MULTI-FREY $\mathbb{Q}$-CURVES AND THE DIOPHANTINE EQUATION $a^2 + b^6 = c^n$

MICHAEL A. BENNETT AND IMIN CHEN

Abstract. We show that the equation $a^2 + b^6 = c^n$ has no nontrivial positive integer solutions with $(a, b) = 1$ via a combination of techniques based upon the modularity of Galois representations attached to certain $\mathbb{Q}$ -curves, corresponding surjectivity results of Ellenberg for these representations, and extensions of multi-Frey curve arguments of Siksek.

1. Introduction

Following the proof of Fermat's Last Theorem by Wiles [54], there has developed an extensive literature on connections between the arithmetic of modular abelian varieties and classical Diophantine problems, much of it devoted to solving *generalized Fermat equations* of the shape

$$a^p + b^q = c^r, \qquad \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1, \tag{1}$$

in coprime integers a, b and c, and positive integers p, q and r. That the number of such solutions (a, b, c) is finite, for a fixed triple (p, q, r), is a consequence of work of Darmon and Granville [26]. It has been conjectured that there are in fact at most finitely many such solutions, even when we allow the triples (p, q, r) to vary, provided we count solutions corresponding to $1^p + 2^3 = 3^2$ only once. Being extremely optimistic, one might even believe that the "known" solutions constitute a complete list, namely (a, b, c, p, q, r) corresponding to

$$1^p + 2^3 = 3^2,$$

for $p \geq 7$, and to nine other identities (see [6], [26]) :

$$2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2, \quad 3^5 + 11^4 = 122^2, \quad 17^7 + 76271^3 = 21063928^2,$$
$$1414^3 + 2213459^2 = 65^7, \quad 9262^3 + 15312283^2 = 113^7, \quad 43^8 + 96222^3 = 30042907^2,$$
$$\text{and} \quad 33^8 + 1549034^2 = 15613^3.$$

Date: 12 April 2011.

2000 *Mathematics Subject Classification.* Primary: 11D41, Secondary: 11D61, 11G05, 14G05.

Key words and phrases. Fermat equations, Galois representations, $\mathbb{Q}$-curves, multi-Frey techniques.

Research supported by NSERC.

Note, for brevity, we omit listing the solutions which differ only by sign changes and permutation of coordinates (for instance, if p is even, $(-1)^p + 2^3 = 3^2$, etc).

Since all known solutions have $\min\{p, q, r\} < 3$, a closely related formulation is that there are no nontrivial solutions in coprime integers once $\min\{p, q, r\} \geq 3$.

There are a variety of names associated to the above conjectures, including, alphabetically, Beal [39], Darmon and Granville [26], Granville, van der Poorten, Tijdeman and Zagier (see e.g. [6], [53]), and it appears that some of them are even willing to offer financial rewards for their resolution, positively or negatively.

Techniques based upon the modularity of Galois representations associated to putative solutions of equation (1) have, in many cases, provided a fruitful approach to these problems, though the limitations of such methods are still unclear. Each situation where finiteness results have been established for infinite families of triples (p, q, r) has followed along these lines. We summarize results to date; in each case, no solutions outside those mentioned above have been discovered :

(p, q, r)	reference(s)
$(n, n, n),\ n \geq 3$	Wiles [54], Taylor-Wiles [52]
$(n, n, 2),\ n \geq 4$	Darmon-Merel [27], Poonen [42]
$(n, n, 3),\ n \geq 3$	Darmon-Merel [27], Poonen [42]
$(2n, 2n, 5),\ n \geq 2$	Bennett [1]
$(2, 4, n),\ n \geq 4$	Ellenberg [29], Bennett-Ellenberg-Ng [3], Bruin [9]
$(2, n, 4),\ n \geq 4$	immediate from Bennett-Skinner [4], Bruin [11]
$(2, 2n, k),\ n \geq 2,\ k \in \{9, 10, 15\}$	Bennett-Chen-Dahmen-Yazdani [2]
$(4, 2n, 3),\ n \geq 2$	Bennett-Chen-Dahmen-Yazdani [2]
$(2, n, 6),\ n \geq 3$	Bennett-Chen-Dahmen-Yazdani [2]
$(3, 3, n),\ n \geq 3^*$	Chen-Siksek [20], Kraus [37], Bruin [10], Dahmen [22]
$(3j, 3k, n),\ j, k, n \geq 2$	Kraus [37]
$(3, 3, 2n),\ n \geq 2$	Bennett-Chen-Dahmen-Yazdani [2]
$(3, 6, n),\ n \geq 2$	Bennett-Chen-Dahmen-Yazdani [2]
$(2, 2n, 3),\ n \geq 3^*$	Bruin [9], Chen [17], Dahmen [22], [23], Siksek [50]
$(2, 2n, 5),\ n \geq 3^*$	Chen [18]
$(2, 3, n),\ 6 \leq n \leq 10$	Poonen-Schaeffer-Stoll [43], Bruin [9], [11], [12], Brown [8], Siksek [49]

The $(*)$ here indicates that the result has been proven for a family of exponents of natural density one (but that there remain infinitely many cases of positive Dirichlet density untreated).

In this paper, we will prove the following theorem.

Theorem 1. *Let $n \geq 3$ be an integer. Then the equation*

$$a^2 + b^6 = c^n \tag{2}$$

has no solutions in positive integers a, b and c, with a and b coprime.

Our motivations for considering this problem are two-fold. Firstly, the exponents $(2, 6, n)$ provides one of the final examples of an exponent family for which there is known to exist a corresponding family of Frey-Hellegouarch elliptic $\mathbb{Q}$-curves. A remarkable program for attacking generalized Fermat equation of signature (n, n, m) (and perhaps others) is outlined in Darmon [24], relying upon the construction of Frey-Hellegouarch abelian varieties. Currently, however, it does not appear that the corresponding technology is suitably advanced to allow the application of such arguments to completely solve families of such equations for fixed $m \geq 5$.

In some sense, the signatures $(2, 6, n)$ and $(2, n, 6)$ (the latter equations are treated in [2]) represent the final remaining families of generalized Fermat equations approachable by current techniques. More specifically, following [26], associated to a generalized Fermat equation $x^p + y^q = z^r$ is a triangle Fuchsian group with signature $(1/p, 1/q, 1/r)$. A reasonable precondition to apply the modular method using rational elliptic curves or $\mathbb{Q}$-curves is that this triangle group be commensurable with the full modular group. Such a classification has been performed by Takeuchi [51]. He shows that the possible signatures which contain ∞ are given by $(2, 3, \infty)$, $(2, 4, \infty)$, $(2, 6, \infty)$, $(2, \infty, \infty)$, $(3, 3, \infty)$, $(3, \infty, \infty)$, $(4, 4, \infty)$, $(6, 6, \infty)$, (∞, ∞, ∞). A related classification of Frey representations for prime exponents can be found in [24] and [26]. The above list does not, admittedly, explain all the possible families of generalized Fermat equations that have been amenable to the modular method. In all other known cases, however, the Frey curve utilized is derived from a descent step to one of the above "pure" Frey curve families. Concerning the applicability of using certain families of $\mathbb{Q}$-curves, see the conclusions section of [18] for further remarks.

Our secondary motivation is as an illustration of the utility of the multi-Frey techniques of Siksek (cf. [13] and [14]). A fundamental difference between the case of signature $(2, 4, n)$ considered in [29] and that of $(2, 6, n)$ is the existence, in this latter situation, of a potential obstruction to our arguments in the guise of a particular modular form *without* complex multiplication. To eliminate the possibility of a solution to the equation $x^2 + y^6 = z^n$ arising from this form requires fundamentally new techniques, based upon a generalization of the multi-Frey technique to $\mathbb{Q}$-curves (rather than just curves over $\mathbb{Q}$).

The computations in this paper were performed in MAGMA [7]. The programs, data, and output files are posted at http://people.math.sfu.ca/∼ichen/firstb3i-data. Throughout the text, we have included specific references to the MAGMA code employed, indicated as follows : $\boxed{\text{sample.txt}}$.

2. Review of $\mathbb{Q}$-curves and their attached Galois representations

The exposition of $\mathbb{Q}$-curves and their attached Galois representations we provide in this section closely follows that of references [19], [30], [44] and [46]; we include it in the interest of keeping our exposition reasonably self-contained.

Let K be a number field and C/K be a non-CM elliptic curve such that there is an isogeny $\mu(\sigma) : {}^{\sigma}C \to C$ defined over K for each $\sigma \in G_{\mathbb{Q}}$. Such a curve C/K is called a $\mathbb{Q}$-curve defined over K. Let $\hat{\phi}_{C,p} : G_K \to \mathrm{GL}_2(\mathbb{Z}_p)$ be the representation of G_K on the Tate module $\hat{V}_p(C)$. One can attach a representation

$$\hat{\rho}_{C,\beta,p} : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}_p^* \, \mathrm{GL}_2(\mathbb{Q}_p)$$

to C such that $\mathbb{P}\hat{\rho}_{C,\beta,p} \mid_{G_K} \cong \mathbb{P}\hat{\phi}_{C,p}$. The representation depends on a choice of splitting map β (in what follows, we will provide more details of this choice). Let π be a prime above p of the field M_β generated by the values of β. In practice, the representation $\hat{\rho}_{C,\beta,\pi}$ is constructed in a way so that its image lies in $M_{\beta,\pi}^* \, \mathrm{GL}_2(\mathbb{Q}_p)$, and we choose to use the notation $\hat{\rho}_{C,\beta,p} = \hat{\rho}_{C,\beta,\pi}$ to indicate the choice of π in this explicit construction.

Let

$$c_C(\sigma,\tau) = \mu_C(\sigma) \, {}^{\sigma}\mu_C(\tau) \mu_C(\sigma\tau)^{-1} \in (\mathrm{Hom}_K(C,C) \otimes_{\mathbb{Z}} \mathbb{Q})^* = \mathbb{Q}^*,$$

where $\mu_C^{-1} := (1/\deg \mu_C)\mu_C'$ and μ_C' is the dual of μ_C. Then $c_C(\sigma,\tau)$ determines a class in $H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$ which depends only on the $\overline{\mathbb{Q}}$-isogeny class of C. The class $c_C(\sigma,\tau)$ factors through $H^2(G_{K/\mathbb{Q}}, \mathbb{Q}^*)$, depending now only on the K-isogeny class of C. Alternatively,

$$c_C(\sigma,\tau) = \alpha(\sigma) \, {}^{\sigma}\alpha(\tau) \alpha(\sigma\tau)^{-1}$$

arises from a class $\alpha \in H^1(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*/\mathbb{Q}^*)$ through the map

$$H^1(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*/\mathbb{Q}^*) \to H^2(G_{\mathbb{Q}}, \mathbb{Q}^*),$$

resulting from the short exact sequence

$$1 \to \mathbb{Q}^* \to \overline{\mathbb{Q}}^* \to \overline{\mathbb{Q}}^*/\mathbb{Q}^* \to 1.$$

Explicitly, $\alpha(\sigma)$ is defined by $\sigma^*(\omega_C) = \alpha(\sigma)\omega_C$.

Tate showed that $H^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*)$ is trivial where the action of $G_{\mathbb{Q}}$ on $\overline{\mathbb{Q}}^*$ is trivial. Thus, there is a continuous map $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ such that

$$c_C(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$$

as cocycles, and we call β a splitting map for c_C. We define

$$\hat{\rho}_{C,\beta,\pi}(\sigma)(1 \otimes x) = \beta(\sigma)^{-1} \otimes \mu_C(\sigma)(\sigma(x)).$$

Given a splitting $c_C(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$, Ribet attaches an abelian variety A_β defined over $\mathbb{Q}$ of GL_2-type having C as a simple factor over $\overline{\mathbb{Q}}$.

In practice, what we do in this paper is to find a continuous $\beta : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$, factoring over an extension of low degree, such that $c_C(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$ as elements in $H^2(G_{\mathbb{Q}}, \overline{\mathbb{Q}}^*)$, using results in [44]. Then we choose a suitable twist C_β/K_β of C, where K_β is the splitting field of β, such that $c_{C_\beta}(\sigma, \tau)$ is exactly the cocycle $c_\beta(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$. In this situation, the abelian variety A_β is constructed as a quotient over $\mathbb{Q}$ of $\mathrm{Res}_{\mathbb{Q}}^{K_\beta} C_\beta$.

The endomorphism algebra of A_β is given by $M_\beta = \mathbb{Q}(\{\beta(\sigma)\})$ and the representation on the π^n-torsion points of A_β coincides with the representation $\hat{\rho}_{C,\beta,\pi}$ defined earlier.

Let $\epsilon : G_{\mathbb{Q}} \to \overline{\mathbb{Q}}^*$ be defined by

$$\epsilon(\sigma) = \beta(\sigma)^2 / \deg \mu(\sigma). \tag{3}$$

Then ϵ is a character and

$$\det \hat{\rho}_{C,\beta,\pi} = \epsilon^{-1} \cdot \chi_p, \tag{4}$$

where $\chi_p : G_{\mathbb{Q}} \to \mathbb{Z}_p^*$ is the p-th cyclotomic character.

3. $\mathbb{Q}$-curves attached to $a^2 + b^6 = c^p$ and their Galois representations

Let $(a, b, c) \in \mathbb{Z}^3$ be a solution to $a^2 + b^6 = c^p$ where we suppose that p is a prime. We call (a, b, c) *proper* if $\gcd(a, b, c) = 1$ and *trivial* if $|c| = 1$. Note that a solution $(a, b, c) \in \mathbb{Z}^3$ is proper if and only if the integers a, b and c are pairwise coprime. In what follows, we will always assume that the triple (a, b, c) is a proper, nontrivial solution. We consider the following associated (Frey or Frey-Hellegouarch) elliptic curve

$$E \ : \ Y^2 = X^3 - 3(5b^3 + 4ai)bX + 2(11b^6 + 14ib^3a - 2a^2),$$

with j-invariant

$$j = 432\, i\, \frac{b^3(4a-5ib^3)^3}{(a-ib^3)(a+ib^3)^3} \tag{5}$$

and discriminant $\Delta = -2^8 \cdot 3^3 \cdot (a-ib^3) \cdot (a+ib^3)^3$.

Lemma 2. *Suppose $a/b^3 \in \mathbb{P}^1(\mathbb{Q})$. Then the j-invariant of E does not lie in $\mathbb{Q}$ except when*

- *$a/b^3 = 0$ and $j = 54000$, or*
- *$a/b^3 = \infty$ and $j = 0$.*

Proof. This can be seen by solving the polynomial equation in $\mathbb{Q}[i][j, a/b^3]$ derived from (5) by clearing denominators and collecting terms with respect to $\{1, i\}$, using the restriction that $j, a/b^3 \in \mathbb{P}^1(\mathbb{Q})$. □

Corollary 3. *E does not have complex multiplication unless*

- *$a/b^3 = 0$, $j = 54000$, $d(\mathcal{O}) = -12$, or*
- *$a/b^3 = \infty$, $j = 0$, $d(\mathcal{O}) = -3$.*

Proof. If E has complex multiplication by an order $\mathcal{O}$ in an imaginary quadratic field, then $j(E)$ has a real conjugate over $\mathbb{Q}$ (for instance, arising from $j(E_0)$, where E_0 is the elliptic curve associated to the lattice $\mathcal{O}$ itself). Hence, $j(E) \in \mathbb{Q}$ in fact. For a list of the j-invariants of elliptic curves with complex multiplication by a class number 1 order, see for instance [21, p. 261]. □

Lemma 4. *If $(a, b, c) \in \mathbb{Z}^3$ with $\gcd(a, b, c) = 1$ and $a^2 + b^6 = c^p$, then either $c = 1$ or c is divisible by a prime not equal to 2 or 3.*

Proof. The condition $\gcd(a, b, c) = 1$ together with inspection of $a^2 + b^6$ modulo 3 shows that c is never divisible by 3. Similar reasoning allows us to conclude, since $p > 1$, that c is necessarily odd, whereby the lemma follows. □

From here on, let us suppose that E arises from a non-trivial proper solution to $a^2 + b^6 = c^p$ where p is an odd prime. Note that ab is even and, from the preceding discussion, that $a - b^3 i$ and $a + b^3 i$ are coprime p-th powers in $\mathbb{Z}[i]$.

The elliptic curve E is defined over $\mathbb{Q}(i)$. Its conjugate over $\mathbb{Q}(i)$ is 3-isogenous to E over $\mathbb{Q}(\sqrt{3}, i)$; see isogeny.txt. This is in contrast to the situation in [29], where the corresponding isogeny is defined over $\mathbb{Q}(i)$. We make a choice of isogenies $\mu(\sigma) : {}^{\sigma}E \to E$ such that $\mu(\sigma) = 1$ for $\sigma \in G_{\mathbb{Q}(i)}$ and $\mu(\sigma)$ is the 3-isogeny above when $\sigma \notin G_{\mathbb{Q}(i)}$.

Let $d(\sigma)$ denote the degree of $\mu(\sigma)$. We have that $d(G_{\mathbb{Q}}) = \{1, 3\} \subseteq \mathbb{Q}^*/\mathbb{Q}^{*2}$. The fixed field K_d of the kernel of $d(\sigma)$ is $\mathbb{Q}(i)$ and so $(a, d) = (-1, 3)$ is a dual basis in the terminology of Quer [44].

The quaternion algebra $(-1, 3)$ is ramified at $2, 3$ and so a choice of splitting character for $c_E(\sigma, \tau)$ is given by $\epsilon = \epsilon_2\epsilon_3$ where ϵ_2 is the non-trivial character of $\mathbb{Z}/4\mathbb{Z}^\times$ and ϵ_3 is the non-trivial character of $\mathbb{Z}/3\mathbb{Z}^\times$. The fixed field of ϵ is $K_\epsilon = \mathbb{Q}(\sqrt{3})$.

Let $G_{\mathbb{Q}(i)/\mathbb{Q}} = \{\sigma_1, \sigma_{-1}\}$. We have that

$$\alpha(\sigma_1) = 1 \quad \text{and} \quad \alpha(\sigma_{-1}) = i\sqrt{3}.$$

This can be checked by noting that the quotient of E by the 3-torsion point of E using Vélu multiplies the invariant differential by 1. The resulting quotient elliptic curve is then a twist over $\mathbb{Q}(\sqrt{3}, i)$ of the original E. This twisting multiplies the invariant differential by $i\sqrt{3}$.

So now we can express $c_E(\sigma, \tau) = \alpha(\sigma){}^{\sigma}\alpha(\tau)\alpha(\sigma\tau)^{-1}$. Let $\beta(\sigma) = \sqrt{\epsilon(\sigma)}\sqrt{d(\sigma)}$ and $c_\beta(\sigma, \tau) = \beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1} \in H^2(G_\mathbb{Q}, \mathbb{Q}^*)$. We know from Quer [44] that $c_\beta(\sigma, \tau)$ and $c_E(\sigma, \tau)$ represent the same class in $H^2(G_\mathbb{Q}, \mathbb{Q}^*)$. The fixed field of β is $K_\beta = K_\epsilon \cdot K_d = \mathbb{Q}(\sqrt{3}, i)$ and $M_\beta = \mathbb{Q}(\sqrt{3}, i)$.

Our goal is to find a $\gamma \in \overline{\mathbb{Q}}^*$ so that $c_\beta(\sigma, \tau) = \alpha_1(\sigma){}^{\sigma}\alpha_1(\tau)\alpha_1(\sigma\tau)^{-1}$, where $\alpha_1(\sigma) = \alpha(\sigma)\frac{{}^{\sigma}\sqrt{\gamma}}{\sqrt{\gamma}}$. Using a similar technique as for the equation $a^2 + b^{2p} = c^5$ (cf. [18], where the corresponding K_β is cyclic quartic), we can narrow down the possibilities for choices of γ and subsequently verify that a particular choice actually works.

In more detail, recall that $K_\beta = \mathbb{Q}(\sqrt{3}, i) = \mathbb{Q}(z)$, where $z = e^{2\pi i/12} = \frac{i+\sqrt{3}}{2}$ is a primitive 12-th root of unity. Let $G_{\mathbb{Q}(\sqrt{3},i)/\mathbb{Q}} = \{\sigma_1, \sigma_{-1}, \sigma_3, \sigma_{-3}\}$ and assume that $\alpha_1(\sigma_{-3})^2/\alpha(\sigma_{-3})^2 = \alpha_1(\sigma_{-3})^2/-3$ is a unit, say 1. This implies that $\frac{{}^{\sigma_{-3}}\gamma}{\gamma} = 1$ whereby $\gamma \in \mathbb{Q}(\sqrt{-3})$. Furthermore, let us assume that $\frac{{}^{\sigma_{-1}}\gamma}{\gamma}$ is a square in K_β of a unit in $\mathbb{Q}(\sqrt{-3})$, say z^2 (the other choices produce isomorphic twists). Solving for γ, we obtain that $\gamma = \frac{-3+i\sqrt{3}}{2}$ is one possible choice.

The resulting values of $\alpha_2(\sigma) = \alpha(\sigma)\sqrt{\frac{{}^{\sigma}\gamma}{\gamma}}$ are

$$\alpha_2(\sigma_1) = 1, \;\; \alpha_2(\sigma_{-1}) = i\sqrt{3}z, \;\; \alpha_2(\sigma_3) = z \quad \text{and} \quad \alpha_2(\sigma_{-3}) = i\sqrt{3},$$

where we have fixed a choice of square root for each $\sigma \in G_{K/\mathbb{Q}}$. It can be verified that $c_\beta(\sigma, \tau) = \alpha_2(\sigma){}^{\sigma}\alpha_2(\tau)\alpha_2(\sigma\tau)^{-1}$.

Consider the twist E_β of E given by the equation

$$E_\beta \;\; : \;\; Y^2 = X^3 - 3(5b^3 + 4ai)b\gamma^2 X + 2(11b^6 + 14ib^3a - 2a^2)\gamma^3. \tag{6}$$

From the relationship between E_β and E, the initial $\mu(\sigma)$'s for E give rise to choices for $\mu_\beta(\sigma)$ for E_β which are, in general, locally constant on a smaller subgroup than G_K. For these choices of $\mu_\beta(\sigma)$ we have that $\alpha_{E_\beta}(\sigma) = \alpha_1(\sigma) = \alpha(\sigma)\frac{{}^{\sigma}\sqrt{\gamma}}{\sqrt{\gamma}}$. Now, $\sqrt{\frac{{}^{\sigma}\gamma}{\gamma}} = \xi(\sigma)\delta(\sigma)$ where $\delta(\sigma) = \frac{{}^{\sigma}\sqrt{\gamma}}{\sqrt{\gamma}}$ and $\xi(\sigma) = \pm 1$. Since $\delta(\sigma){}^{\sigma}\delta(\tau)\delta(\sigma\tau)^{-1} = 1$, it follows that $c_{E_\beta}(\sigma, \tau) = c_\beta(\sigma, \tau)\xi(\sigma)\xi(\tau)\xi(\sigma\tau)^{-1}$. Hence, by using the alternate set of isogenies $\mu'_\beta(\sigma) = \mu_\beta(\sigma)\xi(\sigma)$, which are now locally constant on G_K, the corresponding $\alpha_{E_\beta}(\sigma) = \alpha(\sigma)\sqrt{\frac{{}^\sigma\gamma}{\gamma}} = \alpha_2(\sigma)$, and hence $c_{E_\beta}(\sigma,\tau) = \alpha_2(\sigma)\,{}^\sigma\alpha_2(\tau)\alpha_2(\sigma\tau)^{-1} = c_\beta(\sigma,\tau)$ as cocycles, not just as classes in $H^2(G_{K/\mathbb{Q}}, \mathbb{Q}^*)$. The elliptic curve E_β/K_β is a $\mathbb{Q}$-curve defined over K_β; cf. isogenyp.txt.

Another way to motivate the preceding calculation is as follows. Without loss of generality, we may assume that γ is square-free in the ring of integers of K_β (if γ is a square, then the corresponding E_β is isomorphic over K_β to E). The field K_β has class number one. If $\gamma = \lambda\gamma'$ where $\lambda \in \mathbb{Z}$, then using γ' instead of γ yields an E_β whose $c_{E_\beta}(\sigma,\tau)$ is the same cocycle in $H^2(G_{K/\mathbb{Q}}, \mathbb{Q}^*)$. The condition that $\sqrt{\frac{{}^\sigma\gamma}{\gamma}}$ be a square in K_β for all $\sigma \in G_{K/\mathbb{Q}}$ shows that only ramified primes divide γ and there are two such primes in $K_\beta = \mathbb{Q}(\sqrt{3}, i)$.

The discriminant of K_β is $d_{K_\beta/\mathbb{Q}} = 2^4 \cdot 3^2 = 144$. The prime factorizations of $(2), (3)$ in K_β are given by

$$(2) = \mathfrak{q}_2^2 \quad \text{and} \quad (3) = \mathfrak{q}_3^2.$$

Let ν_2, ν_3 be uniformizers at $\mathfrak{q}_2, \mathfrak{q}_3$ respectively with associated valuations v_2, v_3. The units in K_β are generated by z of order 12 and a unit u_2 of infinite order. Thus, up to squares, γ is product of a subset of the elements $\{z, u_2, \nu_2, \nu_3\}$.

The authors have subsequently learned that a similar technique for finding γ also appeared in [28] (where K_β is polyquadratic).

It would be interesting to study the twists E_β which arise from other choices of splitting maps. We will not undertake this here.

Lemma 5. *Suppose that E and E' are elliptic curves defined by*

$$\begin{aligned} E &: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \\ E' &: Y^2 + a'_1XY + a'_3Y = X^3 + a'_2X^2 + a'_4X + a'_6, \end{aligned}$$

where the a_i, a'_i lie in a discrete valuation ring $\mathcal{O}$ with uniformizer ν.

(1) *Suppose the valuation at ν of the discriminants is, in each case, equal to* 12. *If E has reduction type II^* and $a'_i \equiv a_i \pmod{\nu^6}$, then E' also has reduction type II^*. If E has reduction type I_0 and $a'_i \equiv a_i \pmod{\nu^6}$, then E' also has reduction type I_0.*

(2) *Suppose the valuation at ν of the discriminants is, in each case, equal to* 16. *If E has reduction type II and $a'_i \equiv a_i \pmod{\nu^8}$, then E' also has reduction type II.*

(3) *Suppose the Weierstrass equation of E is in minimal form, and E has reduction type II or III. If $a_i' \equiv a_i \pmod{\nu^8}$, then E' has the same reduction type as E and is also in minimal form.*

Proof. We give a proof for case (1), the remaining cases are similar. Since the discriminants of E and E' have valuation 12, when E and E' are processed through Tate's algorithm [48], the algorithm terminates at one of Steps 1–10 or reaches Step 11 to loop back a second time at most once.

If E has reduction type II^*, the algorithm applied to E terminates at Step 10. Since the transformations used in Steps 1–10 are translations, they preserve the congruence $a_i \equiv a_i' \pmod{\nu^6}$ as E and E' are processed through the algorithm, and since the conditions to exit at Steps 1–10 are congruence conditions modulo ν^6 on the coefficients of the Weierstrass equations, we see that if the algorithm applied to E terminates at Step 10, it must also terminate at Step 10 for E'.

If E has reduction type I_0, the algorithm applied to E reaches Step 11 to loop back a second time to terminate at Step 1 (because the valuation of the discriminant of the model for E is equal to 12). Again, since $a_i' \equiv a_i \pmod{\nu^6}$, it follows that the algorithm applied to E' also reaches Step 11 to loop back a second time and terminate at Step 1 (again because the valuation of the discriminant of the model for E' is equal to 12).

□

Theorem 6. *The conductor of E_β is*

$$\mathfrak{m} = \mathfrak{q}_2^4 \cdot \mathfrak{q}_3^{\varepsilon} \prod_{\mathfrak{q} | c, \mathfrak{q} \nmid 2,3} \mathfrak{q},$$

where $\varepsilon = 0, 4$.

Proof. cf. $\boxed{\text{tate2m.txt, tate3m.txt}}$ for the computations. Recall that E_β is given by

$$E_\beta \quad : \quad Y^2 = X^3 - 3(5b^3 + 4ai)b\gamma^2 X + 2(11b^6 + 14ib^3a - 2a^2)\gamma^3. \tag{7}$$

with

$$\Delta_{E_\beta} = -2^8 \cdot 3^3 \cdot (a - ib^3)(a + ib^3)^3 \cdot \gamma^6. \tag{8}$$

Then

$$\begin{aligned} c_4 &= 2^4 \cdot 3^2 \cdot b(4ia + 5b^3) \cdot \gamma^2 \\ c_6 &= 2^5 \cdot 3^3 \cdot (2a + (-7i - 6z^2 + 3)b^3)(2a + (-7i + 6z^2 - 3)b^3) \cdot \gamma^3. \end{aligned} \tag{9}$$

Let $\mathfrak{q}$ be a prime not dividing $2 \cdot 3$ but dividing Δ_{E_β}. The elliptic curve E_β has multiplicative bad reduction at $\mathfrak{q}$ if one of $c_4, c_6 \not\equiv 0 \pmod{\mathfrak{q}}$. Since γ is not divisible by $\mathfrak{q}$ and $\gcd(a,b) = 1$, we note that $c_4 \equiv c_6 \equiv 0 \pmod{\mathfrak{q}}$ happens if and only if

$$b^3 \equiv 0 \pmod{\mathfrak{q}}, \text{ or } 4ia + 5b^3 \equiv 0 \pmod{\mathfrak{q}},$$

and

$$2a + (-7i - 6z^2 + 3)b^3 \equiv 0 \pmod{\mathfrak{q}}, \text{ or } 2a + (-7i + 6z^2 - 3)b^3 \equiv 0 \pmod{\mathfrak{q}}.$$

The determinants of the resulting linear system in the variables a, b^3, in all 4 cases, are only divisible by primes above 2 and 3. It follows that E_β has multiplicative bad reduction at $\mathfrak{q}$.

By equation (8), since $\gcd(a,b) = 1$, we have $v_3(\Delta_{E_\beta}) = 12$. We run through all possibilities for (a,b) modulo ν_3^6 and, in each case, we compute the reduction type of E_β at $\mathfrak{q}_3$ using MAGMA [7]; in every case, said reduction type turns out to be of type II^* or I_0. By Lemma 5, case (1), this determines all the possible conductor exponents for E_β at $\mathfrak{q}_3$.

Since a and b are of opposite parity, equation(8) implies that $v_2(\Delta_{E_\beta}) = 16$. Checking all possibilities for (a,b) modulo ν_2^8, and in each case computing the reduction type of E_β at $\mathfrak{q}_2$, via MAGMA [7], we always arrive at reduction type II. By Lemma 5, case (2), this determines all the possible conductor exponents for E_β at $\mathfrak{q}_2$. □

Theorem 7. *The conductor of* $\operatorname{Res}_{\mathbb{Q}}^{K_\beta} E_\beta$ *is*

$$d_{K_\beta/\mathbb{Q}}{}^2 \cdot N_{K_\beta/\mathbb{Q}}(\mathfrak{m}) = 2^{16} \cdot 3^{4+2\varepsilon} \cdot \prod_{q|c, q\neq 2,3} q^4,$$

where $\varepsilon = 0, 4$.

Proof. cf. [41, Lemma, p. 178]. We also note that K_β is unramified outside $\{2,3\}$ so the product is of the form stated. □

Corollary 8. *The elliptic curve* E_β *has potentially good reduction at* $\mathfrak{q}_2$ *and* $\mathfrak{q}_3$. *In the latter case, the reduction is potentially supersingular.*

Let $A = \operatorname{Res}_{\mathbb{Q}}^{K_\beta} E_\beta$. By [44, Theorem 5.4], A is an abelian variety of GL_2-type with $M_\beta = \mathbb{Q}(\sqrt{3}, i)$. The conductor of the system of $M_{\beta,\pi}[G_{\mathbb{Q}}]$-modules $\left\{\hat{V}_\pi(A)\right\}$ is given by

$$2^4 \cdot 3^{1+\varepsilon/2} \cdot \prod_{q|c, q\neq 2,3} q, \tag{10}$$

using the conductor results explained in cf. [18].

For the next two theorems, it is useful to recall that $a - b^3 i$ and $a + b^3 i$ are coprime p-th powers in $\mathbb{Z}[i]$.

Theorem 9. *The representation $\phi_{E,p} \mid_{I_p}$ is finite flat for $p \neq 2, 3$.*

Proof. This follows from the fact that E has good or multiplicative bad reduction at primes above p when $p \neq 2, 3$, and in the case of multiplicative bad reduction, the exponent of a prime above p in the minimal discriminant of E is divisible by p. Also, p is unramified in K_β so that $I_p \subseteq G_{K_\beta}$. □

Theorem 10. *The representation $\phi_{E,p} \mid_{I_\ell}$ is trivial for $\ell \neq 2, 3, p$.*

Proof. This follows from the fact that E has good or multiplicative bad reduction at primes above ℓ when $\ell \neq 2, 3$, and, in the case of multiplicative bad reduction, the exponent of a prime above ℓ in the minimal discriminant of E is divisible by p. Also, ℓ is unramified in K_β so that $I_\ell \subseteq G_{K_\beta}$. □

Theorem 11. *Suppose $p \neq 2, 3$. The conductor of $\rho = \rho_{E,\beta,\pi}$ is one of 48 or 432.*

Proof. Since we are determining the Artin conductor of ρ, we consider only ramification at primes above $\ell \neq p$.

Suppose $\ell \neq 2, 3, p$. Since $\ell \neq 2, 3$, we see that K_β is unramified at ℓ and hence G_{K_β} contains I_ℓ. Now, in our case, $\rho \mid_{G_{K_\beta}}$ is isomorphic to $\phi_{E,p}$. Since $\phi_{E,p} \mid_{I_\ell}$ is trivial, we have that $\rho \mid_{I_\ell}$ is trivial so ρ is unramified outside $\{2, 3, p\}$.

Suppose $\ell = 2, 3$. The representation $\hat{\phi}_{E,p} \mid_{I_\ell}$ factors through a finite group of order only divisible by the primes 2, 3. Now, in our case, $\hat{\rho} \mid_{G_{K_\beta}}$ is isomorphic to $\hat{\phi}_{E,p}$. Hence, the representation $\hat{\rho} \mid_{I_\ell}$ also factors through a finite group of order only divisible by the primes 2, 3. It follows that the exponent of ℓ in the conductor of ρ is the same as in the conductor of $\hat{\rho}$ as $p \neq 2, 3$. □

Proposition 12. *Suppose $p \neq 2, 3$. Then the weight of $\rho = \rho_{E,\beta,\pi}$ is 2.*

Proof. The weight of ρ is determined by $\rho \mid_{I_p}$. Since $p \neq 2, 3$, we see that K_β is unramified at p and hence G_{K_β} contains I_p. Now, in our case, $\rho \mid_{G_{K_\beta}}$ is isomorphic to $\phi_{E,p}$. Since $\phi_{E,p} \mid_{I_p}$ is finite flat and its determinant is the p-th cyclotomic character, we have that the weight of ρ is necessarily 2 [47, Proposition 4]. □

Proposition 13. *The character of $\rho_{E,\beta,\pi}$ is ϵ.*

Proof. This follows from equation (4). □

Let $X_{0,B}^K(d,p)$, $X_{0,N}^K(d,p)$, $X_{0,N'}^K(d,p)$ be the modular curves with level p structure corresponding to a Borel subgroup B, the normalizer of a split Cartan subgroup N, the normalizer of a non-split Cartan subgroup N' of $\mathrm{GL}_2(\mathbb{F}_p)$, and level d structure consisting of a cyclic subgroup of order d, twisted by the quadratic character associated to K through the action of the Fricke involution w_d.

Lemma 14. *Let E be a $\mathbb{Q}$-curve defined over K', K be a quadratic number field contained in K', and d a prime number such that*

(1) *the elliptic curve E is defined over K,*

(2) *the choices of $\mu_E(\sigma)$ are constant on G_K cosets, $\mu_E(\sigma)=1$ when $\sigma \in G_K$, and $\deg \mu_E(\sigma) = d$ when $\sigma \notin G_K$,*

(3) *$\mu_E(\sigma)\,{}^{\sigma}\mu_E(\sigma) = \pm d$ whenever $\sigma \notin G_K$.*

If $\rho_{E,\beta,\pi}$ has image lying in a Borel subgroup, normalizer of a split Cartan subgroup, or normalizer of a non-split Cartan subgroup of $\overline{\mathbb{F}}_p^\times \mathrm{GL}_2(\mathbb{F}_p)$, then E gives rise to a $\mathbb{Q}$-rational point on the corresponding modular curve above.

Proof. This proof is based on [29, Proposition 2.2]. Recall the action of $G_\mathbb{Q}$ on $\mathbb{P}E[d]$ is given by $x \mapsto \mu_E(\sigma)({}^{\sigma}x)$. Suppose $\mathbb{P}\rho_{E,\beta,p}$ has image lying in a Borel subgroup. Then we have that $\mu_E(\sigma)({}^{\sigma}C_p) = C_p$ for some cyclic subgroup C_p of order p in $E[p]$ and all $\sigma \in G_\mathbb{Q}$. Let C_d be the cyclic subgroup of order d in $E[d]$ defined by $\mu_E(\sigma)({}^{\sigma}E[d])$ where σ is an element of $G_\mathbb{Q}$ which is non-trivial on K. This does not depend on the choice of σ. Suppose σ is an element of $G_\mathbb{Q}$ which is non-trivial on K. The kernel of $\mu_E(\sigma)$ is precisely ${}^{\sigma}C_d$ as $\mu_E(\sigma)({}^{\sigma}C_d) = \mu_E(\sigma)\,{}^{\sigma}\mu_E(\sigma)\left({}^{\sigma^2}E[d]\right) = [\pm d]\left({}^{\sigma^2}E[d]\right) = 0$. Hence, we see that

$$\begin{aligned} {w_d}^{\sigma}(E, C_d, C_p) &= w_d({}^{\sigma}E, {}^{\sigma}C_d, {}^{\sigma}C_p) \\ &= (\mu_E(\sigma)({}^{\sigma}E), \mu_E(\sigma)({}^{\sigma}E[d]), \mu_E(\sigma)({}^{\sigma}C_p)) \\ &= (E, C_d, C_p) \end{aligned}$$

so ${}^{\sigma}(E, C_d, C_p) = w_d(E, C_d, C_p)$, where w_d is the Fricke involution. Suppose σ is an element of $G_\mathbb{Q}$ which is trivial on K. In this case, we have that ${}^{\sigma}(E, C_d, C_p) = (E, C_d, C_p)$. Thus, (E, C_d, C_p) gives rise to a $\mathbb{Q}$-rational point on $X_{0,B}(d,p)$.

The case when the image of $\rho_{E,\beta,\pi}$ lies in the normalizer of a Cartan subgroup is similar except now we have the existence of a set of distinct points $S_p = \{\alpha_p, \beta_p\}$ of $\mathbb{P}E[p] \otimes \mathbb{F}_{p^2}$ such that the action of $\sigma \in G_\mathbb{Q}$ by $x \mapsto \mu_E(\sigma)({}^{\sigma}x)$ fixes S_p as a set. □

Theorem 15. *Suppose the representation $\rho_{E,\beta,\pi}$ is reducible for $p \neq 2, 3, 5, 7, 13$. Then E has potentially good reduction at all primes above $\ell > 3$.*

Proof. cf. [29, Proposition 3.2]. We note that E gives rise to a $\mathbb{Q}$-rational point on $X_{0,N}^{K}(3, p)$ by Lemma 14, even though the isogeny between E and its conjugate is only defined over $\mathbb{Q}(\sqrt{3}, i)$. □

Corollary 16. *The representation $\rho_{E,\beta,\pi}$ is irreducible for $p \neq 2, 3, 5, 7, 13$.*

Proof. Lemma 4 shows that E must have multiplicative bad reduction at some prime of K above $\ell > 3$. □

Proposition 17. *If $p = 13$, then $\rho_{E,\beta,\pi}$ is irreducible.*

Proof. By Lemma 14, if $\rho_{E,\beta,\pi}$ were reducible, then E would give rise to a non-cuspidal K-rational point on $X_0(39)$ where $K = \mathbb{Q}(i)$ and a non-cuspidal $\mathbb{Q}$-rational point on $X_0(39)/w_3$. We can now use the work of [32] which says that $X_0(39)/w_3$ has four $\mathbb{Q}$-rational points. Two of them are cuspidal. Two of them arise from points in $X_0(39)$ defined over $\mathbb{Q}(\sqrt{-7})$. Hence, no such E can exist, since a K-rational point on $X_0(39)$ which is also $\mathbb{Q}(\sqrt{-7})$-rational must be $\mathbb{Q}$-rational (and again by [32], $X_0(39)$ has no non-cuspidal $\mathbb{Q}$-rational points). □

Outline of Proof of Theorem 1. Using modularity of E, which now follows from Serre's conjecture [47], [33], [34], [35], plus the usual level lowering arguments based on results in [45], we have that $\rho_{E,\pi,\beta} \cong \rho_{g,\pi}$ where g is a newform in $S_2(\Gamma_0(M), \epsilon)$ where $M = 48$ or $M = 432$. This holds for $n = p \geq 11$.

There is one newform F_1 in $S_2(\Gamma_0(48), \epsilon)$ and this has CM by $\mathbb{Q}(-3)$; $\boxed{\text{inner-48.txt,cm-48.txt}}$. At level 432, we find three newforms G_1, G_2, G_3 in $S_2(\Gamma_0(432), \epsilon)$; $\boxed{\text{inner-432.txt}}$. As it transpires, both G_1 and G_2 have CM by $\mathbb{Q}(-3)$; $\boxed{\text{cm-432.txt}}$. The form G_3 is harder to eliminate as it does not have complex multiplication and its field of coefficients is $M_\beta = \mathbb{Q}(\sqrt{3}, i)$. Furthermore, the complex conjugate of G_3 is a twist of G_3 by ϵ^{-1}. In fact, G_3 arises from the near solution $1^2 + 1^6 = 2$ (this near solution gives rise to a form at level 432 and it is the unique non-CM form at that level) so it shares many of the same properties g should have as both arise from the same geometric construction. Note however one cannot have $a \equiv b \equiv 1 \pmod 2$ in the equation $a^2 + b^6 = c^p$ as $p > 1$.

Unfortunately, it is not possible to eliminate the possibility of $g = G_3$ by considering the fields cut out by images of inertia at 2. Using [36, Théorème 3] and its proof, it can be checked that these fields are the same regardless of whether or not $a \equiv b \equiv 1 \pmod 2$.

In the next two sections, we show that in each case $g = G_i$, for $i = 1, 2$ (CM case), and $i = 3$, we are led to a contradiction, if $n = p \geq 11$. Finally, in the last section, we deal with the cases $n = 3, 4, 5, 7$. This suffices to prove the theorem as any integer $n \geq 3$ is either divisible by an odd prime or by 4.

4. Eliminating the CM forms

When $g = G_i$ for $i = 1$ or 2, g has complex multiplication by $\mathbb{Q}(\sqrt{-3})$ so that $\rho_{E,\beta,\pi}$ has image lying in the normalizer of a Cartan subgroup for $p > 3$. However, this leads to a contradiction using the arguments below.

Proposition 18. *Let $p \geq 7$ be prime and suppose there exists either, a p-newform in $S_2(\Gamma_0(3p^2))$ with $w_p f = f$, $w_3 f = -f$ or a p-newform in $S_2(\Gamma_0(p^2))$ with $w_p f = f$, such that $L(f \otimes \chi_{-4}, 1) \neq 0$, where χ_{-4} is the Dirichlet character associated to $K = \mathbb{Q}(i)$. Let E be an elliptic curve which gives rise to a non-cuspidal $\mathbb{Q}$-rational point on $X^K_{0,N}(3,p)$ or $X^K_{0,N'}(3,p)$. Then E has potentially good reduction at all primes of K above $\ell > 3$.*

Proof. cf. [29] and comments in [3, Proposition 6] about the applicability to the split case (see also the argument in [29, Lemma 3.5] which shows potentially good reduction at a prime of K above p in the split case). □

Proposition 19. *If $p \geq 11$ is prime, then there exists a p-newform $f \in S_2(\Gamma_0(p^2))$ with $w_p f = f$ and $L(f \otimes \chi_{-4}, 1) \neq 0$.*

Proof. For $p \geq 61$, this is, essentially, the content of the proof of Proposition 7 of [3] (note that the proof applies to $p \equiv 1 \pmod 8$, not just to $p \not\equiv 1 \pmod 8$ as stated). Further, a relatively short Magma computation newform-twists.txt reveals the same to be true for smaller values of p with the following forms f (the number following the level indicates Magma's ordering of forms; one should note that this numbering is consistent neither with Stein's modular forms database nor with Cremona's tables)

p	f	dim$f$	p	f	dim$f$	p	f	dim$f$
11	121(1)	1	29	841(1)	2	47	2209(9)	16
13	169(2)	3	31	961(1)	2	53	2809(1)	1
17	289(1)	1	37	1369(1)	1	59	3481(1)	2
19	361(1)	1	41	1681(1)	2			
23	529(7)	4	43	1849(1)	1			

□

Theorem 20. *Suppose the representation $\rho_{E,\beta,\pi}$ has image lying in the normalizer of a Cartan subgroup for $p \geq 11$. Then E has potentially good reduction at all primes of K above $\ell > 3$.*

Proof. We note that E still gives rise to a $\mathbb{Q}$-rational point on $X_{0,N}^K(3,p)$ or $X_{0,N'}^K(3,p)$ with $K = \mathbb{Q}(i)$, even though, as a consequence of Lemma 14, the isogeny between E and its conjugate is only defined over $\mathbb{Q}(\sqrt{3}, i)$. □

Theorem 21. *If $p \geq 11$ is prime, the representation $\rho_{E,\beta,\pi}$ does not have image lying in the normalizer of a Cartan subgroup.*

Proof. Lemma 4 immediately implies that E necessarily has multiplicative bad reduction at a prime of K lying above some $\ell > 3$. □

5. Eliminating the newform G_3

Recall that $E = E_{a,b}$ is given by

$$E \ : \ Y^2 = X^3 - 3(5b^3 + 4ai)bX + 2(11b^6 + 14ib^3a - 2a^2).$$

Let $E' = E'_{a,b}$ be the elliptic curve

$$E' \ : \ Y^2 = X^3 + 3b^2X + 2a.$$

which is a Frey-Hellegouarch elliptic curve over $\mathbb{Q}$ for the equation $a^2 + (b^2)^3 = c^p$. We will show how to eliminate the case of $g = G_3$ using a combination of congruences from the two Frey curves E and E'. This is an example of the multi-Frey technique (cf. [13] and [14]), as applied to the situation when one of the Frey curves is a $\mathbb{Q}$-curve. We are grateful to S. Siksek for suggesting a version of Lemma 24 which allows us to do this.

The discriminant of E' is given by

$$\Delta' = -2^6 \cdot 3^3(a^2 + b^6). \tag{11}$$

For $a \not\equiv b \pmod 2$, $v_2(\Delta') = 6$ so E' is in minimal form at 2. Since $(a,b) \not\equiv (0,0) \pmod 3$, we have that $v_3(\Delta') = 3$ and so E' is also minimal at 3. For $q \mid \Delta'$ and $q \neq 2, 3$, E' has multiplicative bad reduction at q.

For each congruence class of (a,b) modulo 2^4 where $a \not\equiv b \pmod 2$, we compute the conductor exponent at 2 of E' using MAGMA. The conductor exponent at 2 of each test case was 5 (reduction type III) or 6 (reduction type II) : tate2m-3.txt. By Lemma 5, case (3), the conductor exponent at 2 of E' is 5 or 6. In a similar way, the conductor exponent at 3 of E' is 2 (reduction type III) or 3 (reduction type II) : $\boxed{\text{tate3m-3.txt}}$.

We are now almost in position to apply the modular method to E'. We need only show that the representation $\rho_{E',p}$ arising from the p-torsion points of E' is irreducible.

Lemma 22. *If $p \geq 11$ is prime, then $\rho_{E',p}$ is irreducible.*

Proof. If $p \neq 13$, the result follows essentially from work of Mazur [40] (see Theorem 22 of [22]), provided $j_{E'}$ is not one of

$$-2^{15}, -11^2, -11 \cdot 131^3, \frac{-17 \cdot 373^3}{2^{17}}, \frac{-17^2 \cdot 101^3}{2}, -2^{15} \cdot 3^3, -7 \cdot 137^3 \cdot 2083^3,$$
$$-7 \cdot 11^3, -2^{18} \cdot 3^3 \cdot 5^3, -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3, -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3.$$

Since

$$j_{E'} = \frac{1728\, b^6}{a^2 + b^6} > 0,$$

we may thus suppose that $p = 13$. In this case, if $\rho_{E',p}$ were reducible, the representation would correspond to a rational point on the curve defined via the equation $j_{13}(t) = j_{E'}$, where $j_{13}(t)$ is the map from the modular curve $X_0(13)$ to $X(1)$, given by

$$\begin{aligned} j_{13}(t) &= \frac{(t^4 + 7t^3 + 20t^2 + 19t + 1)^3 (t^2 + 5t + 13)}{t} \\ &= \frac{(t^6 + 10t^5 + 46t^4 + 108t^3 + 122t^2 + 38t - 1)^2 (t^2 + 6t + 13)}{t} + 1728. \end{aligned}$$

Writing $s = a/b^3$, we thus have $\frac{1728}{s^2+1} = j_{13}(t)$, for some $t \in \mathbb{Q}$, and so

$$s^2 = \frac{1728 - j_{13}(t)}{j_{13}(t)} = -\frac{(t^6 + 10t^5 + 46t^4 + 108t^3 + 122t^2 + 38t - 1)^2 (t^2 + 6t + 13)}{(t^4 + 7t^3 + 20t^2 + 19t + 1)^3 (t^2 + 5t + 13)}.$$

It follows that there exist rational numbers x and y with

$$y^2 = -(x^2 + 6x + 13)(x^2 + 5x + 13)(x^4 + 7x^3 + 20x^2 + 19x + 1),$$

and hence coprime, nonzero integers u and v, and an integer z for which

$$(u^2 + 6uv + 13v^2)(u^2 + 5uv + 13v^2)(u^4 + 7u^3v + 20u^2v^2 + 19uv^3 + v^4) = -z^2.$$

Note that, via a routine resultant calculation, if a prime p divides both $u^2 + 6uv + 13v^2$ and the term $(u^2+5uv+13v^2)(u^4+7u^3v+20u^2v^2+19uv^3+v^4)$, then necessarily $p \in \{2, 3, 13\}$. Since $u^2+6uv+13v^2$ is positive definite and u, v are coprime (whereby $u^2 + 6uv + 13v^2 \equiv \pm 1 \pmod 3$), we thus have

$$u^2 + 6uv + 13v^2 = 2^{\delta_1} 13^{\delta_2} z_1^2, \quad \text{and}$$
$$(u^2 + 5uv + 13v^2)(u^4 + 7u^3v + 20u^2v^2 + 19uv^3 + v^4) = -2^{\delta_1} 13^{\delta_2} z_2^2,$$

for $z_1, z_2 \in \mathbb{Z}$ and $\delta_i \in \{0, 1\}$. The first equation, with $\delta_1 = 1$, implies that $u \equiv v \equiv 1 \pmod 2$, contradicting the second. We thus have $\delta_1 = 0$, whence

$$u^2 + 6uv + 13v^2 \equiv u^2 + v^2 \equiv z_1^2 \equiv 1 \pmod 3,$$

so that 3 divides one of u and v, again contradicting the second equation, this time modulo 3. □

Applying the modular method with E' as the Frey curve thus shows that $\rho_{E',p} \cong \rho_{g',\pi'}$ for some newform $g' \in S_2(\Gamma_0(M))$ where $M = 2^r 3^s$, $r \in \{5, 6\}$, and $s \in \{2, 3\}$ (here π' is a prime above p in the field of coefficients of g'). The possible forms g' were computed using $\boxed{\text{b3i-modformagain.txt}}$. The reason the multi-Frey method works is because when $a \not\equiv b \pmod 2$, we have that $r \in \{5, 6\}$, whereas when $a \equiv b \equiv 1 \pmod 2$, we have that $r = 7$. Thus, the 2-part of the conductor of $\rho_{E',\pi}$ separates the cases $a \not\equiv b \pmod 2$ and $a \equiv b \pmod 2$. Hence, the newform g' that the near solution $a = b = 1$ produces does not cause trouble from the point of view of the Frey curve E'. By linking the two Frey curves E and E', it is possible to pass this information from the Frey curve E' to the Frey curve E, by appealing to the multi-Frey technique.

The following lemma results from the condition $\rho_{E',p} \cong \rho_{g',\pi'}$ and standard modular method arguments.

Lemma 23. *Let $q \geq 5$ be prime and assume $q \neq p$, where $p \geq 11$ is a prime. Let*

$$C_{x,y}(q, g') = \begin{cases} a_q(E'_{x,y}) - a_q(g') & \text{if } x^2 + y^6 \not\equiv 0 \pmod q \\ (q+1)^2 - a_q(g')^2 & \text{if } x^2 + y^6 \equiv 0 \pmod q \end{cases}.$$

If $(a, b) \equiv (x, y) \pmod q$, then $p \mid C_{x,y}(q, g')$.

For our choice of splitting map β, we attached a Galois representation $\rho_{E,\beta,\pi}$ to E such that $\rho_{E,\beta,\pi} \cong \rho_{g,\pi}$ for some newform $g \in S_2(\Gamma_0(M), \epsilon)$ where $M = 48, 432$. We wish to eliminate the case of $g = G_3$. The following is the analog of Lemma 23 for $E = E_{a,b}$.

Lemma 24. *Let $q \geq 5$ be prime and assume $q \neq p$, where $p \geq 11$ is prime. Let*

$$B_{x,y}(q, g) = \begin{cases} N(a_q(E_{x,y})^2 - \epsilon(q) a_q(g)^2) & \text{if } x^2 + y^6 \not\equiv 0 \pmod q \text{ and } \left(\frac{-4}{q}\right) = 1 \\ N(a_q(g)^2 - a_{q^2}(E_{x,y}) - 2q\epsilon(q)) & \text{if } x^2 + y^6 \not\equiv 0 \pmod q \text{ and } \left(\frac{-4}{q}\right) = -1 \\ N(\epsilon(q)(q+1)^2 - a_q(g)^2) & \text{if } x^2 + y^6 \equiv 0 \pmod q \end{cases},$$

where $a_{q^i}(E_{x,y})$ is the trace of Frob_q^i acting on the Tate module $T_p(E_{x,y})$.

If $(a, b) \equiv (x, y) \pmod q$, then $p \mid B_{x,y}(q, g)$.

Proof. Recall the set-up in Section 2 and Section 3. Let π be a prime of M_β above p. The mod π representation $\rho_{A_\beta,\pi}$ of $G_{\mathbb{Q}}$ attached to A_β is related to E_β by

$$\mathbb{P}\rho_{A_\beta,\pi}\mid_{G_K}\cong \mathbb{P}\phi_{E_\beta,p},$$

where $\phi_{E_\beta,p}$ is the representation of G_K on the p-adic Tate module $T_p(E_\beta)$ of E_β, and the $\mathbb{P}$ indicates that we are considering isomorphism up to scalars. The algebraic formula which describes $\rho_{E_\beta,\beta,\pi} = \rho_{A_\beta,\pi}\cong\rho_{f,\pi}$ is

$$\rho_{A_\beta,\pi}(\sigma)(1\otimes x)=\beta(\sigma)^{-1}\otimes\mu'_\beta(\sigma)(\phi_{E_\beta,p}(\sigma)(x))$$

where $1\otimes x\in M_{\beta,\pi}\otimes T_p(E_\beta)$. Here, $\mu'_\beta(\sigma)$ is the chosen isogeny from ${}^\sigma E_\beta\to E_\beta$ for each σ which is constant on G_K (see the paragraph after (6)).

$x^2+y^6\equiv 0 \pmod q$, then $q\mid c$. Recall the conductor of A_β is given by

$$2^4\cdot 3^{1+\varepsilon/2}\cdot\prod_{q\mid c,q\neq 2,3} q$$

so that q exactly divides the conductor of A_β. Using the condition $\rho_{f,\pi}\cong\rho_{g,\pi}$, we can deduce from cf. [15, Théorème 2.1], [16, Théorème (A)], [25, Theorem 3.1], [31, (0.1)] that

$$p\mid N\left(a_q(g)^2-\epsilon^{-1}(q)\,(q+1)^2\right).$$

If $x^2+y^6\not\equiv 0 \pmod q$, then let $\mathfrak{q}$ be a prime of K_β over q. Let $\overline{E}=\overline{E}_{a,b}$ be the reduction modulo $\mathfrak{q}$ of E. Since $(a,b)\equiv(x,y)\pmod q$, we have the $\overline{E}=E_{x,y}$. Furthermore, since $\mathfrak{q}$ is a prime of good reduction, $T_p(E)\cong T_p(\overline{E})$.

We now wish to relate the representation $\rho_{E_\beta,\beta,\pi}=\rho_{A_\beta,\pi}\cong\rho_{f,\pi}$ to the representation $\phi_{E,p}$ for the original E. We know that

$$c_{E_\beta}(\sigma,\tau)=\beta(\sigma)\beta(\tau)\beta(\sigma\tau)^{-1}$$
$$c_{E_\beta}(\sigma,\tau)=c_E(\sigma,\tau)\kappa(\sigma)\kappa(\tau)\kappa(\sigma\tau)^{-1}$$

where $\kappa(\sigma)=\frac{{}^\sigma\sqrt{\gamma}}{\sqrt{\gamma}}$ and $\gamma=\frac{-3+i\sqrt{3}}{2}$. It follows that

$$c_E(\sigma,\tau)=\beta'(\sigma)\beta'(\tau)\beta'(\sigma\tau)^{-1},$$

where $\beta'(\sigma)=\beta(\sigma)\kappa(\sigma)$, so that β' is a splitting map for the original cocycle $c_E(\sigma,\tau)$. Also, recall that $\epsilon(\mathrm{Frob}_q)=\left(\frac{12}{q}\right)$.

Now we have that

$$\rho_{A_{\beta'},\pi}(\sigma)(1\otimes x)=\beta'(\sigma)^{-1}\otimes\mu(\sigma)(\phi_{E,p}(\sigma)(x)),$$

where $1 \otimes x \in M_{\beta,\pi} \otimes T_p(E)$. For this choice of $\beta'(\sigma)$,

$$\rho_{A_{\beta'},\pi} \cong \kappa(\sigma)\xi(\sigma) \otimes \rho_{A_\beta,\pi} \cong \kappa(\sigma)\xi(\sigma) \otimes \rho_{f,\pi}.$$

This can be seen by fixing the isomorphism $\iota : E \cong E_\beta$, using standard Weierstrass models and then appealing to the following commutative diagram.

$$\begin{tikzcd}
E_\beta \arrow[r, "\sigma"] & {}^\sigma E_\beta \arrow[r, "\mu_{E_\beta}(\sigma)"] & E_\beta \\
E \arrow[u, "\iota"] \arrow[r, "\sigma"] & {}^\sigma E \arrow[u, "{}^\sigma\iota"] \arrow[r, "\mu_E(\sigma)"] & E \arrow[u, "\iota"]
\end{tikzcd}$$

Recall $\beta(\sigma) = \sqrt{\epsilon(\sigma)}\sqrt{d(\sigma)}$ so that $\beta'(\sigma) = \sqrt{\epsilon(\sigma)}\sqrt{d(\sigma)}\kappa(\sigma)$. We note that $d(\sigma) = 1$ if $\sigma \in G_{\mathbb{Q}(\sqrt{-1})}$ and $d(\sigma) = 3$ if $\sigma \notin G_{\mathbb{Q}(\sqrt{-1})}$.

Now $\left(\frac{-4}{q}\right) = 1$ means $\sigma = \mathrm{Frob}_q \in G_{\mathbb{Q}(\sqrt{-1})}$. If $\sigma \in G_{\mathbb{Q}(\sqrt{-1})}$, then $\mu(\sigma) = \mathrm{id}$ and $d(\sigma) = 1$ so $\rho_{A_{\beta'},\pi}(\sigma)(1 \otimes x) = \beta'(\sigma)^{-1} \otimes \mu(\sigma)(\phi_{E,p}(\sigma)(x)) = \sqrt{\epsilon(\sigma)}^{-1}\kappa(\sigma)^{-1} \otimes \phi_{E,p}(\sigma)(x)$ so $\mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma) = \sqrt{\epsilon(\sigma)}^{-1}\kappa(\sigma)^{-1} \cdot \mathrm{tr}\,\phi_{E,p}(\sigma)$ and $\epsilon(q)a_q(f)^2 = a_q(E)^2$. And we have that $a_q(f) \equiv a_q(g) \pmod{\pi}$, giving the assertion that $p \mid B_\alpha(q, g)$ in the case $\left(\frac{-4}{q}\right) = 1$.

If $\left(\frac{-4}{q}\right) = -1$, then $\sigma = \mathrm{Frob}_q \notin G_{\mathbb{Q}(\sqrt{-1})}$. But then $\sigma^2 \in G_{\mathbb{Q}(\sqrt{-1})}$, and in fact, $\sigma^2 \in G_{\mathbb{Q}(\sqrt{-1},\sqrt{3})}$, so by the above argument we get that $\mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma^2) = \sqrt{\epsilon(\sigma)}^{-1}\kappa(\sigma)^{-1} \cdot \mathrm{tr}\,\phi_{E,p}(\sigma^2) = \mathrm{tr}\,\phi_{E,p}(\sigma^2) = a_{q^2}(E)$. Also, $\mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma) = \kappa(\sigma)\xi(\sigma)a_q(f)$ so $\mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma)^2 = a_q(f)^2$. We have that

$$\begin{aligned}
\frac{1}{\det(1 - \rho_{A_{\beta'},\pi}(\sigma)q^{-s})} &= \exp\sum_{r=1}^{\infty} \mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma^r)\frac{q^{-sr}}{r} \\
&= \frac{1}{1 - \mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma)q^{-s} + q\epsilon(q)q^{-2s}}.
\end{aligned}$$

The determinant and traces are of vector spaces over $M_{\beta,\pi}$. Computing the coefficient of q^{-2s} and equating, we find that $\mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma^2) = \mathrm{tr}\,\rho_{A_{\beta'},\pi}(\sigma)^2 - 2q\epsilon(q)$ and hence conclude that $a_q(f)^2 - 2q\epsilon(q) = a_{q^2}(E)$. Since $a_q(f) \equiv a_q(g) \pmod{\pi}$, it follows that $p \mid B_\alpha(q, g)$ in the case $\left(\frac{-4}{q}\right) = -1$ as well. $\square$

Let

$$A_q(g, g') := \prod_{(x,y)\in\mathbb{F}_q^2 - \{(0,0)\}} \gcd(B_{x,y}(q, g), C_{x,y}(q, g')).$$

Then we must have that $p \mid A_q(g, g')$. For a pair g, g', we can pick a prime q and compute $A_q(g, g')$. Whenever this $A_q(g, g') \neq 0$, we obtain a bound on p so that the pair g, g' cannot arise for p larger than this bound.

For $g = G_3$, and g' running through the newforms in $S_2(\Gamma_0(2^r3^s))$ where $r \in \{5, 6\}$ and $s \in \{2, 3\}$, the above process eliminates all possible pairs $g = G_3$ and g'; see multi-frey.txt. In particular, using

$q = 5$ or $q = 7$ for each pair shows that $p \in \{2, 3, 5\}$. Hence, if $p \notin \{2, 3, 5, 7\}$, then a solution to our original equation cannot arise from the newform $g = G_3$.

6. The cases $n = 3, 4, 5$ and 7

It thus remains only to treat the equation $a^2 + b^6 = c^n$ for $n \in \{3, 4, 5, 7\}$. In each case, without loss of generality, we may suppose that we have a proper, nontrivial solution in positive integers a, b and c. If $n = 4$ or 7, the desired result is immediate from work of Bruin [9] and Poonen-Schaefer-Stoll [43], respectively. In the case $n = 3$, a solution with $b \neq 0$ implies, via the equation

$$\left(\frac{a}{b^3}\right)^2 = \left(\frac{c}{b^2}\right)^3 - 1,$$

a rational point on the elliptic curve given by $E : y^2 = x^3 - 1$, Cremona's 144A1 of rank 0 over $\mathbb{Q}$ with $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. It follows that $c = b^2$ and hence $a = 0$.

Finally, we suppose that $a^2+b^6 = c^5$, for coprime positive integers a, b and c. From parametrizations for solutions to $x^2 + y^2 = z^5$ (see e.g. [18, Lemma 2]), it is easy to show that there exist coprime integers u and v (and z) for which

$$v^4 - 10v^2u^2 + 5u^4 = 5^\delta z^3 \tag{12}$$

with either (a) $v = \beta^3, \delta = 0$, β coprime to 5; or (b) $v = 5^2\beta^3, \delta = 1$, for some integer β. Let us begin by treating the latter case. From (12), we have that

$$\left(u^2 - v^2\right)^2 - 4 \cdot 5^7 \cdot \beta^{12} = z^3$$

and hence taking

$$x = \frac{z}{5^2\beta^4}, \quad y = \frac{u^2 - v^2}{5^3\beta^6},$$

we have a rational point on $E : y^2 = x^3 + 20$, Cremona's 2700E1 of rank 0 and trivial torsion (with no corresponding solutions of interest to our original equation).

We may thus suppose that we are situation (a), so that

$$\beta^{12} - 10\beta^6u^2 + 5u^4 = z^3. \tag{13}$$

Since β and u are coprime, we may assume that they are of opposite parity (and hence that z is odd), since $\beta \equiv u \equiv 1 \pmod 2$ with (13) leads to an immediate contradiction modulo 8. Writing $T = \beta^6 - 5u^2$, (13) becomes $T^2 - 20u^4 = z^3$, where T is coprime to 10. Factoring over $\mathbb{Q}(\sqrt{5})$ (which has class number 1), we deduce the existence of integers m and n, of the same parity, such that

$$T + 2\sqrt{5}u^2 = \left(\frac{1+\sqrt{5}}{2}\right)^\delta \left(\frac{m+n\sqrt{5}}{2}\right)^3, \tag{14}$$

with $\delta \in \{0, 1, 2\}$.

Let us first suppose that $\delta = 1$. Then, expanding (14), we have

$$m^3 + 15m^2n + 15mn^2 + 25n^3 = 16T \text{ and } m^3 + 3m^2n + 15mn^2 + 5n^3 = 32u^2.$$

It follows that

$$3m^2n + 5n^3 = 4T - 8u^2 \equiv 4 \pmod 8,$$

contradicting the fact that m and n have the same parity. Similarly, if $\delta = 2$, we find that

$$3m^3 + 15m^2n + 45mn^2 + 25n^3 = 16T \text{ and } m^3 + 9m^2n + 15mn^2 + 15n^3 = 32u^2,$$

and so

$$3m^2n + 5n^3 = 24u^2 - 4T \equiv 4 \pmod 8,$$

again a contradiction.

We thus have that $\delta = 0$, and so

$$m(m^2 + 15n^2) = 8T = 8(\beta^6 - 5u^2) \text{ and } n(3m^2 + 5n^2) = 16u^2. \tag{15}$$

Combining these equations, we may write

$$16\,\beta^6 = (m + 5n)(2m^2 + 5mn + 5n^2). \tag{16}$$

Returning to the last equation of (15), since $\gcd(m, n)$ divides 2, we necessarily have that $n = 2^{\delta_1}3^{\delta_2}r^2$ for some integers r and $\delta_i \in \{0, 1\}$. Considering the equation $n(3m^2 + 5n^2) = 16u^2$ modulo 5 implies that $(\delta_1, \delta_2) = (1, 0)$ or $(0, 1)$. In case $(\delta_1, \delta_2) = (1, 0)$, the two equations in (15), taken together, imply a contradiction modulo 9.

We may thus suppose that $(\delta_1, \delta_2) = (0, 1)$ and, setting $y = (2\beta/r)^3$ and $x = 6m/n$ in (16), we find that

$$y^2 = (x + 30)(x^2 + 15\,x + 90).$$

This elliptic curve is Cremona's 3600G1, of rank 0 with nontrivial torsion corresponding to $x = -30, y = 0$.

It follows that there do not exist positive coprime integers a, b and c for which $a^2 + b^6 = c^5$, which completes the proof of Theorem 1.

7. Acknowledgements

The authors would like to thank Samir Siksek and Sander Dahmen for useful suggestions and correspondence pertaining to this paper, and the anonymous referees for numerous helpful comments.

References

[1] M. Bennett. The equation $x^{2n} + y^{2n} = z^5$. *J. Théor. Nombres Bordeaux* 18 (2006), no. 2, 315–321.

[2] M. Bennett, I. Chen, S. Dahmen and S. Yazdani. Generalized Fermat equations : a miscellany. In preparation.

[3] M. Bennett, J. Ellenberg, and N. Ng. The Diophantine equation $A^4 + 2^\delta B^2 = C^n$. *Int. J. Number Theory* 6 (2010), 311–338.

[4] M. Bennett and C. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.* 56 (2004), 23–54.

[5] M. Bennett, V. Vatsal and S. Yazdani. Ternary Diophantine equations of signature $(p, p, 3)$. *Compos. Math.* 140 (2004), 1399–1416.

[6] F. Beukers. The Diophantine equation $Ax^p + By^q = Cz^r$. *Duke Math. J.* 91 (1998), 61–88.

[7] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993). *J. Symbolic Comput.* 24 (1997), 235–265.

[8] D. Brown. Primitive Integral Solutions to $x^2 + y^3 = z^{10}$, *Internat. Math. Res. Notices*, to appear.

[9] N. Bruin. The Diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$. *Compos. Math.* 118 (1999), 305–321.

[10] N. Bruin. On powers as sums of two cubes. In *Algorithmic Number Theory* (Leiden, 2000), Lecture Notes in Comput. Sci., vol 1838, Springer, Berlin, 2000, pp. 169–184.

[11] N. Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.* 562 (2003), 27–49.

[12] N. Bruin. The primitive solutions to $x^3 + y^9 = z^2$. *J. Number Theory* 111 (2005), no. 1, 179–189.

[13] Y. Bugeaud, F. Luca, M. Mignotte, and S. Siksek. Almost powers in the Lucas sequences. *J. Théor. Nombres Bordeaux* 20 (2008), 555–600.

[14] Y. Bugeaud, M. Mignotte, and S. Siksek. A multi-Frey approach to some multi-parameter families of Diophantine equations. *Canad. J. Math.* 60 (2008), 491–519.

[15] H. Carayol. Sur les représentations l-adiques attachées aux formes modulaires de Hilbert. *C. R. Acad. Sci. Paris Sér. I Math.* 296 (1983), 629–632.

[16] H. Carayol. Sur les représentations l-adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup.* 19 (1986), 409–468.

[17] I. Chen. On the equation $s^2 + y^{2p} = \alpha^3$. *Math. Comp.* 77 (2008), 1223–1227.

[18] I. Chen. On the equation $a^2 + b^{2p} = c^5$. *Acta Arith.* 143 (2010), 345–375.

[19] I. Chen. On the equation $a^2 - 2b^6 = c^p$, submitted for publication, September 2008.

[20] I. Chen and S. Siksek. Perfect powers expressible as sums of two cubes. *J. Algebra* 322 (2009), 638–656.

[21] D. Cox. *Primes of the Form $x^2 + ny^2$*. John Wiley & Sons, Inc., 1989.

[22] S. Dahmen. Classical and modular methods applied to Diophantine equations, PhD thesis, University of Utrecht, 2008. Permanently available at
`igitur-archive.library.uu.nl/dissertations/2008-0820-200949/UUindex.html`

[23] S. Dahmen. A refined modular approach to the Diophantine equation $x^2 + y^{2n} = z^3$. *Int. J. Number Theory*, to appear. cf. `arXiv: 1002.0020`

[24] H. Darmon. Rigid local systems, Hilbert modular forms, and Fermat's Last Theorem, *Duke. Math. J.* 102 (2000), 413–449.

[25] H. Darmon, F. Diamond, and R. Taylor. Fermat's Last Theorem. In *Elliptic curves, modular forms & Fermat's Last Theorem (Hong Kong, 1993)*, pages 2–140. International Press, 1997.

[26] H. Darmon and A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.* 27 (1995), 513–543.

[27] H. Darmon and L. Merel. Winding quotients and some variants of Fermat's Last Theorem, *J. Reine Angew. Math.* 490 (1997), 81–100.

[28] L. Dieulefait and J.J. Urroz. Solving Fermat-type equations $x^4 + dy^2 = z^p$ via modular $\mathbb{Q}$-curves over polyquadratic fields. *J. Reine Angew. Math*, 633 (2009),183-195.

[29] J. Ellenberg. Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$. *Amer. J. Math.* 126 (2004), 763–787.

[30] J. Ellenberg and C. Skinner. On the modularity of $\mathbb{Q}$-curves. *Duke Math. J.* 109 (2001), 97–122.

[31] B. H. Gross. A tameness criterion for Galois representations associated to modular forms (mod p). *Duke Math. J.* 61 (1980), 445–517.

[32] M. Kenku. The modular curve $X_0(39)$ and rational isogeny. *Math. Proc. Camb. Philos. Soc.* 85 (1979), 21–23.

[33] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture (I). *Invent. Math.* 178 (2009), 485–504.

[34] C. Khare and J.-P. Wintenberger. Serre's modularity conjecture (II). *Invent. Math.* 178 (2009), 505–586.

[35] M. Kisin. Modularity of 2-adic Barsotti-Tate representations. *Invent. Math.* 178 (2009), 587–634.

[36] A. Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta Math.* 69 (1990), 353–385.

[37] A. Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experiment. Math.* 7 (1998), 1–13.

[38] A. Kraus. Une question sur les équations $x^m - y^m = Rz^n$. *Compos. Math.* 132 (2002), 1–26.

[39] R. Mauldin. A generalization of Fermat's Last Theorem: the Beal conjecture and prize problem. *Notices Amer. Math. Soc.* 44 (1997), 1436–1437.

[40] B. Mazur. Rational isogenies of prime degree. *Invent. Math.* 44 (1978), 129–162

[41] J. Milne. On the arithmetic of abelian varieties. *Invent. Math.* 17 (1972), 177–190.

[42] B. Poonen. Some Diophantine equations of the form $x^n + y^n = z^m$, *Acta Arith.* 86 (1998), 193–205.

[43] B. Poonen, E. Schaefer, and M. Stoll. Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$. *Duke Math. J.* 137 (2007), 103–158.

[44] J. Quer. $\mathbb{Q}$-curves and abelian varieties of GL_2-type. *Proc. London Math. Soc.* 81(2000), 285–317.

[45] K. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. *Invent. Math.* 100 (1990), 431–476.

[46] K. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms. In *Algebra and Topology 1992*, Korea Adv. Inst. Sci. Tech., pages 53–79, 1992.

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

[48] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, 1994.

[49] S. Siksek. Explicit Chabauty over number fields. `arXiv: 1010.2603`

[50] S. Siksek. Personal communication with the second author, 2008.

[51] K. Takeuchi. Commensurability classes of arithmetic triangle groups. *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 24 (1977), 201–212.

[52] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math.* 141 (1995), 553–572.

[53] R. Tijdeman. Diophantine equations and diophantine approximations. *Number theory and applications (Banff, AB, 1988)*, Kluwer Acad. Publ., Dordrecht, 1989, 215–243.

[54] A. Wiles. Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math* 141 (1995), 443–551.

Michael A. Bennett, Department of Mathematics, University of British Columbia, Vancouver, British Columbia, V6T 1Z2, CANADA

E-mail address: `bennett@math.ubc.ca`

Imin Chen, Department of Mathematics, Simon Fraser University, Burnaby, British Columbia, V5A 1S6, CANADA

E-mail address: `ichen@math.sfu.ca`