ON THE EQUATION $a^p + 2^\alpha b^p + c^p = 0$

Kenneth A. Ribet

University of California, Berkeley

We discuss the equation $a^p + 2^\alpha b^p + c^p = 0$ in which a, b, and c are non-zero relatively prime integers, p is an odd prime number, and α is a positive integer. The technique used to prove Fermat's Last Theorem shows that the equation has no solutions with $\alpha > 1$ or b even. When $\alpha = 1$ and b is odd, there are the two trivial solutions $(\pm1, \mp1, \pm1)$. In 1952, Dénes conjectured that these are the only ones. Using methods of Darmon, we prove this conjecture for $p \equiv 1 \bmod 4$. We link the case $p \equiv 3 \bmod 4$ to conjectures of Frey and Darmon about elliptic curves over $\mathbf{Q}$ with isomorphic mod p Galois representations.

1. Introduction

Let $p \geq 5$ be a prime number. One knows that Fermat's equation $a^p + b^p + c^p = 0$ has no non-zero integral solutions. Indeed, suppose that $a^p + b^p + c^p = 0$, where a, b and c are non-zero. Following G. Frey, one considers the elliptic curve E with equation $y^2 = x(x - a^p)(x + b^p)$. The curve E is simultaneously modular [22, 20] and non-modular [18]. Therefore no triple (a, b, c) with the hypothesized properties could have existed.

Ever since A. Wiles's 1993 announcement that Fermat's Last Theorem can be proved along these lines, it has been clear that the proof sketched above can be adapted to other Diophantine equations having the skeletal form $A + B = C$. In particular, suppose that L is a prime number taken from the set

$$\Sigma = \{\, 3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59 \,\}.$$

The analysis of J.-P. Serre [19, §4.3], combined with the author's theorem [18] and the recent work of Wiles [22] and Taylor-Wiles [20], provides information about the family of equations $a^p + L^\alpha b^p + c^p = 0$.

Theorem 1. *Suppose that p and L are distinct prime numbers, with $p \geq 11$ and $L \in \Sigma$. If $\alpha \geq 0$, then there are no triples of non-zero integers (a, b, c) which satisfy $a^p + L^\alpha b^p + c^p = 0$.*

The proof of this theorem can again be summarized succinctly. A non-zero solution to $a^p + L^\alpha b^p + c^p = 0$ would define a semistable elliptic curve E; this curve would

---

This article was prepared while the author was a research professor at the MSRI, where research is supported in part by NSF grant DMS-9022140. This work was further supported by the investigator's NSF Grant DMS 93-06898. It is a pleasure to thank R. Borcherds, H. Darmon S. Kamienny, I. Kaplansky, B. Mazur and R. Tijdeman for helpful feedback and information.

be modular by [22, 20]. The group of p-division points on E would define an irreducible two-dimensional representation ρ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\mathbf{F}_p$ with very limited ramification. Moreover, ρ would be modular because E is modular. An application of the main theorem of [18] would lead to the statement that ρ arises from the space of weight-two cusp forms on $\Gamma_0(2L)$. As Serre explains in [19], one may deduce a contradiction from this statement for L in Σ.

This article concerns the case $L = 2$, i.e., the equation

$$a^p + 2^\alpha b^p + c^p = 0 \qquad (\star)$$

when p is an odd prime.[1] This equation is qualitatively different from those considered by Serre, since $(\star)$ has the non-zero solutions $a = c = -b$ with $\alpha = 1$. Their presence is connected up with the fact that the elliptic curves E defined by solutions to $(\star)$ are not necessarily semistable. In order to proceed with our analysis, we must exploit the fact that the Shimura-Taniyama conjecture holds for all elliptic curves over $\mathbf{Q}$ defined by equations of the form $y^2 = x(x - A)(x + B)$, even those curves which are not semistable. As K. Rubin and A. Silverberg have observed, this extension of Wiles's theorem follows easily from F. Diamond's refinement [7] of the work of Wiles and Taylor-Wiles. Alternatively, a somewhat simplified proof of the extended theorem has been given by Diamond and Kramer [8]; these authors appeal directly to [22, 20], rather than to [7].

In our analysis, we take α to be an integer between 1 and $p-1$ without loss of generality. Also, for technical reasons we exclude the case $p = 3$. The reader interested in this omitted case may consult Vol. II, pp. 572–573 of Dickson's *History of the Theory of Numbers* [9]. According to this *History*, Euler showed that $a^3 + 4b^3 + c^3 = 0$ has no solutions in non-zero integers, while Legendre established that $a^3 + 2b^3 + c^3 = 0$ has only the trivial solutions with $a = c = -b$. Recently, H. Wasserman [21] has communicated a proof of Euler's result which is inspired by the treatment of $a^3 + b^3 + c^3 = 0$ given by Ireland and Rosen in [12, Ch. 17, §8].

When $\alpha = 1$, the equation $a^p + 2b^p + c^p = 0$ states that the three perfect pth powers a^p, $(-b)^p$ and c^p form an arithmetic progression. As the author learned from R. Tijdeman, there has been considerable interest in arithmetic progressions consisting of perfect nth powers. While it is easy to exhibit three perfect squares which form an arithmetic progression (e.g., 7^2, 13^2 and 17^2), Fermat stated and Euler (among others) proved that four distinct squares cannot form an arithmetic progression. (For a discussion, see [9, Vol. II, Ch. XIV].) Furthermore, as Dickson reports in [9, Vol. II, Ch. XXII], Euler proved that $2a^4 \pm 2b^4$ is a perfect square only when $a = b$; in particular, three distinct fourth powers cannot form an arithmetic progression. (For a proof of this latter fact, cf. [10, Ex. 4, p. 43].)

For pth powers (where p is an odd prime), Dénes [6] made the following conjecture in 1952:

Conjecture 1. Let p be an odd prime. If x, y and z are non-zero integers such that x^p, y^p and z^p form an arithmetic progression, then x, y and z are all equal.

[1] Our study of this equation was suggested by a letter from J. W. Weidenman concerning Diophantine equations which are special cases of $(\star)$. The author wishes to thank him for this inquiry.

Conjecture 1 amounts to the statement that the only solutions to $a^p + 2b^p + c^p = 0$ in non-zero integers are those for which $a = -b = c$. In support of the conjecture, Dénes proved the following theorem [6, Satz 9], which implies the conjecture for all odd primes $p < 31$.

Theorem 2. *Suppose that p is a regular odd prime for which the order of 2 in $(\mathbf{Z}/p\mathbf{Z})^*$ is either an even number or else equal to $\frac{p-1}{2}$. Suppose further that $2^{p-1} \not\equiv 1$ modulo p^2. Then the conjecture is true for p.*

We prove two theorems about the family $(\star)$:

Theorem 3. *The equation $a^p + 2^\alpha b^p + c^p = 0$ has no solution in non-zero integers a, b, c if α satisfies $2 \leq \alpha < p$. Furthermore, there are no solutions to $a^p + 2b^p + c^p = 0$ in relatively prime non-zero integers for which 2 divides abc.*

Given that all elliptic curves $y^2 = x(x-A)(x+B)$ are modular, we obtain Theorem 3 by mimicing the proof of Fermat's Last Theorem which we sketched above.

Theorem 4. *If $p \equiv 1 \bmod 4$, then Conjecture 1 is true for p.*

Theorem 4 is proved by techniques introduced by Darmon in [2, 3]. (See also the discussions in [4, §4] and [5, §4.3].) The condition $p \equiv 1 \bmod 4$ in Theorem 4 is needed so that we can apply the work of B. Mazur [15], F. Momose [17], and S. Kamienny [13] on the rational points of modular curves associated with split Cartan subgroups of $\mathbf{GL}(2, \mathbf{F}_p)$. In fact, we require as well the secondary hypothesis $p \geq 17$ to apply this work, so we do not prove Theorem 4 for $p = 5$ or $p = 13$. Fortunately, these two primes are covered by Dénes's work.

It is perhaps worth stressing that the hypothesis $p \equiv 1 \bmod 4$ will disappear as soon as theorems for non-split Cartan subgroups become available.

2. Frey curves

Let p be an odd prime number. We view $(\star)$ as an equation in the three variables a, b and c with an auxiliary parameter, α. We can and do assume that we have $0 < \alpha < p$. Suppose that (a, b, c) is a solution to $(\star)$ in non-zero relatively prime integers. It is immediate then that a and c are odd; i.e., the three monomials $A = a^p$, $B = 2^\alpha b^p$ and $C = c^p$ are relatively prime. Thus, the congruence $a \equiv -1 \bmod 4$ will be satisfied after possibly multiplying (a, b, c) by -1. We shall normalize our solutions by imposing this congruence. With this normalization in place, the trivial solutions $a = c = -b$ with $\alpha = 1$ are reduced to the single triple $(a, b, c) = (-1, 1, -1)$.

Given a normalized solution of $(\star)$, one forms the Frey elliptic curve E with equation

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

Theorem 5. *The elliptic curve E is modular.*

As indicated above, this theorem was pointed out by Rubin and Silverberg, who deduced it as a consequence of the results of [7]. After learning of the Rubin-Silverberg observation, F. Diamond and K. Kramer gave a more "elementary" proof of the theorem in [8]. This latter article applies the work of Wiles and Taylor-Wiles, but does not rely on the refinements of [7]. It contains a great deal of information about the arithmetic of Frey curves, some of which we shall recall below.

Because of our normalization, the integer A satisfies $A \equiv -1 \bmod 4$; furthermore, B is even. These are the conventions that were employed in [19] and [8]. The calculations of [19, §4.1] show that the conductor N_E of E has the form $2^t \operatorname{rad}'(ABC)$ where t is a non-negative integer. Here, we have written $\operatorname{rad}'(ABC)$ for the product of the odd prime divisors of ABC. In particular, the curve E is semistable at all primes $p \neq 2$. The precise value of t is computed by Diamond and Kramer [8], who find that t is 5, 3, 3, 0 or 1 according as $\operatorname{ord}_2(B)$ is 1, 2, 3, 4, or an integer greater than 4. Thus E is semistable at 2 if and only if B is divisible by 16. Since E is in any case semistable away from 2, E is a semistable elliptic curve precisely when 16 divides B. The minimal discriminant Δ_E of E may be written $2^u(ABC)^2$ where u is an integer which is calculated in [8]. For instance, $u = -8$ when $t = 1$. Therefore

$$\operatorname{ord}_\ell(\Delta_E) \equiv 0 \bmod p$$

for all primes $\ell \neq 2$.

Lemma. *The conductor N_E is a power of 2 if and only if (a, b, c) is the trivial solution $(-1, 1, -1)$.*

Proof. The solution $(-1, 1, -1)$ to $(\star)$ for the value $\alpha = 1$ leads to the elliptic curve $E = E_0$ with equation $y^2 = x(x+1)(x+2)$. A translation in x transforms E_0 into the familiar complex multiplication elliptic curve $y^2 = x^3 - x$ of conductor 32. Conversely, suppose that N_E is a power of 2. Then $\operatorname{rad}'(ABC) = 1$, so that ABC is a power of 2. Since $a \equiv -1 \bmod 4$, we have $a = -1$. Similarly, the odd number c can only be ± 1 and b must be a power of 2. The equation $-1 + 2^\alpha b^p + (\pm 1) = 0$ forces $b = 1$, $\alpha = 1$ and $\pm 1 = -1$. ■

Corollary. *If (a, b, c) is not the trivial solution, then E has multiplicative reduction at some prime $q \neq 2$.*

Proof. This is clear since N_E is a power of 2 times a square-free odd number. ■

For each prime number ℓ, let $E[\ell]$ be the group of ℓ-division points on E, regarded as a two-dimensional representation of $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over the field $\mathbf{F}_\ell$. We recall the following fact.

Proposition 1. *The representation $E[\ell]$ is irreducible for all primes $\ell \geq 5$. Moreover, if E is not semistable, then $E[3]$ is irreducible.*

Proof. First suppose that E is semistable over $\mathbf{Q}$. Then, as was noted in [19], the result to be proved follows easily from a theorem of Mazur [14, 15]. More precisely, suppose that $\ell \geq 5$ and that $E[\ell]$ is reducible. Then E has a rational subgroup C of order ℓ. The semistability hypothesis implies that the action of $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ on C is ramified only at ℓ, and a local study at ℓ then shows that $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ must act on C either trivially or via the mod ℓ cyclotomic character. This implies that some elliptic curve over $\mathbf{Q}$ which is isogenous to E contains a group of rational points which is isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\ell\mathbf{Z}$. The existence of such a curve is incompatible with Ogg's Conjecture, which was proved by Mazur in [14].

Now suppose that E is not semistable; this means that E has additive reduction at 2. Then the indicated irreducibility follows from a stronger statement which is proved by Diamond and Kramer in [8]: Let I be an inertia subgroup of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ for the prime 2; then the action of I on $E[\ell]$ is irreducible if $\ell \geq 3$. Since the proof of this statement is quite elementary, we shall recall it now for the convenience of the reader.

Since E has additive reduction at 2, the 2-part of N_E may be written $2^{2+\delta}$, where δ is the exponent of the Swan conductor of the representation given by the action of I on $E[\ell]$. As we noted above, $2+\delta$ is equal to either 5 or 3; thus δ is an odd number. Assume now that $E[\ell]$ is reducible as an I-module. Then $E[\ell]$ is an extension of one 1-dimensional representation by another, and δ is the sum of the conductors of the two characters associated with the 1-dimensional representations. These characters are in fact inverses of each other, since I acts trivially on the determinant of $E[\ell]$. (This determinant corresponds to the mod ℓ cyclotomic character, which is unramified at 2.) Hence the conductors of the two characters are equal, giving that δ is even. ∎

Corollary. *Suppose that $p \geq 5$ or that $p = 3$ and b is odd. Then $E[p]$ is irreducible.*

Proof. The only point to be checked is that E is non-semistable if $p = 3$ and b is odd. In fact, suppose that $p = 3$. Then E is semistable if and only if b is even. Indeed, if b is even, then 8 divides b^p, so that 16 divides B. Conversely, suppose that 16 divides $B = 2^\alpha b^p$. Since $1 \leq \alpha \leq 2$, it is clear that b is even. ∎

3. Proofs of Theorem 3 and 4

Suppose that $a^p + 2^\alpha b^p + c^p = 0$, where the integers a, b and c are non-zero and relatively prime, and where α satisfies $1 \leq \alpha < p$. It is evident then that a and c are odd. As above, we multiply (a, b, c) by -1 if necessary in order to ensure that a is congruent to 3 mod 4. We again form the Frey curve $E : y^2 = x(x-A)(x+B)$. In the notation introduced above the conductor N_E of E is the product $2^t \operatorname{rad}'(ABC)$, for some integer t in the set $\{0, 1, 3, 5\}$. We have $t \leq 3$ if and only if the even number B is divisible by 4; we have $t = 5$ in the contrary case. We will suppose from now on that $p \geq 5$.

We first prove Theorem 3, i.e., that $t = 5$. Because $p \geq 5$, we may deduce from the Corollary to Proposition 1 that the representation

$$\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{F}_p)$$

defined by $E[p]$ is irreducible. It is modular of level N_E (i.e., it arises from the space of weight-two cusp forms on $\Gamma_0(N_E)$) because E is a modular elliptic curve of conductor N_E. Since Δ_E is a perfect pth power times a power of 2, the representation ρ is finite at each prime $\ell \neq 2$. The main theorem of [18] thus implies that ρ is modular of level 2^t. (Each odd prime ℓ dividing N_E can be jettisoned from the level of ρ.) We conclude that $t = 5$, since there are no non-zero cusp forms of weight two on $\Gamma_0(8)$. Equivalently, $\operatorname{ord}_2(B) = 2$, as asserted by Theorem A.

Remark. In the omitted case $p = 3$, suppose that b is odd. Then $E[3]$ is again an irreducible representation, and the argument we have given may be used to deduce that $\alpha = 1$.

Continuing the argument, we now prove Theorem 4. Let E_0 again be the elliptic curve which is associated with the trivial solution $(-1,1,-1)$, i.e., the elliptic curve over $\mathbf{Q}$ with equation $y^2 = x^3 - x$.

Proposition 2. *The two-dimensional mod p representations of* $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *which are defined by E and E_0 are isomorphic.*

Proof. Let ρ be the mod p representation which is defined by E, i.e., by the space $E[p]$ of p-division points of E; let ρ_0 be the analogue of ρ for E_0. We have seen that the irreducible representation ρ is associated with an eigenform in the space of weight-two cusp forms on $\Gamma_0(2^t) = \Gamma_0(32)$. It is a known fact that this space is one-dimensional; equivalently, $J_0(32)$ is an elliptic curve. (See, e.g., [1, p. 136].) It follows that ρ is the mod p representation $J_0(32)[p]$. In particular, the isomorphism class of ρ is independent of the solution (a,b,c) giving rise to E. Therefore, ρ and ρ_0 are isomorphic, as stated. ∎

We next recall the well known fact that the image of ρ_0 is contained in the normalizer of a Cartan subgroup of $\mathbf{GL}(2,\mathbf{F}_p)$. Indeed, let $R = \mathbf{Z}[\mu_4]$ be the full ring of endomorphisms of E_0. Then $E_0[p]$ is easily seen to be a free rank-1 module over R/pR. Let C be the image of $(R/pR)^*$ in the group of automorphisms of $E_0[p]$, so that C is either $\mathbf{F}_p^* \times \mathbf{F}_p^*$ or $\mathbf{F}_{p^2}^*$, according as p is congruent to 1 or to -1 mod 4. Then C is a Cartan subgroup of $\operatorname{Aut} E_0[p] \approx \mathbf{GL}(2,\mathbf{F}_p)$. One says that C is split or non-split according as p is 1 or-1 mod 4. The restriction of ρ_0 to $\operatorname{Gal}\bigl(\overline{\mathbf{Q}}/\mathbf{Q}(\sqrt{-1})\bigr)$ takes values in C, and the full image of ρ takes values in the normalizer of C in $\mathbf{GL}(2,\mathbf{F}_p)$. The index of C in its normalizer is 2.

Suppose now that $p \equiv 1 \bmod 4$. Then E defines a point on the modular curve denoted $X_{\mathrm{split}}(p)$, cf. [14, Ch. III, §6] and the discussions in §3 and §4e of [15]. This circumstance puts strong constraints on the set of prime numbers dividing the denominator of the j-invariant of E, i.e., the set of primes at which E does not have potential good reduction. Specifically, if $p \geq 17$, a result of Mazur [15, Cor. 4.8] proves that E has potential good reduction at all primes $\ell \neq 2, p$ satisfying $\ell \not\equiv \pm 1$ mod p. (This result holds also for $p = 11$, but this is irrelevant to our application, which requires $p \equiv 1 \bmod 4$.) Mazur's theorem has been strengthened by subsequent work. In particular, F. Momose [17, Prop. 3.1] proves that E has potential good reduction at all primes $\ell \neq 2$, as long as the prime p satisfies $p \geq 17$.

Alternatively, under the same hypothesis on p, Darmon notes in [2, Cor. 1.7] that E has potential good reduction at all primes $\ell \neq 2, 3$; this observation is obtained by combining a theorem of Kamienny [13] with [15, Cor. 4.3]. Darmon's result concerns elliptic curves over $\mathbf{Q}(\sqrt{-1})$ and requires only that E possess a rational subgroup of order $2p$ over this field.

Suppose now that we have $p \geq 17$ and $p \equiv 1 \bmod 4$. Then if (a,b,c) is a normalized solution to $a^p + 2b^p + c^p = 0$, the corresponding curve E has multiplicative reduction at all odd primes ℓ dividing abc. Momose's result implies that there is no such prime; Darmon's implies that 3 is the only possible such prime. On either count, we find that two of a, b and c are ± 1 while the third is $\pm 3^n$ for some $n \geq 0$. Indeed, a, b and c are relatively prime and all of them are odd in view of Theorem 3. Elementary reasoning allows us to reach a contradiction.

4. A conjecture of Frey

Conjecture 2. Let A be an elliptic curve over $\mathbf{Q}$. Then all sufficiently large prime numbers p have the following property: if B is an elliptic curve over $\mathbf{Q}$ for which $A[p]$ and $B[p]$ are isomorphic representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then A and B are isogenous over $\mathbf{Q}$.

Conjecture 2 appears as Conjecture 4.3 in [4], where it is attributed to G. Frey. It is similar in flavor to the conjectural statements in Frey's article [11]. The reader is invited to consult Mazur's article [16] as well as [4] and [11] for variants and generalizations. Here is one such generalization [4, Conj. 4.4 and Conj. 4.5]:

Conjecture 3. There is an integer $t > 0$ with the following property. Suppose that A and B are elliptic curves over $\mathbf{Q}$ and that the Galois representations $A[p]$ and $B[p]$ have isomorphic semisimplifications. If $p > t$, then A and B are isogenous.

We record the following simple observation:

Proposition 3. *Suppose that Conjecture 2 is true. Then Conjecture 1 holds for all sufficiently large prime numbers p.*

Proof. Suppose that (a, b, c) is a normalized solution to $a^p + 2b^p + c^p = 0$. If E is the associated Frey curve, then we have seen that $E[p]$ and $E_0[p]$ are isomorphic. Applying Conjecture 2 with $A = E_0$, we find that E and E_0 are isogenous for p sufficiently large. The isogeny relation between E and E_0 implies that these two elliptic curves have the same primes of bad reduction, so that E has good reduction outside 2. By the lemma of §2, this implies that $(a, b, c) = (-1, 1, -1)$. Hence $a^p + 2b^p + c^p = 0$ has only the trivial normalized solution for sufficiently large p. ■

References

1. B. J. Birch and W. Kuyk, eds., *Modular functions of one variable IV*, Lecture Notes in Math., vol. 476, Springer-Verlag, Berlin and New York, 1975.
2. H. Darmon, *The equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$*, International Mathematics Research Notices **10** (1993), 263–274.
3. ———, *The equation $x^4 - y^4 = z^p$*, C. R. Math. Rep. Acad. Sci. Canada **15** (1993), 286–290.
4. ———, *Serre's conjectures*, Seminar on Fermat's Last Theorem, CMS Conference Proceedings, American Mathematical Society, Providence (to appear).
5. H. Darmon and A. Granville, *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$* (preprint).
6. P. Dénes, *Über die Diophantische Gleichung $x^l + y^l = cz^l$*, Acta Math **88** (1952), 241–251.
7. F. Diamond, *On deformation rings and Hecke rings* (preprint).
8. F. Diamond and K. Kramer, *Modularity of a family of elliptic curves*, Mathematics Research Letters **2** (1995), 299–304.
9. L. E. Dickson, *History of the theory of numbers*, Chelsea, New York, 1971.
10. ———, *Introduction to the theory of numbers*, University of Chicago Press, Chicago, 1929.
11. G. Frey, *On elliptic curves with isomorphic torsion structures and corresponding curves of genus 2*, Elliptic curves, modular forms, & Fermat's Last Theorem, J. Coates, S. T. Yau, eds., International Press, Cambridge, MA, 1995, pp. 79–98.
12. K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Graduate Texts in Math., vol. 84, 2nd edition, Springer-Verlag, Berlin and New York, 1990.
13. S. Kamienny, *Rational points on Shimura curves over fields of even degree*, Math. Ann. **286** (1990), 731–734.
14. B. Mazur, *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47** (1977), 33–186.

15. ______, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
16. ______, *Questions about number*, New directions in mathematics (to appear).
17. F. Momose, *Rational points on the modular curves* $X_{\mathrm{split}}(p)$, Compositio Math. **52** (1984), 115–137.
18. K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.
19. J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), 179–230.
20. R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.
21. H. Wasserman, *Variations on the exponent-3 Fermat equation*, Manuscript, 1995.
22. A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.

Mathematics Department, Evans Hall, University of California, Berkeley, CA 94720-3840 USA

E-mail address: ribet@math.berkeley.edu