ACTA ARITHMETICA
163.4 (2014)

On the equation $a^3 + b^{3n} = c^2$

by

Michael A. Bennett (Vancouver, BC), Imin Chen (Burnaby, BC),
Sander R. Dahmen (Amsterdam)
and Soroosh Yazdani (Lethbridge, AB)

1. Introduction. In [2], a detailed survey of the generalized Fermat equations which occur through descent from spherical cases was performed. One situation encountered is that of the equation

$$a^3 + b^{3n} = c^2, \tag{1.1}$$

arising from consideration of the spherical case $x^3 + y^3 = z^2$. In this paper, we apply the machinery of Galois representations and modular forms to (1.1) to prove the following.

Theorem 1.1. *If n is prime with $n \equiv 1 \pmod 8$, then equation* (1.1) *has no solutions in coprime non-zero integers a, b and c, apart from those given by $(a, b, c) = (2, 1, \pm 3)$.*

It should be noted that the presence of a "trivial" solution here (that corresponding to the solution to Catalan's equation) is a basic obstruction to solving (1.1) that we must work rather hard to overcome.

Theorem 1.1 is an immediate consequence of the following two results, where we specialize to the cases of c odd and even, respectively.

Proposition 1.2. *If n is prime with $n \equiv 1, 3 \pmod 8$ and $n \geq 17$, then the equation $a^3 + b^{3n} = c^2$ has no solutions in coprime non-zero integers a, b and c with c odd, apart from those given by $(a, b, c) = (2, 1, \pm 3)$.*

Proposition 1.3. *If n is prime with $n \equiv 1 \pmod 4$ and $n \geq 17$, then the equation $a^3 + b^{3n} = c^2$ has no solutions in coprime non-zero integers a, b and c with c even.*

2010 *Mathematics Subject Classification*: Primary 11D41; Secondary 11D61, 11G05, 14G05.
Key words and phrases: Fermat equations, Galois representations, $\mathbb{Q}$-curves, multi-Frey techniques.

DOI: 10.4064/aa163-4-3

After collecting some preliminary technical tools in Section 2, we will provide a proof of these two propositions (and thereby of our main theorem) in Section 3. The techniques involve a rather intricate combination of ingredients, including the use of $\mathbb{Q}$-curves and delicate multi-Frey and "image of inertia" arguments.

2. Preliminaries. In this section, we begin by collecting some of the technical tools that we will use throughout this paper. We first consider the equation $x^3+y^3=z^2$. Note that, from [6, pp. 467–470], the coprime integer solutions to this equation satisfy one of

$$\begin{cases} x = s(s+2t)(s^2-2ts+4t^2), \\ y = -4t(s-t)(s^2+ts+t^2), \\ z = \pm(s^2-2ts-2t^2)(s^4+2ts^3+6t^2s^2-4t^3s+4t^4), \end{cases} \tag{2.1}$$

$$\begin{cases} x = s^4-4ts^3-6t^2s^2-4t^3s+t^4, \\ y = 2(s^4+2ts^3+2t^3s+t^4), \\ z = 3(s-t)(s+t)(s^4+2s^3t+6s^2t^2+2st^3+t^4), \end{cases} \tag{2.2}$$

or

$$\begin{cases} x = -3s^4+6t^2s^2+t^4, \\ y = 3s^4+6t^2s^2-t^4, \\ z = 6st(3s^4+t^4). \end{cases} \tag{2.3}$$

Here, s and t are coprime integers with

$$\begin{cases} s \equiv 1 \pmod 2 \text{ and } s \not\equiv t \pmod 3 & \text{in case (2.1)}, \\ s \not\equiv t \pmod 2 \text{ and } s \not\equiv t \pmod 3 & \text{in case (2.2)}, \\ s \not\equiv t \pmod 2 \text{ and } t \not\equiv 0 \pmod 3 & \text{in case (2.3)}, \end{cases}$$

and the given parametrizations are up to exchange of x and y. To study our Diophantine equation (1.1), we are therefore reduced to solving the equations $x(s,t)=b^n$ and $y(s,t)=b^n$.

Our main tool to attack these equations is what is now known as the multi-Frey method. This proceeds by associating multiple Frey–Hellegouarch curves to a putative solution of one of these Diophantine equations, and subsequently applying techniques arising from the modularity of related Galois representations to extract information from each curve to (hopefully) deduce a contradiction. To carry out such an argument, one must start by computing the possible conductors for these Frey–Hellegouarch curves, a procedure which may be carried out by using Tate's algorithm (cf. [18]). However, it is convenient to note that the conductor exponent is locally constant, in the v-adic topology, on the coefficients defining the Frey–Hellegouarch curves.

This allows us to compute the conductor of a congruence class of elliptic curves by applying Tate's algorithm to concrete representative elliptic curves in MAGMA or SAGE (see also [5, Theorem 32]). To proceed, one requires an explicit bound on the v-adic balls on which the family of Frey–Hellegouarch curves have constant conductor exponent.

LEMMA 2.1. *Suppose E and E' are elliptic curves defined by*

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

where a_i and a'_i lie in a discrete valuation ring $\mathcal{O}$ with valuation v and uniformizer π. Let $\Delta_E, \Delta_{E'}, N_E$ and $N_{E'}$ denote the discriminants and conductors of E and E', and suppose that

$$\max\{v(\Delta_E), v(\Delta_{E'})\} \leq 12k$$

for some positive integer k. Suppose further that $v(a_i - a'_i) \geq ik$ for each $i \in \{1, 2, 3, 4, 6\}$.

(1) *If the reduction type of E' is not I^*_m for $m > 2$, then the reduction types of E and E' are the same. In this case, $v(N_E) = v(N_{E'})$.*
(2) *If the reduction type of E' is I^*_m for $m > 2$, then the reduction type of E is $I^*_{m'}$ for some $m' > 2$.*
(3) *In particular, E has good reduction if and only if E' has good reduction.*

Proof. This result is a consequence of carrying out Tate's algorithm (cf. [18]) on both curves simultaneously. ∎

In the remainder of this paper, n will always be an odd prime, and a newform will be assumed to be cuspidal of weight two with respect to $\Gamma_1(N)$ for some positive integer N (called, as usual, the *level*). For a prime ν in the field of coefficients of such a newform g, we denote the (standard) associated ν-adic Galois representation of $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and (the semisimplification of) its reduction modulo ν by $\rho_{g,\nu}$ and $\overline{\rho}_{g,\nu}$, respectively.

For a newform g on $\Gamma_1(N)$, let $a_q(g)$ denote its qth Fourier coefficient, or equivalently its eigenvalue for the Hecke operator T_q.

In the modular method, one attaches to each non-trivial putative solution of our Diophantine equation a Frey–Hellegouarch curve which gives rise to an associated Galois representation $\overline{\rho}$. Assuming that $\overline{\rho}$ is irreducible, by the recent proof of Serre's conjecture [17, 8, 9, 10], the modular machinery allows us to show that $\overline{\rho} \cong \overline{\rho}_{g,\nu}$ for a finite collection of newforms g. We then need to rule out each modular form g.

The following well-known theorem allows us to establish irreducibility when $\overline{\rho} = \overline{\rho}_{E,n}$ is the modulo n Galois representation of $G_{\mathbb{Q}}$ induced from the natural action of $G_{\mathbb{Q}}$ on the n-torsion points of an elliptic curve $E/\mathbb{Q}$.

THEOREM 2.2 (Mazur). *Let $E/\mathbb{Q}$ be an elliptic curve. Assume that E has bad multiplicative reduction at an odd prime. If $n \geq 11$, $n \neq 13$, is prime, then $\overline{\rho}_{E,n}$ is irreducible.*

Proof. See [12, Corollary 4.4]. ∎

A continuous irreducible Galois representation $\overline{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_n)$ is modular if

$$\overline{\rho} \cong \overline{\rho}_{g,\nu}$$

for a newform g on some $\Gamma_1(N)$ and prime ν above n. If this is the case, then g is a newform on $\Gamma_0(N)$ with some nebentypus ϵ^{-1}, and we have

$$\mathrm{tr}(\overline{\rho}(\mathrm{Frob}_q)) \equiv a_q(g) \pmod{\nu},$$
$$\det(\overline{\rho}(\mathrm{Frob}_q)) \equiv \epsilon^{-1}(q)q \pmod{\nu},$$

for all primes $q \nmid N, \nu$.

LEMMA 2.3. *Let E and E' be elliptic curves over $\mathbb{Q}$. Assume that $\overline{\rho}_{E,n} \cong \overline{\rho}_{g,\nu}$ for some newform g, some odd prime n (in $\mathbb{Z}$) and some prime ν lying over n. Let $q \geq 5$ be a prime not dividing the level of g, and assume $q \neq n$. Define*

$$A_{E'}(q,g) = \begin{cases} \mathrm{Norm}(a_q(E') - a_q(g)) & \text{if } \Delta_{E'} \not\equiv 0 \pmod{q}, \\ \mathrm{Norm}((q+1)^2 - a_q(g)^2) & \text{if } \Delta_{E'} \equiv 0 \pmod{q}, \end{cases}$$

where $a_q(E')$ is the trace of Frob_q acting on the Tate module $T_n(E')$. If $E \equiv E' \pmod{q}$ (that is $c_4(E) \equiv c_4(E') \pmod{q}$ and $c_6(E) \equiv c_6(E') \pmod{q}$), then $n \mid A_{E'}(q,g)$. (The quantities c_4, c_6 and Δ are those associated to minimal models of E and E'.)

Proof. This follows easily by comparing traces of Frobenius. ∎

For the Diophantine equation of interest, namely $a^3 + b^{3n} = c^2$, we will also have need of (at a basic level, at least) the theory of $\mathbb{Q}$-curves. We refer the reader to [16] and [5] for standard definitions and results, which we only briefly summarize here.

Recall, a $\mathbb{Q}$-curve defined (resp. defined completely) over a quadratic field $K/\mathbb{Q}$ is an elliptic curve E/K that is isogenous over $\overline{K}$ (resp. over K) to its Galois conjugate. As a result, $\mathrm{End}(\mathrm{Res}_{K/\mathbb{Q}}(E)) = M$ will be an order in a quadratic field. In fact $\mathrm{Res}_{K/\mathbb{Q}}(E)$ will be a GL_2-Abelian variety. Therefore, for a prime π of M lying over n, we can attach a two-dimensional Galois representation $\rho_{E,\beta,\pi}$ with β a splitting map for $c_E \in H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$. A defining property of $\rho_{E,\beta,\pi}$ is that $\rho_{E,\beta,\pi}|_{G_K}$ is projectively isomorphic to the Tate module $T_n(E)$.

For later use, we denote by $\overline{\rho}_{E,\beta,\pi}$ (the semisimplification of) a reduction modulo π of the continuous π-adic Galois representation $\rho_{E,\beta,\pi}$. The arguments of [16, §7] show that $\rho_{E,\beta,\pi}$ has central character ϵ^{-1} where

ϵ is the Dirichlet character associated with a non-trivial Galois character $G_{K/\mathbb{Q}} \to \{\pm 1\}$. The following lemma is the analogue of Lemma 2.3 for $\mathbb{Q}$-curves defined completely over K.

LEMMA 2.4. *Let E and E' be $\mathbb{Q}$-curves defined completely over the quadratic field K. Assume that $\overline{\rho}_{E,\beta,\pi} \cong \overline{\rho}_{g,\nu}$ for some newform g, some primes π and ν lying over an odd prime n (in $\mathbb{Z}$) and some splitting map β. Let $q \geq 5$ be a prime not dividing the level of g, which is unramified in K and assume $q \neq n$. Define*

$$B_{E'}(q,g) = \begin{cases} \mathrm{Norm}(a_q(g) - a_q(E')) & \text{if } q \text{ splits in } K \text{ and } q \nmid \Delta_{E'}, \\ \mathrm{Norm}(a_q(g)^2 - a_{q^2}(E') + 2q) & \text{if } q \text{ is inert in } K \text{ and } q \nmid \Delta_{E'}, \\ \mathrm{Norm}(\epsilon^{-1}(q)(q+1)^2 - a_q(g)^2) & \text{if } q \mid \Delta_{E'}, \end{cases}$$

where $a_{q^i}(E')$ is the trace of Frob_q^i acting on the Tate module $T_n(E')$. If $E \equiv E' \pmod{q}$, then $n \mid B_{E'}(q,g)$.

Proof. This is very similar to [1, Lemma 24], although, since our $\mathbb{Q}$-curve is completely defined over K, we obtain a slightly stronger result in the case when q splits in K and $\Delta_{E'}$ is coprime to q. We will therefore assume that $\Delta_{E'}$ is coprime to q and refer to [1] for the case of bad reduction.

For any Abelian variety A over K, let $V_n(A)$ be the $\mathbb{Q}_n[G_K]$ module given by tensoring the n-adic Tate module of A with $\mathbb{Q}_n$. Since E is completely defined over K, we find that

$$V_n(\mathrm{Res}_{K/\mathbb{Q}}(E)) \cong \mathrm{End}(\mathrm{Res}_{K/\mathbb{Q}}(E)) \otimes V_n(E)$$

as $\mathrm{End}(\mathrm{Res}_{K/\mathbb{Q}}(E)) \otimes \mathbb{Q}_n[G_K]$ modules (see [5, Proposition 12]). Note that since E is completely defined over K, the action of G_K only acts on the Tate module part. Therefore, for $\sigma \in G_K$, we have $\rho_{E,\beta,\pi}(\sigma) \cong \rho_{E,n}(\sigma)$.

Now, let q be a prime of good reduction. Fix an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}_q}$, and assume that q splits in K. We therefore have $K \subset \mathbb{Q}_q$. Let Frob_q be a Frobenius element in $G_{\mathbb{Q}_q}$, which we can view as an element in G_K. We thus have

$$\mathrm{tr}(\rho_{E,\beta,\pi}(\mathrm{Frob}_q)) = \mathrm{tr}(\rho_{E,n}(\mathrm{Frob}_q)) = a_q(E).$$

Since $a_q(E) = a_q(E')$ when $E \equiv E' \pmod{q}$, from the fact that $\overline{\rho}_{E,\beta,\pi} \cong \overline{\rho}_{g,\nu}$, we may conclude that $n \mid N(a_q(g) - a_q(E'))$.

Similarly, if we assume that q does not split in K, then by choosing Frob_q a Frobenius element in $G_{\mathbb{Q}_q}$, we have $\mathrm{Frob}_q^2 \in G_K$, and so

$$\mathrm{tr}(\rho_{E,n}(\mathrm{Frob}_q^2)) = \mathrm{tr}(\rho_{E,\beta,\pi}(\mathrm{Frob}_q^2)) = \mathrm{tr}(\rho_{E,\beta,\pi}(\mathrm{Frob}_q)^2).$$

Letting $\rho_{E,\beta,\pi}(\mathrm{Frob}_q) = A$, it follows that $A^2 = \mathrm{tr}(A)A - \det(A)I$, and hence $\mathrm{tr}(A^2) = \mathrm{tr}(A)^2 - 2\det(A)$. Note that $\det(A) = \epsilon(q)q$ and that $\epsilon(q) = -1$ since q does not split in K. Therefore $\mathrm{tr}(\rho_{E,\beta,\pi}(\mathrm{Frob}_q))^2 = a_{q^2}(E) - 2q$.

Again, $a_{q^2}(E) = a_{q^2}(E')$ when $E \equiv E' \pmod{q}$, and since $\overline{\rho}_{E,\beta,\pi} \cong \overline{\rho}_{g,\nu}$, we conclude that $n \mid N(a_q(g)^2 - a_{q^2}(E) + 2q)$. ∎

We note that the above two lemmata will be applied with the curves E and E' as Frey–Hellegouarch curves $E_{s,t}$ attached to a particular solution $(s,t,b) \in \mathbb{Z}^3$. As a result, we usually write $A_{s,t}(q,g)$ (resp. $B_{s,t}(q,g)$) for $A_{E_{s,t}}(q,g)$ (resp. $B_{E_{s,t}}(q,g)$), when there is no chance of confusion. Also, note that if all possible choices for $(u,v) \pmod{q}$ lead to either $A_{u,v}(q,g)$ or $B_{u,v}(q,g)$ being non-zero, we necessarily obtain an upper bound on n.

3. The equation $a^3+b^{3n}=c^2$. Let us assume that $a^3+b^{3n}=c^2$ for coprime integers a, b and c and prime $n > 7$. When $3 \nmid c$, using parametrization (2.1), we find that either

$$b^n = -4t(s-t)(s^2+ts+t^2),$$

or

$$b^n = s(s+2t)(s^2-2ts+4t^2),$$

depending on the parity of b, for coprime integers s and t, with s odd and $s \not\equiv t \pmod 3$. We can thus find integers A, B and C for which one of

$$t = 2^{n-2}A^n, \quad s-t = B^n \quad \text{and} \quad s^2+ts+t^2 = C^n,$$
$$t = A^n, \quad s-t = 2^{n-2}B^n \quad \text{and} \quad s^2+ts+t^2 = C^n,$$

or

$$s = A^n, \quad s+2t = B^n \quad \text{and} \quad s^2-2ts+4t^2 = C^n$$

holds. In the first two cases, the identity $4(s^2+ts+t^2)-3t^2 = (t+2s)^2$ leads via [3, Theorems 1.2 and 1.5] to ternary equations of signature $(n,n,2)$ with no non-trivial solutions. In the third case, the fact that $4(s^2-2ts+4t^2) - 3s^2 = (s-4t)^2$ leads, again via [3, Theorem 1.2], to a like conclusion.

For the remainder of this section we may thus suppose that $3 \mid c$, so we are led to consider parameterizations (2.2) and (2.3). Furthermore, since $v_2(2(s^4+2ts^3+2t^3s+t^4)) = 1$ when $s \not\equiv t \pmod 2$, it follows that $b^n \neq 2(s^4+2ts^3+2t^3s+t^4)$. It remains, therefore, to treat the following Diophantine equations:

$$b^n = s^4 - 4ts^3 - 6t^2s^2 - 4t^3s + t^4, \quad s \not\equiv t \pmod 2,\ s \not\equiv t \pmod 3, \tag{3.1}$$

$$b^n = -3s^4 + 6t^2s^2 + t^4, \quad t \not\equiv 0 \pmod 3,\ s \not\equiv t \pmod 2, \tag{3.2}$$

$$b^n = 3s^4 + 6t^2s^2 - t^4, \quad t \not\equiv 0 \pmod 3,\ s \not\equiv t \pmod 2. \tag{3.3}$$

The MAGMA [4] and SAGE [19] programs used to perform various computations cited in the remainder of the paper are posted at

people.math.sfu.ca/~ichen/gflt-3-3n-2.

The specific program used in each paragraph below is indicated inside a box.

We will assume throughout that $|b| > 1$. Indeed, if $b = \pm 1$, we have $a^3 \pm 1 = c^2$, and so either $abc = 0$ or $(a, |b|, |c|) = (2, 1, 3)$. Since $3 \mid c$, it follows that $\gcd(b, 6) = 1$. Supposing $|b| > 1$, since b is odd, it is necessarily divisible by an odd prime. Note that (3.1) corresponds to the case when c is odd, while equations (3.2) and (3.3) coincide with c being even. We will treat these two cases separately. From now on, we assume that $n \geq 11$ and $n \neq 13$.

As a last observation before we proceed, we note that in order to carry out our desired application of the "modular method" for $\mathbb{Q}$-curves, we need to rule out the case that the corresponding curves have complex multiplication. In the situation at hand, the fact that all Frey–Hellegouarch curves used in this paper lack complex multiplication is immediate from considering their corresponding j-invariants or conductors, using the fact that b is divisible by a prime ≥ 5 (whence each curve necessarily has a prime of multiplicative reduction).

3.1. c **odd.** Assume that c is odd. In this case, we use two Frey–Hellegouarch curves that we denote by E_1 and E_2. These are constructed by considering the factorization of $b^n = x(s,t) = s^4 - 4s^3t - 6s^2t^2 - 4st^3 + t^4$ from (2.2), so that they are defined over an extension of degree ≤ 2 and have discriminant which is essentially an nth power.

For $i \in \{1, 2\}$ we give a quick reference below for the equation defining E_i, the conductor N_{E_i}, the (not necessarily minimal) discriminant for the model Δ_{E_i} and the conductor N_{ρ_i} for the associated Galois representation ρ_i.

i	E_i	N_{E_i}	Δ_{E_i}	N_{ρ_i}
1	(3.4)	(3.5)	(3.6)	(3.7)
2	(3.8)	(3.11)	(3.12)	(3.13)

From (2.2) we have

$$a = a(s,t) = 2(s^4 + 2ts^3 + 2t^3s + t^4)$$

and

$$c = c(s,t) = 3(s-t)(s+t)(s^4 + 2s^3t + 6s^2t^2 + 2st^3 + t^4).$$

Consider first the Frey–Hellegouarch elliptic curve

$$E_1(s,t) \;:\; y^2 = x^3 - 3a(s,t)x - 2c(s,t). \tag{3.4}$$

We can calculate the conductor of E_1.

LEMMA 3.1. *The conductor of $E_1(s,t)$ is given by*

$$2^6 \cdot 3^\delta \prod_{q \mid b,\, q \neq 2,3} q, \tag{3.5}$$

where $\delta \in \{2,3\}$.

Proof. Note that

$$\Delta_{E_1} = -1728\, b(s,t)^{3n}. \tag{3.6}$$

Therefore, all primes dividing b are primes of bad reduction. Since a and c are coprime, the elliptic curve $E_1(s,t)$ has semistable reduction away from 2 and 3. To calculate the conductor at 2 and 3, we can of course appeal to Tate's algorithm directly. Alternatively, note that $\Delta_{E_1} = -1728\, b(s,t)^{3n}$ whereby, since $\gcd(b,6) = 1$, we have $v_2(\Delta_{E_1}) = 6$ and $v_3(\Delta_{E_1}) = 3$. Using Tate's algorithm (cf. [18], for instance applying Lemma 2.1 with $k = 1$), we can find all possible values of the conductor at $p \in \{2,3\}$ by calculating the conductor and the Kodaira symbol of specific elliptic curves $E(s,t)$ for all possible values of s and t modulo p^6, say, using MAGMA or SAGE. ∎

Since we are assuming that an odd prime divides b, using Theorem 2.2 it follows that $\overline{\rho}_{E_1,n}$ is irreducible when $n \geq 11$ and $n \neq 13$. By modularity of E_1 and standard level lowering arguments using [15], we may thus conclude that $\overline{\rho}_{E_1,n} \simeq \overline{\rho}_{g_1,n}$ for some newform

$$g_1 \in S_2(\Gamma_0(576))^{\text{new}} \cup S_2(\Gamma_0(1728))^{\text{new}}. \tag{3.7}$$

We also note that we can rewrite (3.1) as

$$b^n = (s-t)^4 - 12(st)^2,$$

to which we can attach the Frey–Hellegouarch $\mathbb{Q}$-curve

$$E_2(s,t)\ :\ y^2 = x^3 + 2(\sqrt{3}-1)(s-t)x^2 + (2-\sqrt{3})((s-t)^2 - 2\sqrt{3}\, st)x. \tag{3.8}$$

Let $\rho \in G_{\mathbb{Q}}$ be such that ρ is non-trivial on $K = \mathbb{Q}(\sqrt{3})$. The 2-isogeny map $\mu_\rho : {}^\rho E_2(s,t) \to E_2(s,t)$ is given by $\mu_\rho(x,y) = (\mu_1, \mu_2)$, where

$$\begin{aligned} \mu_1 &= \frac{-\sqrt{3}+2}{2}x + (-\sqrt{3}+1)(s-t) + \frac{(s-t)^2 + 2\sqrt{3}\, st}{2x}, \\ \mu_2 &= \frac{-3\sqrt{3}+5}{4}y + \left(\frac{\sqrt{3}-1}{4}(s-t)^2 + \frac{-\sqrt{3}+3}{4}\right)\frac{y}{x^2}. \end{aligned} \tag{3.9}$$

It can be verified that $\mu_\rho \circ {}^\rho\mu_\rho : E_2 \to E_2$ has degree 4, corresponding to $[-2]$. Since E_2 is a $\mathbb{Q}$-curve completely defined over a quadratic field, the results of [16, §7] can be applied to give an explicit splitting map β for $c_{E_2} \in H^2(G_{\mathbb{Q}}, \mathbb{Q}^*)$; it factors through $G_{K/\mathbb{Q}}$, and is defined by $\beta(1) = 1$ and $\beta(\rho) = \sqrt{-2}$.

If σ_q is a Frobenius element at a prime $q \neq 2, 3$, then

$$\beta(\sigma_q) = \begin{cases} 1 & q \equiv \pm 1 \pmod{12}, \\ \sqrt{-2} & q \equiv \pm 5 \pmod{12}. \end{cases} \tag{3.10}$$

Consider the number field $M_\beta = \mathbb{Q}(\beta(\sigma)) = \mathbb{Q}(\sqrt{-2})$. Let $\rho_{E_2,\beta,\pi}$ be the Galois representation attached to E_2 with respect to β and a choice of prime π of M_β above n.

The arguments of [16, §7] show that the character of $\rho_{E_2,\beta,\pi}$ is ϵ^{-1} where ϵ is the Dirichlet character associated with the non-trivial Galois character $G_{K/\mathbb{Q}} \to \{\pm 1\}$. More precisely, $\epsilon = \epsilon_3\epsilon_4$ where ϵ_m is the non-trivial character of $(\mathbb{Z}/m\mathbb{Z})^\times$. Furthermore, $\rho_{E_2,\beta,\pi}$ may be described as the Galois representation obtained on the π-adic Tate module of $\mathrm{Res}_{K/\mathbb{Q}} E_2$ whose endomorphism algebra is $\mathbb{Z}[\sqrt{-2}]$.

Let $\mathfrak{q}_2$ and $\mathfrak{q}_3$ be the primes of $K = \mathbb{Q}(\sqrt{3})$ lying above 2 and 3, respectively.

LEMMA 3.2. *The conductor of E_2 over K is given by*

$$\mathfrak{q}_2^{12} \prod_{\mathfrak{q} \mid b,\, \mathfrak{q} \nmid 2,3} \mathfrak{q}. \tag{3.11}$$

Proof. Since we assume that s and t are coprime with $\gcd(s-t, 6) = 1$, if $\mathfrak{q} \mid 2(\sqrt{3}-1)(s-t)$ and $\mathfrak{q} \mid (2-\sqrt{3})((s-t)^2 - 2\sqrt{3}st)$, then the characteristic of the residue field at $\mathfrak{q}$ is either 2 or 3. Therefore E has semistable reduction away from 2 and 3. Furthermore, since

$$\Delta_{E_2} = (1664 - 960\sqrt{3})((s-t)^2 + 2\sqrt{3}\,st)((s-t)^2 - 2\sqrt{3}\,st)^2 \tag{3.12}$$

and $3 \nmid s - t$, it follows that $\mathfrak{q}_3 \nmid \Delta_{E_2}$, and hence E_2 has good reduction at $\mathfrak{q}_3$. It remains to calculate the conductor of E_2 at $\mathfrak{q}_2$. Let $E' = E_2(1, 0)$. Using MAGMA or SAGE, we can check that the conductor of E' is $\mathfrak{q}_2^{12}$ with Kodaira Symbol II. Note that $v_{\mathfrak{q}_2}(\Delta_{E_2}) = v_{\mathfrak{q}_2}(\Delta_{E'}) = 12$ (recall that we have assumed $s - t$ to be odd). Furthermore, we have

$$a_1 - a_1' = a_3 - a_3' = a_6 - a_6' = 0$$

and

$$v_{\mathfrak{q}_2}(a_2 - a_2') \geq 5, \qquad v_{\mathfrak{q}_2}(a_4 - a_4') \geq 4,$$

since $s-t$ is odd and st is even. Using Tate's algorithm (cf. [18], for instance applying Lemma 2.1 with $k = 1$), therefore implies the desired result. ∎

COROLLARY 3.3. *The conductor of $\rho_{E_2,\beta,\pi}$ is given by*

$$N = 2^8 \cdot 3 \cdot \prod_{q \mid b,\, q \neq 2,3} q. \tag{3.13}$$

Proof. This follows from [13, Lemma on p. 178] and the fact discussed in [13] that the ℓ-adic representation of a restriction of scalars is the induced representation of the ℓ-adic representation of the given abelian variety. ∎

Using the arguments of [7], if $\overline{\rho}_{E_2,\beta,\pi}$ is reducible, it follows that $b = \pm 1$, contrary to our assumptions. Therefore, by [8, 9, 10], $\overline{\rho}_{E_2,\beta,\pi}$ is modular. By standard level lowering arguments (cf. for instance [5]), we thus obtain that $\overline{\rho}_{E_2,\beta,\pi} \cong \overline{\rho}_{g_2,\pi}$ for some newform $g_2 \in S_2(\Gamma_0(768), \epsilon^{-1})$. By direct MAGMA computation, we find that there are precisely ten Galois conjugacy classes of newforms in $S_2(\Gamma_0(768), \epsilon^{-1})$ which we denote by $F_1, \ldots, F_{10}$. Here, as well as in the remainder of this paper, the numbering we use for our modular forms is given by the order in our data files.

We now apply the multi-Frey method, i.e. for a fixed pair of forms (g_1, g_2), we run through the parameters (s, t) modulo an auxiliary prime $q \neq 2, 3, n$; for each (s, t), we extract the information imposed by the simultaneous conditions $\overline{\rho}_{E_2,\beta,\pi} \cong \overline{\rho}_{g_2,\nu}$ and $\overline{\rho}_{E_1,n} \cong \overline{\rho}_{g_1,\nu}$ using Lemmas 2.3 and 2.4. We refer the reader to Section 4 for an explicit treatment when $g_2 = F_1$.

In the case at hand, the results of the multi-Frey computation, denoted multi-frey-1.txt, using (E_1, E_2) are that all pairs (g_1, g_2) are eliminated for suitably large n, except when

- $g_2 \in \{F_1, F_2, F_4, F_5\}$ and g_1 is form 6 of level 576,
- $g_2 \in \{F_3, F_6\}$ and g_1 is form 18 or 27 of level 1728.

In each case where we were able to remove a pair (g_1, g_2) from consideration, this was accomplished through use of $q \in \{5, 7, 11\}$ with resulting conclusion that $n \in \{2, 3, 5, 7, 11\}$. Each eliminated pair required only a single auxiliary prime q.

The four forms F_1, F_2, F_4 and F_5 arise from the "near" solutions corresponding to the values $(s, t) = (\pm 1, \mp 1)$ and $(s, t) = (-1)^\delta (-1 \pm \sqrt{2}, 1 \pm \sqrt{2})$, where $\delta \in \{0, 1\}$. For these values of s and t, we have $s - t = \pm 2$ and $st = \pm 1$, with Frey–Hellegouarch curves

$$\begin{aligned} C &: y^2 = x^3 \pm 4(\sqrt{3} - 1)x^2 + (2 - \sqrt{3})(4 - 2\sqrt{3})x, \\ C' &: y^2 = x^3 \pm 4(\sqrt{3} - 1)x^2 + (2 - \sqrt{3})(4 + 2\sqrt{3})x. \end{aligned}$$

Each of the forms F_1, F_2, F_4 and F_5 has field of coefficients $\mathbb{Q}(\sqrt{-2})$ and satisfies all of the required congruence conditions imposed by $\overline{\rho}_{E_2,\beta,\pi} \cong \overline{\rho}_{g,\nu}$. Fortunately, we are able to employ an image of inertia argument to rule out these cases.

LEMMA 3.4. *Let $L = \mathbb{Q}(\theta)$ (respectively $L' = \mathbb{Q}(\theta')$), where θ (respectively θ') is a root in $\overline{\mathbb{Q}}_2$ of*

$$x^{16} - 20x^{14} + 88x^{12} - 64x^{10} - 109x^8 - 160x^6 - 248x^4 - 20x^2 + 1$$

(respectively $x^{16} + 4x^{14} - 32x^{12} - 16x^{10} + 83x^8 + 80x^6 + 16x^4 + 4x^2 + 1$).

Fix an embedding of $\mathbb{Q}(\sqrt{3})$ *into* L (*respectively* L'). *Then the elliptic curve* C (*respectively* C') *has good reduction over* L (*respectively* L') *at the unique prime* $\mathfrak{p}$ (*respectively* $\mathfrak{p}'$) *lying above* 2.

The Galois representation $\overline{\rho}_{g,\nu}$, *when restricted to* $I_{L_\mathfrak{p}}$ (*respectively* $I_{L'_{\mathfrak{p}'}}$) *for* g *in the conjugacy class* F_1 *or* F_4 (*respectively* F_2 *or* F_5), *is unramified.*

Proof. We first remark that the fields L and L' were computed using the three torsion points of C and C', respectively (see [11] for explicit results on the semistable reduction of elliptic curves). The desired good reduction of C at $\mathfrak{p}$ and C' at $\mathfrak{p}'$ is easily verified with either SAGE or MAGMA, as we do in goodred1.txt.

The second statement follows from the fact that C gives rise to F_1, F_4 and C' to F_2, F_5. This claim may be justified by point counting; see ellcurve.txt for details. ∎

We now show that when s and t are of opposite parity, then $E_2(s,t)$ does not have good reduction at $L_\mathfrak{p}$ and $L'_{\mathfrak{p}'}$. Note that since s and t have opposite parity, $E_2(s,t)$ and $E_2(2,1)$ over $L_\mathfrak{p}$ (respectively $L'_{\mathfrak{p}'}$) satisfy all the conditions required to apply Lemma 2.1. In particular,

$$v_\mathfrak{p}(\Delta_{E_2(s,t)}) = v_\mathfrak{p}(\Delta_{E_2(2,1)}) = v_\mathfrak{p}(1664 - 960\sqrt{3}) = 48 = 4 \cdot 12$$

and

$$v_{\mathfrak{p}'}(\Delta_{E_2(s,t)}) = v_{\mathfrak{p}'}(\Delta_{E_2(2,1)}) = 48 = 4 \cdot 12.$$

Since $s - t$ is odd, we have

$$v_\mathfrak{p}(a_2 - a'_2) = v_{\mathfrak{p}'}(a_2 - a'_2) \geq 20 \geq 4 \cdot 2, \quad v_\mathfrak{p}(a_4 - a'_4) = v_{\mathfrak{p}'}(a_4 - a'_4) \geq 16 \geq 4 \cdot 4,$$

as desired.

Furthermore, $E_2(2,1)$ does not have good reduction over $L_\mathfrak{p}$ (respectively $L'_{\mathfrak{p}'}$) as one can check with SAGE or MAGMA. We conclude, therefore, that $E_2(s,t)$ has bad reduction over $L_\mathfrak{p}$ (respectively $L'_{\mathfrak{p}'}$). In fact we find that $E_2(s,t)$ has Kodaira symbol I_0^*, whereby $\rho_{E_2(s,t),\beta,\pi}$ will be non-trivial when restricted to $I_{L_\mathfrak{p}}$ and $I_{L'_\mathfrak{p}}$. Since the Kodaira symbol is I_0^*, over a quadratic extension of L (respectively L'), $E_2(s,t)$ acquires good reduction, which implies that $\rho_{E_2(s,t),\beta,\pi}(I_{L_\mathfrak{p}})$ is a group of order 2. Since π has characteristic larger than 2, it follows that $\overline{\rho}_{E_2(s,t),\beta,\pi}$ is non-trivial when restricted to $I_{L_\mathfrak{p}}$ (similarly, when restricted to $I_{L'_{\mathfrak{p}'}}$). This rules out the modular forms F_1 and F_4 (respectively F_2 and F_5).

The forms F_3 and F_6 have complex multiplication by $\mathbb{Q}(\sqrt{-2})$, so if $\overline{\rho}_{E_2,\beta,\pi} \cong \overline{\rho}_{g,\pi}$ for $g \in \{F_3, F_6\}$, then the projectivized image of $\overline{\rho}_{E_2,\beta,\pi}$ will be the normalizer of a split (respectively non-split) Cartan subgroup when $n \equiv 1, 3 \pmod 8$ (respectively $n \equiv 5, 7 \pmod 8$). For the split case, we can use Ellenberg's result [7, Proposition 3.4] to show that the projectivized

image of $\overline{\rho}_{E_2,\beta,\pi}$ is not in the split Cartan subgroup when $|b| > 1$. Therefore we have proven Proposition 1.2.

REMARK 3.5. We are unaware of a method to deal with the case of a non-split Cartan image (the arguments of Mazur for the relevant non-split Cartan modular curves fail, since all non-zero modular abelian variety quotients will have odd rank; see [5]). The general non-split Cartan case will likely require substantial new developments. As a result, extending Theorem 1.1 to include other values of n modulo 8 remains problematic.

3.2. c **even.** Now assume that c is even. In this case, we are led to consider three Frey–Hellegouarch curves that we denote by E_1, E_2 and E_3. These are constructed by considering the factorization of $b^n = y(s,t) = 3s^4 + 6t^2s^2 - t^4$ from (2.3), so that they are defined over an extension of degree ≤ 2 and have discriminant which is essentially an nth power.

For $i \in \{1,2,3\}$ we give a quick reference below for the equation defining E_i and the conductor N_{ρ_i} for its associated Galois representation ρ_i.

i	E_i	N_{ρ_i}
1	(3.14)	(3.16)
2	(3.18)	(3.20)
3	(3.22)	(3.23)

From (2.3), we have

$$a(s,t) = \begin{cases} 3s^4 + 6t^2s^2 - t^4 & \text{for case (3.2)}, \\ -3s^4 + 6t^2s^2 + t^4 & \text{for case (3.3)}, \end{cases}$$

and $c(s,t) = 6st(3s^4 + t^4)$ in either case. Let

$$E_1(s,t) \ : \ \begin{cases} y^2 = x^3 - 3a(s,t)x - 2c(s,t) & \text{for case (3.2)}, \\ y^2 = x^3 - 12a(s,t)x - 16c(s,t) & \text{for case (3.3)}. \end{cases} \tag{3.14}$$

LEMMA 3.6. *The conductor of* $E_1(s,t)$ *is*

$$2^5 \cdot 3^\delta \prod_{q|b,\, q\neq 2,3} q, \tag{3.15}$$

where $\delta \in \{2,3\}$.

Proof. The computation is similar to that of Lemma 3.1. ∎

As before, it follows that $\overline{\rho}_{E_1,n}$ is irreducible and hence, by modularity and standard level lowering, we conclude that $\overline{\rho}_{E_1,n} \simeq \overline{\rho}_{g_1,\nu}$ for some newform

$$g_1 \in S_2(\Gamma_0(576))^{\text{new}} \cup S_2(\Gamma_0(1728))^{\text{new}}. \tag{3.16}$$

We can also rewrite (3.2) and (3.3) (replacing b by $-b$ if necessary) as

$$b^n = 3(s^2 \pm t^2)^2 - 4t^4. \tag{3.17}$$

To these equations we can attach the Frey–Hellegouarch $\mathbb{Q}$-curve $E_2 = E_2(s,t)$ given by

$$E_2(s,t)\ :\ y^2 = x^3 + 4(\sqrt{3}-1)tx^2 - (\sqrt{3}-1)^2(\sqrt{3}\,s^2 + (-2\pm\sqrt{3})t^2)x, \tag{3.18}$$

where $3 \nmid t$ and $s \not\equiv t \pmod 2$. Note that $E_2(s,t)$ is isomorphic to one of the $\mathbb{Q}$-curves $E_2(S,T)$ defined in (3.8), with $s-t$ replaced by $2t$ and st replaced by $s^2 \pm t^2$. Therefore, as before, $\rho_{E_2,\beta,\pi}$ arises from the Galois representation on the π-adic Tate module $\mathrm{Res}_{K/\mathbb{Q}}\, E_2$, whose endomorphism algebra is $\mathbb{Z}[\sqrt{-2}]$. As previously, it is a routine matter to compute the conductor of E_2.

LEMMA 3.7. *Suppose $3 \nmid b$ and $s \not\equiv t \pmod 2$. Then the conductor of E_2 over K is given by*

$$\mathfrak{q}_2^{12} \prod_{\mathfrak{q}\mid b,\ \mathfrak{q}\nmid 2,3} \mathfrak{q}. \tag{3.19}$$

Proof. The computation is similar to that of Lemma 3.2. ∎

COROLLARY 3.8. *Suppose $3 \nmid b$ and $s \not\equiv t \pmod 2$. Then the conductor of $\rho_{E_2,\beta,\pi}$ is given by*

$$2^8 \cdot 3 \cdot \prod_{q\mid b,\ q\neq 2,3} q. \tag{3.20}$$

Proof. As for Corollary 3.3. ∎

When $n > 7$ and $n \neq 13$ is prime, modularity and standard level lowering arguments thus imply that $\overline{\rho}_{E_2,\beta,\pi} \simeq \overline{\rho}_{g_2,\pi}$ for some newform g_2 in $S_2(\Gamma_0(768), \varepsilon^{-1})$. Recall that there are ten conjugacy classes of newforms in $S_2(\Gamma_0(768), \varepsilon^{-1})$, which we have labelled as $F_1, \ldots, F_{10}$.

The result of the multi-Frey computation using (E_1, E_2) is that all pairs (g_1, g_2) are eliminated except when:

CASE (3.2) multi-frey-3.txt:

- $g_2 \in \{F_1, F_2, F_4, F_5\}$ and g_1 is form 1 of level 288 (corresponding to $(s,t) = (0, \pm 1)$ and twists),
- $g_2 \in \{F_3, F_6\}$ and g_1 is form 2 or 6 of level 864 (corresponding to $(s,t) = (1, \pm 1)$),

CASE (3.3) multi-frey-2.txt:

- $g_2 \in \{F_1, F_2, F_4, F_5\}$ and g_1 is form 1 of level 288 (corresponding to $(s,t) = (0, \pm 1)$ and twists).

The primes q used were $5, 7$ and 11, leading to the conclusion that n is in $\{2, 3, 5, 7, 11\}$. All eliminated pairs required the use of only one auxiliary prime q.

Among the remaining forms, we note that form 1 of level 288 has complex multiplication by $\mathbb{Q}(\sqrt{-4})$, while forms F_3 and F_6 have complex multiplication by $\mathbb{Q}(\sqrt{-8})$. If $n \equiv 1,3 \pmod 8$ and $g_2 = F_3$ or F_6, this therefore forces $\rho_{E_2,\beta,\pi}$ to have image in a split Cartan subgroup, contradicting Ellenberg's result [7] if $n > 7$, $n \neq 13$, is prime. If $n \equiv 1,5 \pmod 8$ and g_1 is form 1 of level 288, necessarily $\rho_{E_1,n}$ has image in a split Cartan subgroup, contradicting Momose's result [14], provided $n > 7$, $n \neq 13$, is prime.

In fact, in case (3.2) we can do somewhat better through careful argument. First note that we can rewrite this equation as

$$b^n = (t^2 + 3s^2)^2 - 12s^4. \tag{3.21}$$

As in previous situations, there are other Frey–Hellegouarch $\mathbb{Q}$-curves we can attach to solutions of (3.21), including

$$E_3(s,t) \ : \ y^2 = x^3 + 12(\sqrt{3}-1)sx^2 + 3\sqrt{3}(\sqrt{3}-1)^2(t^2 + (2\sqrt{3} \pm 3)s^2)x. \tag{3.22}$$

As we did for E_2, we can check that E_3 is in fact a $\mathbb{Q}$-curve, leading to a Galois representation $\overline{\rho}_{E_3,\beta,\pi}$. When $n > 7$, $n \neq 13$, is prime, arguing as previously, modularity and level lowering imply that $\overline{\rho}_{E_3,\beta,\pi} \simeq \overline{\rho}_{g_3,\nu}$ for some newform

$$g_3 \in S_2(\Gamma_0(2304), \varepsilon^{-1}). \tag{3.23}$$

Using MAGMA, we find that there are ten conjugacy classes of newforms in $S_2(\Gamma_0(2304), \varepsilon^{-1})$, which we denote by $G_1, \ldots, G_{10}$. We will now appeal to the Frey–Hellegouarch curve E_3 to eliminate the possibility of forms F_3, F_6 giving rise to solutions to (3.2), provided $n \equiv 1 \pmod 4$ and $n \geq 17$ (note that we have already demonstrated this result if $n \equiv 1 \pmod 8$). This will enable us to reach a like conclusion in each of cases (3.2) and (3.3). To do this, assume we are in case (3.2) with $g_3 \in \{F_3, F_6\}$ and g_1 either form 2 or 6 of level 864. In this case, using the multi-Frey method multi-frey-4.txt, we find that $\overline{\rho}_{E_3,\beta,\pi} \simeq \overline{\rho}_{g_3,\nu}$ with $g_3 \in \{G_5, G_6, G_7, G_8\}$. We can check that G_5, G_6, G_7, G_8 correspond to elliptic curves $E_3(1, \pm 1)$. Now, applying an image of inertia argument at 2, simultaneously to $\overline{\rho}_{E_3,\beta,\pi}$ and $\overline{\rho}_{E_2,\beta,\pi}$, we obtain the desired result. In particular, we have

LEMMA 3.9. *Let $L_2 = \mathbb{Q}_2(\theta_2)$ (respectively $L_3 = \mathbb{Q}_2(\theta_3)$) where θ_2 (respectively θ_3) is a root of*

$$x^{16} + 4x^{14} + 8x^{12} + 24x^{10} + 47x^8 + 24x^6 + 8x^4 + 4x^2 + 1$$

(respectively $x^{16} + 4x^{14} + 4x^{12} - 96x^{10} - 165x^8 + 240x^6 - 108x^4 + 36x^2 + 9$).

Fix an embedding of $\mathbb{Q}(\sqrt{3})$ into L_2 (respectively L_3).

(1) *The Galois representation $\overline{\rho}_{g_2,\nu}$ for g_2 in the conjugacy class of F_3 or F_6 is trivial when restricted to I_{L_2}.*

(2) *The Galois representation* $\overline{\rho}_{g_3,\pi}$ *for* g_3 *in the conjugacy class of* G_5, G_6, G_7, *or* G_8 *is trivial when restricted to* I_{L_3}.
(3) *Let* $E \in \{E_2(\pm 1, 2), E_2(0, \pm 1), E_2(2, \pm 1)\}$. *Then* $\overline{\rho}_{E,\beta,\pi}$ *restricted to* I_{L_2} *is non-trivial.*
(4) *Let* $E \in \{E_3(\pm 1, 0), E_3(0, \pm 1), E_3(2, \pm 1)\}$. *Then* $\overline{\rho}_{E,\beta,\pi}$ *restricted to* I_{L_3} *is non-trivial.*
(5) *Let* $E = E_2(s,t)$ *with* $s \not\equiv t \pmod 2$ *and* $4 \nmid t$. *Then* $\overline{\rho}_{E,\beta,\pi}$ *restricted to* I_{L_2} *is non-trivial.*
(6) *Let* $E = E_3(s,t)$ *with* $s \not\equiv t \pmod 2$ *and* $t \not\equiv 2 \pmod 4$. *Then* $\overline{\rho}_{E,\beta,\pi}$ *restricted to* I_{L_3} *is non-trivial.*

Proof. We first note that F_3 and F_6 arise from the Frey–Hellegouarch curves $E_2(1, \pm 1)$, and G_5, G_6, G_7 and G_8 arise from the Frey–Hellegouarch curves $E_3(1, \pm 1)$ (again, this is easily verified via point counting). Using either SAGE or MAGMA, see e.g. goodred2.txt, we find that both the curves $E_2(1, \pm 1)/L_2$ and $E_3(1, \pm 1)/L_3$ have good reduction. Similarly, each of $E_2(\pm 1, 2)/L_2$, $E_2(0, \pm 1)/L_2$ and $E_2(2, \pm 1)/L_2$ have bad additive reduction, with Kodaira symbols II^*, I_0^* and I_0^*, respectively, and $E_3(\pm 1, 0)/L_3$, $E_3(0, \pm 1)/L_3$ and $E_3(2, \pm 1)/L_3$ have bad additive reduction, with Kodaira symbols II^*, I_0^* and I_0^*, respectively. Therefore, we have the first four claims of the lemma.

To prove the last two claims, note that if s and t are of different parities and $4 \nmid t$, then (s,t) will be congruent to one of $(\pm 1, 2)$, $(0, \pm 1)$ and $(2, \pm 1)$ modulo 4. Similarly, if $t \not\equiv 2 \pmod 4$, then (s,t) will be congruent to one of $(\pm 1, 0)$, $(0, \pm 1)$ and $(2, \pm 1)$ modulo 4. Let v be the valuation on L_i. Notice that $v(\Delta_{E_i(s,t)}) = 72 = 12 \cdot 6$ when s and t are of different parity (for $i = 2$ or 3). Finally, if $E = E_i(s,t)$ and $E' = E_i(s',t')$ with $s \equiv s' \pmod 4$ and $t \equiv t' \pmod 4$, then $v(a_2 - a_2') \geq 32 \geq 2 \cdot 6$ and $v(a_4 - a_4') \geq 24 \geq 4 \cdot 6$. Therefore, applying Lemma 2.1, we conclude that $E_i(s,t)$ has reduction type II^* or I_0^*, assuming that s and t are of different parities and (i,t) is not in $\{(3, 4k), (4, 4k+2)\}$. More importantly, $E = E_i(s,t)$ has bad reduction in either case, which proves the final two claims. ∎

We are now ready to eliminate the second case in (3.2) for $n \equiv 5 \pmod 8$. In particular, if $4 \nmid t$, then by considering $E_2 = E_2(s,t)$ necessarily $\overline{\rho}_{E_2,\beta,\pi} \simeq \overline{\rho}_{g_2,\nu}$ with $g_2 \in \{F_3, F_6\}$. However, $\overline{\rho}_{g_2,\nu}$ has trivial image when restricted to I_{L_2}, while $\overline{\rho}_{E_2,\beta,\pi}$ does not. We may thus assume that $t \not\equiv 2 \pmod 4$. Considering $E_3 = E_3(s,t)$, we find that $\overline{\rho}_{E_3,\beta,\pi}$ has non-trivial image when restricted to I_{L_3}. On the other hand, we know that in this case $\overline{\rho}_{E_3,\beta,\pi} \simeq \overline{\rho}_{g_3,\nu}$ where $g_3 \in \{G_5, G_6, G_7, G_8\}$, and we also know that $\overline{\rho}_{g_3,\nu}$ has trivial image when restricted to I_{L_3}. This proves the desired result; in particular, we have proved Proposition 1.3.

Combining the results for the different parities of c thus yields Theorem 1.1.

4. Explicit example of the multi-Frey method. Here we will show, by an example, how the multi-Frey method rules out particular pairs of (g_1, g_2) in Section 3.1. In particular, let $E_1(s,t)$ and $E_2(s,t)$ be as defined in Section 3.1. Assume that $n \geq 11$ and $n \neq 13$. As demonstrated, we have $\overline{\rho}_{E_1,n} \simeq \overline{\rho}_{g_1,n}$ and $\overline{\rho}_{E_2,\beta,\pi} \simeq \overline{\rho}_{g_2,\pi}$, where

$$g_1 \in S_2(\Gamma_0(576))^{\mathrm{new}} \cup S_2(\Gamma_0(1728))^{\mathrm{new}}, \quad g_2 \in S_2(\Gamma_0(768), \varepsilon^{-1})^{\mathrm{new}}.$$

We will deal with the case where $g_2 = F_1$ and $g_1 \in S_2(\Gamma_0(576))^{\mathrm{new}}$. Using MAGMA, we can compute the q-expansion of g_2 all-768.data:

$$g_2 = q + (\sqrt{-2}+1)q^3 + 2\sqrt{-2}q^5 + 2\sqrt{-2}q^7 + (2\sqrt{-2}-1)q^9 + 2q^{11} + O(q^{12}).$$

For all $(s,t) \in \mathbb{F}_5 \times \mathbb{F}_5 - \{(0,0)\}$, we have $a(s,t)^3 - c(s,t)^2 \neq 0$, whereby E_1 has good reduction at 5. Note this implies that E_2 has good reduction at the prime lying above 5. Checking all possible values for $a_5(E_1(s,t))$, we find that $a_5(E_1(s,t)) \in \{-2, 1, 4\}$. This implies that either g_1 is form 4, 6, 8, or 9 of level 576 all-again-edit.data, or $n \in \{2, 3, 5\}$ (with the latter contradicting our assumption that $n \geq 11$).

If g_1 is form 4, 8, or 9, then we have $a_5(g_1) = -2$. We can check that if $a_5(E_1(s,t)) = -2$, then $st(s-t) \equiv 0 \pmod 5$, or else $n \in \{2, 3\}$ (again, contradicting $n \geq 11$). In this case, $a_{5^2}(E_2(s,t)) \in \{10, -8\}$. This means that $B_{E_2}(5, g_2) \in \{100, 64\}$, contradicting $n \geq 11$.

Thus, we have eliminated all pairs (g_1, g_2) with $g_2 = F_1$ and g_1 in $S_2(\Gamma_0(576))^{\mathrm{new}}$ using the multi-Frey method, except for g_1 being form 6 of level 576.

Acknowledgements. The authors would like to thank the anonymous referee for useful comments which improved the exposition of this article. The third author was supported by a VENI grant from the Netherlands Organisation for Scientific Research (NWO). The first, second and fourth authors were supported by grants from NSERC.

References

[1] M. A. Bennett and I. Chen, *Multi-Frey $\mathbb{Q}$-curves and the Diophantine equation $a^2 + b^6 = c^n$*, Algebra Number Theory 6 (2012), 707–730.

[2] M. A. Bennett, I. Chen, S. R. Dahmen and S. Yazdani, *Generalized Fermat equations: a miscellany*, preprint.

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

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

[5] I. Chen, *On the equation* $a^2 + b^{2p} = c^5$, Acta Arith. 143 (2010), 345–375.
[6] H. Cohen, *Number Theory. Vol. II: Analytic and Modern Tools*, Grad. Texts in Math. 240, Springer, 2007.
[7] J. S. 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.
[8] C. Khare, *Serre's modularity conjecture: The level one case*, Duke Math. J. 134 (2006), 557–589.
[9] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I)*, Invent. Math. 178 (2009), 485–504.
[10] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (II)*, Invent. Math. 178 (2009), 505–586.
[11] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. 69 (1990), 353–385.
[12] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), 129–162.
[13] J. S. Milne, *On the arithmetic of abelian varieties*, Invent. Math. 17 (1972), 177–190.
[14] F. Momose, *Rational points on the modular curves* $X_{\mathrm{split}}(p)$, Compos. Math. 52 (1984), 115–137.
[15] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. 100 (1990), 431–476.
[16] K. A. Ribet, *Abelian varieties over* $\mathbb{Q}$ *and modular forms*, in: Algebra and Topology 1992, Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, 53–79.
[17] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\mathbb{Q}/\mathbb{Q})$, Duke Math. J. 52 (1987), 179–230.
[18] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, 1994.
[19] W. A. Stein et al., *Sage Mathematics Software* (*Version 5.10*), The Sage Development Team, 2013; http://www.sagemath.org.

Michael A. Bennett
Department of Mathematics
University of British Columbia
Vancouver, British Columbia, V6T 1Z2, Canada
E-mail: bennett@math.ubc.ca

Imin Chen
Department of Mathematics
Simon Fraser University
Burnaby, British Columbia, Canada
E-mail: ichen@math.sfu.ca

Sander R. Dahmen
Department of Mathematics
VU University Amsterdam
De Boelelaan 1081a
1081 HV Amsterdam, The Netherlands
E-mail: s.r.dahmen@vu.nl

Soroosh Yazdani
Department of Mathematics and Computer Science
University of Lethbridge
Lethbridge, Alberta, T1K 3M4, Canada
E-mail: soroosh.yazdani@uleth.ca

Received on 8.8.2013
and in revised form on 5.2.2014 (7547)