 1990. MR1042773 (91g:11055)
19. J-P. Serre, "Local Fields," Springer-Verlag, New York, 1979 (translated from the French by Marvin Jay Greenberg). MR0554237 (82e:12016)
20. J. Sturm, On the congruence of modular forms, "Number Theory (New York, 1984–1985)," pp. 275–280, Springer, Berlin, 1987. MR0894516 (88h:11031)

**MR1900139 (2003c:11059)** 11G05 11G18

**Stein, William A.** (1-HRV)

**There are genus one curves over $\mathbb{Q}$ of every odd index. (English. English summary)**

*J. Reine Angew. Math.* **547** (2002), 139–147.

For a genus 1 curve $X$ over a field $K$, let $r$ be the smallest degree of an extension $L|K$ such that $X(L)$ is non-empty, called the index of $X|K$. The author shows, for each $r$ not divisible by 8, that there are infinitely many genus 1 curves over $K$ of index $r$, partially answering a question of S. Lang and J. Tate [Amer. J. Math. **80** (1958), 659–684; MR0106226 (21 #4960)]. The paper starts by giving a cohomological definition of the index $r$ of $X|K$ and then some background on Heegner points and Kolyvagin's Euler system. The author proves an intermediate result for $K = \mathbf{Q}$ using Kolyvagin's Euler system. Using some additional computations, the author then deduces the main result by considering twists of $E = X_0(17)$. *Imin Chen* (3-SFR-MS)

**[References]**

1. C. Breuil, B. Conrad, F. Diamond, and R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises, J. Amer. Math. Soc. **14** (2001) no. 4, 843–939. MR1839918 (2002d:11058)
2. D. Bump, S. Friedberg, and J. Hoffstein, Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic $L$-functions and their derivatives, Ann. Math. (2) **131** (1990), no. 1, 53–127. MR1038358 (92e:11053)
3. J. W. S. Cassels, Arithmetic on curves of genus 1. IV. Proof of the Hauptvermutung, J. reine angew. Math. **211** (1962), 95–112. MR0163915 (29 #1214)
4. J. W. S. Cassels, Arithmetic on curves of genus 1. V. Two counterexamples, J. London Math. Soc. **38** (1963), 244–248. MR0148664 (26 #6171)
5. J. W. S. Cassels, Diophantine equations with special reference to elliptic curves, J. London Math. Soc. **41** (1966), 193–291. MR0199150 (33 #7299)
6. J. E. Cremona, Algorithms for modular elliptic curves, second ed., Cambridge University Press, Cambridge 1997. MR1628193 (99e:11068)
7. J. E. Cremona, Elliptic curves of conductor $\leqq$ 12000, http://www.maths.nott.ac.uk/personal/jec/ftp/data/.
8. B. Gross and D. Zagier, Heegner points and derivatives of $L$-series, Invent. Math. **84** (1986), no. 2, 225–320. MR0833192 (87j:11057)

9. B. H. Gross, Kolyvagin's work on modular elliptic curves, $L$-functions and arithmetic (Durham 1989), Cambridge Univ. Press, Cambridge (1991), 235–256. MR1110395 (93c:11039)
10. V. A. Kolyvagin, On the structure of Shafarevich-Tate groups, Algebraic geometry (Chicago, IL, 1989), Springer, Berlin (1991), 94–121. MR1181210 (94b:11055)
11. S. Lang and J. Tate, Principal homogeneous spaces over abelian varieties, Amer. J. Math. **80** (1958), 659–684. MR0106226 (21 #4960)
12. S. Lichtenbaum, Duality theorems for curves over $p$-adic fields, Invent. Math. **7** (1969), 120–136. MR0242831 (39 #4158)
13. W. G. McCallum, Kolyvagin's work on Shafarevich-Tate groups, $L$-functions and arithmetic (Durham 1989), Cambridge Univ. Press, Cambridge (1991), 295–316. MR1110398 (92m:11062)
14. J. S. Milne, Arithmetic duality theorems, Academic Press Inc., Boston, Mass., 1986. MR0881804 (88e:14028)
15. M. R. Murty and V. K. Murty, Non-vanishing of $L$-functions and applications, Birkhäuser Verlag, Basel 1997. MR1482805 (98h:11106)
16. C. O'Neil, The Period-Index Obstruction for Elliptic Curves, J. Number Th., to appear. MR1924106 (2003f:11079)
17. K. A. Ribet and W. A. Stein, Lectures on Serre's conjectures, IAS/Park City Math. Ser. **9** (2001). MR1860042 (2002h:11047)
18. K. Rubin, The work of Kolyvagin on the arithmetic of elliptic curves, Arithmetic of complex manifolds (Erlangen 1988), Springer, Berlin (1989), 128–136. MR1034261 (91i:11070)
19. J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), no. 4, 259–331. MR0387283 (52 #8126)
20. J.-P. Serre, Travaux de Wiles (et Taylor,...). I, Astérisque **237**, Exp. No. 803, 5 (1996), 319–332, Séminaire Bourbaki, Vol. 1994/95. MR1423630 (97m:11076)
21. I. R. Shafarevich, Exponents of elliptic curves, Dokl. Akad. Nauk SSSR (N.S.) **114** (1957), 714–716. MR0094363 (20 #881)

**MR1897901 (2003c:11052)** 11F80

**Buzzard, Kevin** (4-LNDIC); **Stein, William A.** (1-HRV)

**A mod five approach to modularity of icosahedral Galois representations. (English. English summary)**

*Pacific J. Math.* **203** (2002), *no.* 2, 265–282.

Let $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\mathbf{C})$ be a continuous irreducible two-dimensional complex representation of the absolute Galois group of the field $\mathbf{Q}$ of rational numbers. Assume further that $\rho$ is odd, that is, the image of a complex conjugation element in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ has determinant $-1$. A special case of the strong Artin conjecture asserts that there should be a weight one cuspidal newform $f$ whose $L$-function $L(s,f)$ matches the Artin $L$-function $L(s,\rho)$ attached to $\rho$; briefly, $\rho$ should be modular. The conjecture is known to hold when the image of $\rho$ (a finite subgroup of $\mathrm{GL}_2(\mathbf{C})$) is solvable [R. P. Langlands, *Base change for* GL(2), Ann. of Math. Stud., 96, Princeton Univ. Press, Princeton, N.J., 1980; MR0574808 (82a:10032); J. Tunnell, Bull. Amer. Math. Soc. (N.S.) **5** (1981), no. 2, 173–175; MR0621884 (82j:12015)]. In the remaining cases the projective image of $\rho$ in $\mathrm{PGL}_2(\mathbf{C})$ is isomorphic to the alternating group $A_5$, the group of rotational symmetries of the icosahedron. For these "icosahedral" Artin representations modularity was (until recently—see below) unknown except in a handful of cases [J. P. Buhler, *Icosahedral Galois representations*, Lecture Notes in Math., 654, Springer, Berlin, 1978; MR0506171 (58 #22019); *On Artin's conjecture for odd* 2*-dimensional representations*, Lecture Notes in Math., 1585, Springer, Berlin, 1994; MR1322315 (95i:11001)].

In the paper under review, Buzzard and Stein demonstrate an effective computational approach to proving the modularity of a class of icosahedral Artin representations. They apply this approach to eight representations, thereby demonstrating the modularity of each. The approach is described in detail for the first representation, of conductor $1376 = 2^5 \cdot 43$, and the necessary data for carrying out the computations for the remaining seven examples are provided.

A summary of the approach: Suppose that $\rho$ is an icosahedral representation which is unramified at 5, and for which the eigenvalues of a Frobenius element at 5 have distinct reduction modulo 5. By the main theorem of [K. Buzzard and R. L. Taylor, Ann. of Math. (2) **149** (1999), no. 3, 905–919; MR1709306 (2000j:11062)], it suffices to establish that the mod 5 reduction $\overline{\rho}$ of $\rho$ is modular; that is, that there is some mod 5 cuspidal eigenform $f$ such that for all but finitely many primes $p$ the eigenvalue of the Hecke operator $T_p$ on $f$ is equal to the trace of $\overline{\rho}$ applied to a Frobenius element at $p$. By computing the space of mod 5 modular forms of weight 5 and appropriate level, the authors identify a mod 5 modular form $f$ whose first few Hecke eigenvalues match the corresponding traces of Frobenius of $\overline{\rho}$; this form is then almost certainly the one required. They then compute enough information about the icosahedral extension of $\mathbf{Q}$ cut out by the mod 5 representation $\overline{\rho}_f$ associated to $f$ to identify it uniquely as an element of Table 1 of [*On Artin's conjecture for odd* 2*-dimensional representations*, Lecture Notes in Math., 1585, Springer, Berlin, 1994; MR1322315 (95i:11001)], which lists icosahedral extensions of $\mathbf{Q}$ of small discriminant, and hence match $\overline{\rho}_f$ with $\overline{\rho}$.

The paper also contains a result which makes it practical to determine computationally when two normalized cuspidal eigenforms of the same level $N > 4$, weight $k$ and character, over a field of characteristic not dividing $N$, are equal: essentially, the number of coefficients of the $q$-expansions of the eigenforms that have to be checked to guarantee equality is at worst linear in $N$ (for fixed $k$). For computational purposes, this improves considerably on similar results of J. Sturm [in *Number theory (New York, 1984–1985)*, 275–280, Lecture Notes in Math., 1240, Springer, Berlin, 1987; MR0894516 (88h:11031)] which require checking on the order of $N^3$ coefficients.

After the first draft of this paper was written, two more relevant articles appeared [K. Buzzard et al., Duke Math. J. **109** (2001), no. 2, 283–318; MR1845181 (2002k:11078); R. Taylor, "On icosahedral Artin representations. II", to appear]. Each of these establishes the modularity of a general icosahedral Artin representation, subject to various local conditions. However, none of the eight examples in this paper is covered by the first of these articles, and only three of them by the second. *Mark Edward Tristan Dickinson* (1-PITT)

**[References]**

1. E. Artin, *Über eine neue Art von L-reihen*, Abh. Math. Sem. in Univ. Hamburg, **3(1)** (1923/1924), 89–108.
2. W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system* I: *The user language*, J. Symb. Comp., **24(3-4)** (1997), 235–265, CMP 1 484 478, Zbl 0898.68039, http://www.maths.usyd.edu.au:8000/u/magma/. MR1484478
3. J.P. Buhler, *Icosahedral Galois representations*, Springer-Verlag, Berlin, 1978, Lecture Notes in Mathematics, Vol. 654, , Zbl 0374.12002. MR0506171 (58 #22019)
4. K. Buzzard, M. Dickinson, N. Shepherd-Barron and R. Taylor, *On icosahedral Artin representations*, Duke Math. J., **109(2)** (2001), 283–318, CMP 1 845 181. MR1845181 (2002k:11078)

5. K. Buzzard and R. Taylor, *Companion forms and weight one forms*, Ann. of Math. (2), **149(3)** (1999), 905–919, , Zbl 0965.11019. MR1709306 (2000j:11062)
6. H. Cohen and J. Oesterlé, *Dimensions des espaces de formes modulaires*, Lecture Notes in Math., **627** (1977), 69–78, , Zbl 0371.10020. MR0472703 (57 #12396)
7. P. Deligne and J-P. Serre, *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup. (4), **7** (1974), 507–530, , Zbl 0321.10026. MR0379379 (52 #284)
8. G. Frey (ed.), *On Artin's conjecture for odd* 2*-dimensional representations*, Springer-Verlag, Berlin, 1994, , Zbl 0801.00004. MR1322315 (95i:11001)
9. B.H. Gross, *A tameness criterion for Galois representations associated to modular forms* (mod $p$), Duke Math. J., **61(2)** (1990), 445–517, , Zbl 0743.11030. MR1074305 (91i:11060)
10. H. Hijikata, *Explicit formula of the traces of Hecke operators for* $\Gamma_0(N)$, J. Math. Soc. Japan, **26(1)** (1974), 56–82, , Zbl 0266.12009. MR0337783 (49 #2552)
11. R.P. Langlands, *Base Change for* GL(2), Princeton University Press, Princeton, N.J., 1980, , Zbl 0444.22007. MR0574808 (82a:10032)
12. L. Merel, *Universal Fourier expansions of modular forms*, On Artin's conjecture for odd 2-dimensional representations (Berlin), Springer, Lecture Notes in Math., **1585** (1994), 59–94, , Zbl 0844.11033. MR1322319 (96h:11032)
13. T. Miyake, *Modular Forms*, Springer-Verlag, Berlin, 1989, Translated from the Japanese by Yoshitaka Maeda, , Zbl 0701.11014. MR1021004 (90m:11062)
14. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, **1**, , Zbl 0872.11023. MR1291394 (95e:11048)
15. W.A. Stein, *Explicit approaches to modular abelian varieties*, U.C. Berkeley, Ph.D. thesis (2000).
16. J. Sturm, *On the congruence of modular forms*, Number theory (New York, 1984–1985), Springer, Berlin, Lecture Notes in Math., **1240** (1987), 275–280, , Zbl 0615.10035. MR0894516 (88h:11031)
17. R. Taylor, *On icosahedral Artin representations* II, in preparation.
18. J. Tunnell, *Artin's conjecture for representations of octahedral type*, Bull. Amer. Math. Soc. (N.S.), **5(2)** (1981), 173–175, , Zbl 0475.12016. MR0621884 (82j:12015)

**MR1901355 (2003m:11074)** 11F67

**Stein, William A.** (1-HRV); **Verrill, Helena A.** (D-HANN-IM)

**Cuspidal modular symbols are transportable. (English. English summary)**

*LMS J. Comput. Math.* **4** (2001), 170–181 (*electronic*).

Summary: "Modular symbols of weight 2 for a congruence subgroup $\Gamma$ satisfy the identity $\{\alpha, \gamma(\alpha)\} = \{\beta, \gamma(\beta)\}$ for all $\alpha$, $\beta$ in the extended upper half plane and $\gamma \in \Gamma$. The analogue of this identity is false for modular symbols of weight greater than 2. This paper provides a definition of transportable modular symbols, which are symbols for which an analogue of the above identity holds, and proves that every cuspidal symbol can be written as a transportable symbol. As a corollary, an algorithm is obtained for computing periods of cusp forms."

**MR1879817 (2003f:11087)** 11G18 11G10 11G40 14K15

**Conrad, Brian** (1-MI); **Stein, William A.** (1-HRV)

**Component groups of purely toric quotients. (English. English summary)**

*Math. Res. Lett.* **8** (2001), *no.* 5-6, 745–766.

Let $R$ be a discrete valuation ring, $K$ its field of fractions and $k$ its residue field. Suppose $J$ is an abelian variety over $K$, endowed with a symmetric principal polarization and let $\pi\colon J \to A$ be an optimal quotient of $J$ meaning that the kernel of $\pi$ is an abelian variety.

The principal polarization on $J$ induces a polarization $\theta_A$ on $A$, whose degree is the square of a positive integer $m_A$.

Assume that the special fibre of the Néron model of $A$ is the extension of a finite group $\Phi_A$ by a torus. Let $X_A$ denote the group of $\overline{k}$-characters of this torus.

Similarly, let $X_J$ denote the group of $\overline{k}$-characters of the toric part of the special fibre of the Néron model of $J$.

A. Grothendieck defined in [*Groupes de monodromie en géométrie algébrique. I*, Lecture Notes in Math., 288, Springer, Berlin, 1972; MR0354656 (50 #7134)] a monodromy pairing between $X_A$ and $X_{A^\vee}$, inducing an exact sequence

$$0 \to X_{A^\vee} \to \mathrm{Hom}(X_A, \mathbf{Z}) \to \Phi_A \to 0$$

and similarly for $J$, the symmetric principal polarization on $J$ allowing one to write the pairing as

$$0 \to X_J \to \mathrm{Hom}(X_J, \mathbf{Z}) \to \Phi_J \to 0.$$

By functoriality of Néron models and characters, $\pi\colon J \to A$ induces a map $\pi^*\colon X_A \to X_J$, the saturation of whose image is denoted by $\mathcal{L}$. One deduces from the monodromy pairing a map $\alpha\colon X_J \to \mathrm{Hom}(\mathcal{L}, \mathbf{Z})$; let $\Phi_X$ be its cokernel. Moreover, let $m_X$ be the order of the finite group $\alpha(X_J)/\alpha(\mathcal{L})$.

The main result of this paper (Theorem 6.1) implies the equality

$$\frac{\#\Phi_A}{m_A} = \frac{\#\Phi_X}{m_X}.$$

This situation is quite common in the context of modular forms, where $J$ is the Jacobian of a modular curve and $A$ arises from a newform. Using modular symbols, one can then compute $m_A$ explicitly. Moreover, using the method of graphs or the ideal theory of quaternion algebras, one can compute $m_X$ and $\Phi_X$. The main theorem of this paper can thus be used to compute $\#\Phi_A$.

Two tables of computations are given.

It should finally be noted that this paper also offers proofs of some more or less well-known facts concerning group schemes, but for which adequate references are missing. They certainly will be of independent interest. *Antoine Chambert-Loir* (F-RENNB-IM)

**[References]**

1. A. Agashe and W. A. Stein, *Visibility of Shafarevich-Tate groups of abelian varieties: Evidence for the Birch and Swinnerton-Dyer conjecture*, (2001). MR1939144 (2003h:11070)
2. S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), 21. Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)
3. C. Chevalley, *Une démonstration d'un théorème sur les groupes algébriques*, J. Math. Pures Appl. (9) **39** 1960, 307–317. MR0126447 (23 #A3743)
4. B. Conrad, *A modern proof of Chevalley's theorem on algebraic groups*, **http://www-math.mit.edu/~dejong/papers/chev.dvi**
5. B. Edixhoven, *L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein"*. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988). Astérisque No. 196-197, (1991), 7–8, 159–170 (1992). MR1141457 (92k:11059)
6. M. Emerton, *Optimal quotients of modular Jacobians*, (2001), preprint. MR2021024
7. E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M.

Stoll, and J. L. Wetherell, *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. Comp. **70** (2001), no. 236, 1675–1697 (electronic). MR1836926 (2002d:11072)

8. A. Grothendieck, *Éléments de géométrie algébrique*, Publications Mathématiques IHES, **4,8,11,17,20,24,28,32**, 1960–7. MR0217083 (36 #177a)
9. A. Grothendieck, *Groupes de monodromie en géométrie algébrique*, Lecture Notes in Math **288**, Springer-Verlag, Heidelberg (1972). MR0354656 (50 #7134)
10. N. Katz, B. Mazur, *Arithmetic moduli of elliptic curves.* Annals of Mathematics Studies, 108. Princeton University Press, Princeton, NJ, 1985. MR0772569 (86i:11024)
11. D. R. Kohel, *Hecke module structure of quaternions.* Class field theory—its centenary and prospect (Tokyo, 1998), 177–195, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001. MR1846458 (2002i:11059)
12. D. R. Kohel and W. A. Stein, *Component Groups of Quotients of $J_0(N)$*, Proceedings of the 4th International Symposium (ANTS-IV), Leiden, Netherlands, July 2–7, 2000 (Berlin), Springer, 2000. MR1850621 (2002h:11051)
13. B. Mazur, *Modular curves and the Eisenstein ideal.* Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33–186 (1978). MR0488287 (80c:14015)
14. J.-F. Mestre, *La méthode des graphes. Exemples et applications.* Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986), 217–242, Nagoya Univ., Nagoya, 1986. MR0891898 (88e:11025)
15. J.-F. Mestre and J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-ième*, J. Reine Angew. Math. **400** (1989), 173–184. MR1013729 (90g:11078)
16. D. Mumford, *Abelian varieties.* Tata Institute of Fundamental Research Studies in Mathematics, No. 5, Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London 1970. MR0282985 (44 #219)
17. K. A. Ribet, *Letter about component groups of elliptic curves*, **arXiv:math.AG/0105124v1** (2001).
18. J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil.* Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 33–52. Lecture Notes in Math., Vol. 476, Springer, Berlin, 1975. MR0393039 (52 #13850)

**MR1860042 (2002h:11047)** 11F80 11F66 11G05

**Ribet, Kenneth A.** (1-CA); **Stein, William A.** (1-HRV)

**Lectures on Serre's conjectures.**

*Arithmetic algebraic geometry* (*Park City*, *UT*, 1999), 143–232, *IAS/Park City Math. Ser.*, 9, *Amer. Math. Soc.*, *Providence*, *RI*, 2001.

This is a nicely written survey article on the conjectures in the title of the paper. The conjectures of Serre in question are about the modularity of mod $p$, 2-dimensional, continuous, odd, absolutely irreducible representations of the absolute Galois group $G_{\mathbf{Q}}$ of $\mathbf{Q}$. There is a more refined version which also predicts certain minimal modular invariants from which these Galois representations arise. While the conjectures in their qualitative form are still wide open there has been considerable progress in proving that the qualitative form of the conjecture implies the refined form. It is this implication, which is a consequence of deep work of many mathematicians, that this paper surveys in the main. The paper also has useful exercises that will be of help to someone wishing to learn about this area, and two appendices by K. Buzzard and B. Conrad on mod $l$ multiplicity one principles and constructions of Galois representations attached to weight 2 newforms.

{For the entire collection see MR1860012 (2002d:11003)}

*Chandrashekhar Khare* (1-UT)

**MR1857596 (2003d:11082)** 11G05

**Merel, Loïc** (F-PARIS6-MI); **Stein, William A.** (1-HRV)

**The field generated by the points of small prime order on an elliptic curve.**

*Internat. Math. Res. Notices* **2001,** *no.* 20, 1075–1082.

Let $p$ be a prime number, and let $\mathbf{Q}(\mu_p)$ denote the $p$th cyclotomic field. The authors prove the following theorem: If there exists an elliptic curve over $\mathbf{Q}(\mu_p)$ such that the points of order $p$ on $E$ are all $\mathbf{Q}(\mu_p)$-rational, then $p=2,3,5,13$, or $p>1000$. (In addition, the case $p=13$ has recently been ruled out by M. Rebolledo.) This result generalizes previous results of L. Merel [Duke Math. J. **110** (2001), no. 1, 81–119; MR1861089 (2002k:11080)], and the techniques used in the two papers are similar. The main new ingredient is the (quite nontrivial) verification of a technical hypothesis on $p$ involving the non-vanishing of certain $L$-functions. The reduction (for each fixed $p$) of the main theorem to the verification of this hypothesis is discussed in Sections 1 and 2 of the paper. The computational methods used for verifying the hypothesis are described in detail in Section 3.

*Matthew H. Baker* (1-GA)

**[References]**


1. A. Agashé, *On invisible elements of the Tate-Shafarevich group*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), 369–374. MR1678131 (2000e:11083)
2. J. Cremona, *Algorithms for Modular Elliptic Curves*, 2d ed., Cambridge Univ. Press, Cambridge, 1997. MR1628193 (99e:11068)
3. L. Merel, *Sur la nature non-cyclotomique des points d'ordre fini des courbes elliptiques*, Duke Math. J. **110**, 81–119. MR1861089 (2002k:11080)
4. J.-F. Mestre, "La méthode des graphes. Exemples et applications" in *Proceedings of the International Conference on Class Numbers and Fundamental Units of Algebraic Number Fields (Katata, 1986)*, Nagoya University, Nagoya, Japan, 1986, 217–242. MR0891898 (88e:11025)


**MR1836926 (2002d:11072)** 11G40 11G10 11G30

**Flynn, E. Victor** (4-LVRP); **Leprévost, Franck** (F-GREN-F); **Schaefer, Edward F.** (1-STCL-CS); **Stein, William A.** (1-HRV); **Stoll, Michael** (D-DSLD-MI); **Wetherell, Joseph L.** (1-SCA)

**Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves. (English. English summary)**

*Math. Comp.* **70** (2001), *no.* 236, 1675–1697 (*electronic*).

For an abelian variety $A$ over a number field $K$, the conjectures of B. J. Birch and H. P. F. Swinnerton-Dyer [J. Reine Angew. Math. **218** (1965), 79–108; MR0179168 (31 #3419)] and of J. T. Tate [in *Séminaire Bourbaki, Vol. 9*, Exp. No. 306, 415–440, Soc. Math. France, Paris, 1995; see MR1610880 (99f:00041) MR1610977 ] relate arithmetic properties of $A$ to the analytic behaviour of its $L$-function $L(A,s)$. The first conjecture states that the rank of the (finitely generated commutative) group $A(K)$ of $K$-rational points on $A$ is equal to the order of vanishing of the function $L(A,s)$ at $s=1$. The second conjecture expresses the leading coefficient $L^*(A,1)$ in the Taylor expansion of $L(A,s)$ at $s=1$ in terms of certain arithmetic invariants of $A$, among them the order of the group $Ш(A,K)$ of those principal homogeneous $A$-spaces over $K$ which become isomorphic to $A$ over every completion of $K$.

Each of these conjectures requires an act of faith even for its statement. For the first one, the analytic continuation of the function $L(A,s)$ to a domain containing the point $s=1$ needs to be assumed; for the second, the finiteness of the group $Ш(A,K)$ needs to be assumed as well. As of now, neither of these two requirements is known to hold in general.

However, for modular abelian varieties $A$ over $\mathbf{Q}$, the analytic continuation of $L(A,s)$ to the whole of $\mathbf{C}$ is known. For such varieties, V. A. Kolyvagin and others [V. A. Kolyvagin and D. Yu. Logachëv, Algebra i Analiz **1** (1989), no. 5, 171–196; MR1036843 (91c:11032)] have shown that if the $L$-function $L(A,s)$ has at most a simple zero at $s=1$, then the order of vanishing equals the rank of the group $A(\mathbf{Q})$ (as predicted by the first conjecture) and the group $Ш(A,\mathbf{Q})$ is finite (so the statement of the second conjecture is meaningful).

One of the triumphs of recent years has been to show that all 1-dimensional abelian varieties over $\mathbf{Q}$ are modular [C. Breuil et al., J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic); MR1839918 (2002d:11058)]. Extensive calculations, beginning with Birch and Swinnerton-Dyer in the early 1960s on one of the first electronic computers at Cambridge, have lent support to the conjectures in this 1-dimensional case [J. E. Cremona, *Algorithms for modular elliptic curves*, Second edition, Cambridge Univ. Press, Cambridge, 1997; MR1628193 (99e:11068)].

The authors extend these calculations to some 2-dimensional cases. They consider thirty-two curves $C$ of genus 2 over $\mathbf{Q}$ whose Jacobians $J$ are modular abelian surfaces. For each $J$ they compute, with a high degree of precision, the leading coefficient $L^*(J,1)$ and the arithmetic invariants $t$ (the order of the torsion subgroup of $J(\mathbf{Q})$), $c$ (the product of the local Tamagawa numbers at the finite places), $R$ (the regulator) and $\Omega$ (the period). Within the accuracy of their computations, the number $L^*(J,1)t^2/cR\Omega$—conjecturally the order of the group $Ш(J,\mathbf{Q})$—does turn out to be an integer. In all thirty-two cases, this integer happens to be equal to the order of the 2-torsion subgroup of $Ш(J,\mathbf{Q})$. So the second conjecture has been reduced for them to the statement that the number $L^*(J,1)t^2/cR\Omega$ is an integer and the group $Ш(J,\mathbf{Q})$ is annihilated by 2. As an example, for the last curve on their list, namely

$$y^2+(x^3+x+1)y+(x^3-x^2-x)=0,$$

the Jacobian $J$ satisfies the conjecture if the number $L^*(J,1)t^2/cR\Omega$, which agrees with 1 to 44 decimal places, is indeed equal to 1 and if the group $Ш(J,\mathbf{Q})$ is trivial. *Chandan Singh Dalawat* (6-HCRI)

**[References]**

1. A. Agashé and W.A. Stein, *Some abelian varieties with visible Shafarevich-Tate groups*, preprint, 2000. MR1772005 (2001g:17019)
2. A. Agashé, and W.A. Stein, *The generalized Manin constant, congruence primes, and the modular degree*, in preparation, 2000.
3. B. Birch and H.P.F. Swinnerton-Dyer, *Notes on elliptic curves. II*, J. Reine Angew. Math., **218** (1965), 79–108. MR0179168 (31 #3419)
4. S. Bosch and Q. Liu, *Rational points of the group of components of a Néron model*, Manuscripta Math, **98** (1999), 275–293. MR1717533 (2000i:11094)
5. S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990. MR1045822 (91i:14034)
6. C. Breuil, B. Conrad, F. Diamond and R. Taylor *On the modularity of elliptic curves over* **Q***: Wild 3-adic exercises.* **http://abel.math.harvard.edu/HTML/Individuals/Richard_Taylor.html** (2000). MR1839918 (2002d:11058)
7. J. Buhler, B.H. Gross and D.B. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank* 3. Math. Comp., **44** (1985), 473–481. MR0777279 (86g:11037)
8. J.W.S. Cassels, *Arithmetic on curves of genus 1. VIII. On conjectures of Birch and Swinnerton-Dyer.*, J. Reine Angew. Math., **217** (1965), 180–199. MR0179169 (31 #3420)
9. J.W.S. Cassels and E.V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Math. Soc., Lecture Note Series 230, Cambridge Univ. Press, Cambridge, 1996. MR1406090 (97i:11071)
10. J.E. Cremona, *Abelian varieties with extra twist, cusp forms, and elliptic curves over imaginary quadratic fields*, J. London Math. Soc. (2), **45** (1992), 404–416. MR1180252 (93h:11056)
11. J.E. Cremona, *Algorithms for modular elliptic curves. 2nd edition*, Cambridge Univ. Press, Cambridge, 1997. MR **93m:**11053 MR1628193 (99e:11068)
12. J.E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group, Experiment. Math.* **9** (2000) 13–28. MR1758797 (2001g:11083)
13. B. Edixhoven, *On the Manin constants of modular elliptic curves*, Arithmetic algebraic geometry (Texel, 1989), Progr. Math., 89, Birkhauser Boston, Boston, MA, 1991, pp. 25–39. MR1085254 (92a:11066)
14. B. Edixhoven, *L'action de l'algèbre de Hecke sur les groupes de*

*composantes des jacobiennes des courbes modulaires est "Eisenstein"*, Astérisque, No. 196-197 (1992), 159–170. MR1141457 (92k:11059)

15. E.V. Flynn, B. Poonen and E.F. Schaefer, *Cycles of quadratic polynomials and rational points on a genus-two curve*, Duke Math. J., **90** (1997), 435–463. MR1480542 (98j:11048)
16. E.V. Flynn and N.P. Smart, *Canonical heights on the Jacobians of curves of genus 2 and the infinite descent*, Acta Arith., **79** (1997), 333–352. MR1450916 (98f:11066)
17. G. Frey and M. Müller, *Arithmetic of modular curves and applications*, in *Algorithmic algebra and number theory*, Ed. Matzat et al., Springer-Verlag, Berlin, 1999, pp. 11–48. MR **00a:**11095 MR1672093 (2000a:11095)
18. B.H. Gross and D.B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math., **84** (1986), 225–320. MR0833192 (87j:11057)
19. A. Grothendieck, *Groupes de monodromie en géométrie algébrique*, SGA 7 I, Exposé IX, Lecture Notes in Math. vol. 288, Springer, Berlin-Heidelberg-New York, 1972, pp. 313–523. MR0354656 (50 #7134)
20. R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math. 52, Springer-Verlag, New York, 1977. MR0463157 (57 #3116)
21. Y. Hasegawa, *Table of quotient curves of modular curves $X_0(N)$ with genus 2*, Proc. Japan. Acad., **71** (1995), 235–239. MR1373390 (97e:11071)
22. D.R. Kohel and W.A. Stein, *Component groups of quotients of $J_0(N)$*, in: Algorithmic number theory (Leiden, The Netherlands, 2000), Lecture Notes in Computer Science, 1838, Ed. W. Bosma, Springer, Berlin, 2000, 405–412. MR1850621 (2002h:11051)
23. V.A. Kolyvagin, *Finiteness of $E(\mathbf{Q})$ and $\mathrm{III}(E,\mathbf{Q})$ for a subclass of Weil curves*, Izv. Akad. Nauk SSSR Ser. Mat., **52** (1988), 522–540. MR0954295 (89m:11056)
24. V.A. Kolyvagin and D.Y. Logachev, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Leningrad Math J., **1** (1990), 1229–1253. MR1036843 (91c:11032)
25. S. Lang, *Introduction to modular forms*, Springer-Verlag, Berlin, 1976. MR0429740 (55 #2751)
26. F. Leprévost, *Jacobiennes de certaines courbes de genre 2: torsion et simplicité*, J. Théor. Nombres Bordeaux, **7** (1995), 283–306. MR1413580 (98a:11078)
27. Q. Liu, *Conducteur et discriminant minimal de courbes de genre*

*2*, Compos. Math., **94** (1994), 51–79. MR1302311 (96b:14038)
28. B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math., **44** (1978), 129–162. MR0482230 (80h:14022)
29. J.R. Merriman and N.P. Smart; *Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point*, Math. Proc. Cambridge Philos. Soc., **114** (1993), 203–214. MR1230127 (94h:14031)
30. J.S. Milne, *Arithmetic duality theorems*, Academic Press, Boston, 1986. MR0881804 (88e:14028)
31. J.S. Milne, *Jacobian varieties*, in: *Arithmetic geometry*, Ed. G. Cornell, G. and J.H. Silverman, Springer-Verlag, New York, 1986, pp. 167–212. MR0861976
32. Y. Namikawa and K. Ueno, *The complete classification of fibres in pencils of curves of genus two*, Manuscripta Math., **9** (1973), 143–186. MR0369362 (51 #5595)
33. B. Poonen and E.F. Schaefer, *Explicit descent for Jacobians of cyclic covers of the projective line*, J. Reine Angew. Math., **488** (1997), 141–188. MR1465369 (98k:11087)
34. B. Poonen and M. Stoll, *The Cassels-Tate pairing on polarized abelian varieties*, Ann. of Math. (2), **150** (1999), 1109–1149. MR1740984 (2000m:11048)
35. K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math., **100** (1990), 431–476. MR1047143 (91g:11066)
36. E.F. Schaefer, *Computing a Selmer group of a Jacobian using functions on the curve*, Math. Ann., **310** (1998), 447–471. MR1612262 (99h:11063)
37. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, 1994. MR1291394 (95e:11048)
38. J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. 151, Springer-Verlag, New York, 1994. MR1312368 (96b:11074)
39. M. Stoll, *Two simple 2-dimensional abelian varieties defined over* $\mathbf{Q}$ *with Mordell-Weil rank at least* 19, C. R. Acad. Sci. Paris, Sér. I, **321** (1995), 1341–1344. MR1363577 (96j:11084)
40. M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, to appear in Acta Arith. MR1829626 (2002b:11089)
41. M. Stoll, *On the height constant for curves of genus two*, Acta Arith., **90** (1999), 183–201. MR1709054 (2000h:11069)
42. M. Stoll, *On the height constant for curves of genus two, II*, in

preparation.
43. J. Tate, *On the conjectures of Birch and Swinneron-Dyer and a geometric analog*. Séminaire Bourbaki, **306** 1965/1966. CMP 98:09
44. J.-L. Waldspurger, *Correspondances de Shimura*, Proceedings of the International Congress of Mathematicians, Vol. 1, 2, (Warsaw, 1983), 1984, pp. 525–531. MR0804708 (86m:11036)
45. J.-L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demientier*, J. Math. Pures Appl. (9), **60** (1981), 375–484. MR0646366 (83h:10061)
46. X. Wang, *2-dimensional simple factors of* $J_0(N)$, Manuscripta Math., **87** (1995), 179–197. MR1334940 (96h:11059)

**MR1850621 (2002h:11051)** 11G18 11F11 11G10 11G40 14G35

**Kohel, David R.** (5-SYD); **Stein, William A.** (1-CA)

**Component groups of quotients of $J_0(N)$. (English. English summary)**

*Algorithmic number theory* (*Leiden*, 2000), 405–412, *Lecture Notes in Comput. Sci.*, 1838, *Springer*, *Berlin*, 2000.

Let $A$ be an abelian variety over $\mathbf{Q}$ and let $p$ be a prime number. An important arithmetic invariant attached to $A$ and $p$ is the order of the group $\Phi_{A,p}$ of connected components of the reduction modulo $p$ of the Néron model of $A$ over $\mathbf{Z}$.

To each modular newform $f$ of weight 2 for the congruence subgroup $\Gamma_0(N)$ $(N \geq 1)$, Shimura has associated an abelian variety $A_f$ defined over $\mathbf{Q}$; it is a certain quotient of $J_0(N)$ and has good reduction at primes which do not divide $N$.

The authors give an algorithm for computing the order of $\Phi_{A_f,p}$ when the prime $p$ divides $N$ but $p^2$ does not divide $N$. They include a table listing these orders when $N \leq 127$.

{For the entire collection see MR1850596 (2002d:11002)}

*Chandan Singh Dalawat* (6-HCRI)