SUMS OF TWO CUBES AS TWISTED PERFECT POWERS, REVISITED

MICHAEL A. BENNETT, CARMEN BRUNI, AND NUNO FREITAS

ABSTRACT. In this paper, we sharpen earlier work of the first author, Luca and Mulholland [4], showing that the Diophantine equation
$$A^3 + B^3 = q^\alpha C^p, \;\; ABC \neq 0, \;\; \gcd(A, B) = 1,$$
has, for "most" primes q and suitably large prime exponents p, no solutions. We handle a number of (presumably infinite) families where no such conclusion was hitherto known. Through further application of certain *symplectic criteria*, we are able to make some conditional statements about still more values of q; a sample such result is that, for all but $O(\sqrt{x}/\log x)$ primes q up to x, the equation
$$A^3 + B^3 = qC^p.$$
has no solutions in coprime, nonzero integers A, B and C, for a positive proportion of prime exponents p.

1. INTRODUCTION

The problem of classifying perfect powers that are representable as a sum of two coprime integer cubes has a long history. The nonexistence of cubes $C^3 > 1$ with this property, a special case of Fermat's Last Theorem, was essentially proven by Euler. For higher powers, we have a substantial amount of recent work; at the time of writing, this can be summarized in the following theorem.

Theorem 1.1 (Bruin [6], Chen-Siksek [8], Dahmen [10], Freitas [12], Kraus [19])**.** *There are no solutions in relatively prime nonzero integers A, B and C to the equation*

(1.1) $$A^3 + B^3 = C^n$$

with exponent n satisfying one of

$$3 \leq n \leq 10^9, \; n \equiv 2 \pmod 3, \; n \equiv 2, 3 \pmod 5,$$
$$n \equiv 61 \pmod{78}, \; n \equiv 51, 103, 105 \pmod{106}, \; or$$
$$n \equiv 43, 49, 61, 79, 97, 151, 157, 169, 187, 205, 259, 265, 277,$$
$$295, 313, 367, 373, 385, 403, 421, 475, 481, 493, 511, 529,$$
$$583, 601, 619, 637, 691, 697, 709, 727, 745, 799, 805, 817, 835,$$
$$853, 907, 913, 925, 943, 961, 1015, 1021, 1033, 1051, 1069, 1123,$$
$$1129, 1141, 1159, 1177, 1231, 1237, 1249, 1267, 1285 \pmod{1296}.$$

Underlying each of these results is an appeal to a particular Frey-Hellegouarch elliptic curve, defined over $\mathbb{Q}$. Just as in the case of Fermat's Last Theorem, with analogous equation $A^n + B^n = C^n$, this curve corresponds to a particular weight 2, cuspidal newform f. In the latter case, Wiles [27] showed that f necessarily has level 2 (whereby the absence of such newforms implies an immediate contradiction). In the case of equation (1.1), however, one finds a corresponding f at one of levels $18, 36$ or 72. The first two of these are readily handled, but the last is not. The obstruction to completely resolving equation (1.1) is the existence of a particular elliptic curve over $\mathbb{Q}$ with conductor 72 which, on some level, "mimics" a solution to (1.1) (the curve in question is labelled $72A1$ in Cremona's tables [9])

In an earlier paper [4], the first author, joint with Luca and Mulholland, considered a modification of equation (1.1), where the right-hand-side is replaced by a "twisted" version of the shape $q^\alpha C^p$, for q prime (the replacement of the exponent n with a prime one p is without loss of generality). The question the authors of [4] wished to answer was whether or not a similar obstruction exists in this new situation. Here and henceforth, let us assume that we have a proper, nontrivial solution (a, b, c) of the equation

$$(1.2) \qquad\qquad A^3 + B^3 = q^\alpha C^p,$$

i.e. a solution with A, B and C nonzero, coprime integers and α a positive integer. Write S for the set of primes $q \geq 5$ for which there exists an elliptic curve $E/\mathbb{Q}$ with conductor $N(E) \in \{18q, 36q, 72q\}$ and at least one nontrivial rational 2-torsion point. The two main results of [4] are the following :

Theorem 1.2 (B., Luca, Mulholland [4])**.** *If p and $q \geq 5$ are primes with $p \geq q^{2q}$ such that there exist coprime, nonzero integers A, B and C, and a positive integer α, satisfying equation (1.2), then $q \in S$.*

Theorem 1.3 (B., Luca, Mulholland [4])**.** *Let $\pi_S(x) = \#\{q \leq x \ : \ q \in S\}$. Then*

$$(1.3) \qquad\qquad \pi_S(x) \ll \sqrt{x} \log^2(x).$$

This latter result may be reasonably easily sharpened, through sieve methods, but, even as stated, demonstrates that $\pi_S(x) = o(\pi(x))$ and hence that we may "solve" equation (1.2) for "almost all" primes q (i.e. for almost all primes, there is no analogous obstruction to that provided by the curve $72A1$ for equation (1.1)).

Our goal in the paper at hand is to improve this result by treating equation (1.2) for a significant number of the primes in S. We begin by defining S_0 to be the subset of S consisting of those primes $q \geq 5$ for which there exists an elliptic curve $E/\mathbb{Q}$ with conductor $N(E) \in \{18q, 36q, 72q\}$, nontrivial rational 2-torsion and the additional property that discriminant $\Delta(E) = T^2$ or $\Delta(E) = -3T^2$ for some integer T. The first main result of this paper is the following sharpening of Theorem 1.2.

Theorem 1.4. *If p and $q \geq 5$ are primes with $p \geq q^{2q}$ such that there exist coprime, nonzero integers A, B and C, and a positive integer α, satisfying equation (1.2), then $q \in S_0$.*

It is by no means clear that the set S_0 is appreciably "smaller" than S. In fact, our expectation is that their counting functions satisfy

$$\pi_S(x) \sim c_1 \sqrt{x} \log x \quad \text{and} \quad \pi_{S_0}(x) \sim c_2 \sqrt{x} \log x,$$

for positive constants c_1 and c_2, where $c_2 < c_1$. A cursory check of Cremona's elliptic curve database [9] reveals that the primes $5 \leq q < 1000$ lying outside S are precisely

$$q = 197, 317, 439, 557, 653, 677, 701, 773, 797 \text{ and } 821,$$

while, in the same range, the primes in S but not S_0 are

$$q = 53, 83, 149, 167, 173, 199, 223, 227, 233, 263, 281, 293, 311, 347, 353, 359, 389,$$
$$401, 419, 443, 449, 461, 467, 479, 487, 491, 563, 569, 571, 587, 599, 617, 641, 643,$$
$$659, 719, 727, 739, 743, 751, 809, 811, 823, 827, 829, 839, 859, 881, 887, 907, 911,$$
$$929, 941, 947, 953, 977 \text{ and } 983.$$

It is, in fact, possible to give a much more concrete characterization of S_0. Let us define sets

$$S_1 = \left\{ q \text{ prime } : q = 2^a 3^b \pm 1, \ \ a \in \{2,3\} \text{ or } a \geq 5, b \geq 0 \right\},$$

$$S_2 = \left\{ q \text{ prime } : q = \left| 2^a \pm 3^b \right|, \ \ a \in \{2,3\} \text{ or } a \geq 5, b \geq 1 \right\},$$

$$S_3 = \left\{ q \text{ prime } : q = \frac{2^a + 1}{3}, \ \ a \geq 5 \text{ odd} \right\},$$

$$S_4 = \left\{ q \text{ prime } : q = d^2 + 2^a 3^b, \ \ a \in \{2,4\} \text{ or } a \geq 8 \text{ even}, b \text{ odd} \right\},$$

$$S_5 = \left\{ q \text{ prime } : q = 3d^2 + 2^a, \ \ a \in \{2,4\} \text{ or } a \geq 8 \text{ even} \right\},$$

$$S_6 = \left\{ q \text{ prime } : q = \frac{d^2 + 3^b}{4}, \ \ d \text{ and } b \text{ odd} \right\},$$

$$S_7 = \left\{ q \text{ prime } : q = \frac{3d^2 + 1}{4}, \ \ d \text{ odd} \right\}$$

and

$$S_8 = \left\{ q \text{ prime } : q = \frac{3v^2 - 1}{2}, \ \ u^2 - 3v^2 = -2 \right\}.$$

Here, a, b, u, v and d are integers.

Proposition 1.5. *We have*

$$S_0 = S_1 \cup S_2 \cup S_3 \cup S_4 \cup S_5 \cup S_6 \cup S_7 \cup S_8.$$

An advantage of this characterization is that it makes it a routine matter to check if a given prime is in S_0 (something that is far from being true for S). It also allows one to rather easily find, via local conditions, sets of primes outside S_0; simply checking that S_0 contains no primes which are simultaneously 5 (mod 8), 2 (mod 3) and 3 (mod 5), yields that if $q \equiv 53 \pmod{120}$, then $q \notin S_0$. More generally, from Theorem 1.4, we deduce the following.

Corollary 1.6. *If p and q are primes with either $q \equiv 53 \pmod{D_1}$ for $D_1 \in \{96, 120, 144\}$ or $q \equiv 65 \pmod{D_2}$ for $D_2 \in \{81, 84\}$, and $p \geq q^{2q}$, then there are no coprime, nonzero integers A, B and C, and positive integers α, satisfying equation (1.2).*

For primes in S_0, we are often still able to say something about solutions to (1.2), in many cases eliminating a positive proportion of the possible prime exponents p. Indeed, let us define

$$T = S_7 \cup \left\{ q \text{ prime } : q = 3d^2 + 16, \ d \in \mathbb{Z} \right\},$$

and, to simplify matters, suppose that $\alpha = 1$ in (1.2), focussing our attention on the equation

$$(1.4) \qquad\qquad A^3 + B^3 = q\,C^p.$$

We have the following.

Theorem 1.7. *If q is a prime with $q \notin T$, then, for a positive proportion of primes p, there are no solutions to equation (1.4) in coprime nonzero integers A, B and C.*

We note that, defining $\pi_T(x)$ to be the counting function for primes in T, it is not difficult to show that

$$\pi_T(x) \ll \frac{\sqrt{x}}{\log x},$$

whereby standard heuristics suggest that the set T is genuinely of smaller order than S_0 (though, in point of fact, it would be remarkably difficult to prove that either set is even infinite).

As a sampling of more explicit work along these lines, we mention the following results for certain primes in S_0 (see also Theorem 7.1 in Section 7).

Theorem 1.8. *Suppose that $q = 2^a 3^b - 1$ is prime, where $a \geq 5$ and $b \geq 1$ integers. If $p > q^{2q}$ is prime and there exists a positive integer α and coprime, nonzero integers A, B and C satisfying equation (1.2), then*

$$\left(\frac{\alpha}{p} \right) = \left(\frac{4 - a}{p} \right) = \left(\frac{-6b}{p} \right).$$

Theorem 1.9. *If p is prime with $p \equiv 13, 19$ or $23 \pmod{24}$, then there are no coprime, nonzero integers A, B and C satisfying*

$$(1.5) \qquad\qquad A^3 + B^3 = 5C^p.$$

These results all follow from applying the modular method, together with a somewhat elaborate blend of techniques from algebraic and analytic number theory, and Diophantine approximation, with a variety of *symplectic criteria* (see Section 6) to equation (1.2). This last approach was developed initially by Halberstadt and Kraus [16] and has recently been refined and generalized in the work of the third author [12], jointly with Naskręcki and Stoll [15] and with Kraus [13]. One of the justifications for the current paper is to provide a number of examples which, on some level, utilize the full power of these recently developed symplectic tools.

As a final comment, we note that it should be possible to apply techniques based upon quadratic reciprocity, as in, say, work of Chen and Siksek [8], to say something further about equation (1.2) for certain primes q and certain exponents. We will not undertake this here.

The outline of this paper is as follows. In Section 2, we restate a number of results from [4] pertaining to Frey-Hellegouarch curves that we require in the sequel. In Section 3, we characterize isomorphism classes of elliptic curves over $\mathbb{Q}$ with nontrivial rational 2-torsion and conductor $18q, 36q$ or $72q$, for q prime. Section 4 contains the proof of Theorem 1.4. In Section 5, we make a number of remarks

about the sets S_i comprising S_0. In Section 6, we apply several symplectic criteria to the Frey-Hellegouarch curve and the elliptic curves corresponding to the primes in S_0. In Section 7, we prove Theorems 1.7, 1.8 and 1.9 (and somewhat more besides). Section 8 is an appendix containing information on the invariants $c_4(E)$ and $c_6(E)$ for elliptic curves of conductor $18q, 36q$ and $72q$, corresponding to the primes in S.

2. FREY-HELLEGOUARCH CURVES

Let us suppose that $q \geq 5$ is prime, α is a positive integer, and that we have a solution to equation (1.2) in coprime nonzero integers A, B and C where, without loss of generality, AC is even and $B \equiv (-1)^{C+1} \pmod 4$. Following Darmon and Granville [11], we associate to such a solution a *Frey-Hellegouarch elliptic curve* $F = F_{A,B}^{(i)}$ of the shape

$$F_{A,B}^{(0)} \quad : \quad y^2 + xy = x^3 + \frac{3(B - A) + 2}{8}x^2 + \frac{3(A + B)^2}{64}x + \frac{9(B - A)(A + B)^2}{512}$$

or

$$F_{A,B}^{(1)} \quad : \quad y^2 = x^3 + 3ABx + B^3 - A^3,$$

depending on whether C is even or odd, respectively. For future reference, we note that these are minimal models. The standard invariants $c_4(F), c_6(F)$ and $\Delta(F)$ attached to $F = F_{A,B}^{(i)}$ are

$$(2.1) \qquad \begin{cases} c_4(F) = -2^{4i}3^2 AB, \\ c_6(F) = 2^{6i-1}3^3(A^3 - B^3), \\ \Delta(F) = -2^{12i-8}3^3 q^{2\alpha}C^{2p}. \end{cases}$$

Let $\mathcal{R}$ denote the product of the primes ℓ satisfying $\ell \mid C$ and $\ell \nmid 6q$. A standard application of Tate's algorithm leads to the following.

Lemma 2.1. *If $F = F_{A,B}^{(i)}$, then the conductor N_F satisfies*

$$N_F = \begin{cases} 18\,q\,\mathcal{R} & \text{if } C \text{ even, } B \equiv -1 \pmod 4, \text{ or} \\ 36\,q\,\mathcal{R} & \text{if } C \text{ odd, } v_2(A) \geq 2 \text{ and } B \equiv 1 \pmod 4, \text{ or} \\ 72\,q\,\mathcal{R} & \text{if } C \text{ odd, } v_2(A) = 1 \text{ and } B \equiv 1 \pmod 4. \end{cases}$$

In particular, F has multiplicative reduction at the prime q.

Arguing as in [4] and [19] we find that, for $p \geq 17$, there necessarily exists a newform $f \in S_2^+(N_F/\mathcal{R})$ (the space of weight 2 cuspidal newforms for the congruence subgroup $\Gamma_0(N_F/\mathcal{R})$), whose Taylor expansion is

$$f = q + \sum_{m \geq 2} a_m(f)q^m \text{ where } q = e^{2\pi i t},$$

and a place $\mathfrak{p}$ of $\overline{\mathbb{Q}}$ lying above p, such that

$$(2.2) \qquad \overline{\rho}_{F,p} \sim \overline{\rho}_{f,\mathfrak{p}},$$

where $\overline{\rho}_{F,p}$ and $\overline{\rho}_{f,\mathfrak{p}}$ denote, respectively, the mod $\mathfrak{p}$ Galois representations attached to F and f. In particular, for all prime numbers $\ell \nmid pN_F$, we have

$$a_\ell(f) \equiv a_\ell(F) \pmod{\mathfrak{p}},$$

where $a_\ell(F)$ denotes the trace of Frobenius of F at the prime ℓ. Therefore,

$$(2.3) \qquad\qquad p \mid \operatorname{Norm}_{K_f/\mathbb{Q}}(a_\ell(f) - a_\ell(F)),$$

for K_f the field of definition of the coefficients of f. Furthermore, the level lowering condition implies

$$(2.4) \qquad\qquad p \mid \operatorname{Norm}_{K_f/\mathbb{Q}}(a_\ell(f) \pm (\ell+1)),$$

for each prime $\ell \neq p$ dividing $\mathcal{R}$.

From the arguments of [4], under the assumption that $p > q^{2p}$, we may conclude that the form f has rational integer Fourier coefficients $a_m(f)$ for all $m \geq 1$, whereby f corresponds to an isogeny class of elliptic curves over $\mathbb{Q}$ with conductor $N = 18q$, $36q$ or $72q$, and further that the corresponding elliptic curve E has a rational 2-torsion point. This, in essence, is Theorem 1.2. To complete the proof of Theorem 1.4, it remains to eliminate the possibility of the Frey-Hellegouarch curve F "arising mod p" from an elliptic curve E that fails to be isogenous to a curve with discriminant of the shape T^2 or $-3T^2$. To do this, we first require a very precise characterization of elliptic curves of conductor $N = 18q$, $36q$ or $72q$, with nontrivial rational 2-torsion.

3. CLASSIFICATION RESULTS FOR PRIMES OF CONDUCTOR $18q$, $36q$ AND $72q$

In this section, we will state theorems that provide an explicit classification for primes q of the corresponding isomorphism classes of elliptic curves $E/\mathbb{Q}$ with conductor $18q$, $36q$ or $72q$ and nontrivial rational 2-torsion. The following results are mild sharpenings and simplifications of special cases of Theorems 3.13, 3.14 and 3.15 of Mulholland [21] (see also Theorems 4.0.8, 4.0.10 and 4.0.12 of [7]), where analogous results are derived more generally for elliptic curves with nontrivial rational 2-torsion and conductor of the shape $2^\alpha 3^\beta q^\gamma$.

Theorem 3.1. *If $q > 3$ is prime, then there exists an elliptic curve $E/\mathbb{Q}$ of conductor $18q$ with at least one rational 2-torsion point precisely when either E is isogenous to one of (in Cremona's notation)*

$$90a, 90b, 90c, 126a, 126b, 198b, 198c, 198d, 198e, 306a,$$
$$306b, 306c, 342c, 342f, 414a, 1314a \text{ or } 1314f,$$

or E is $\mathbb{Q}$-isomorphic to

$$\tilde{E} \quad : \quad y^2 + xy = x^3 + a_2 x^2 + a_4 x + a_6$$

and at least one of the following occurs:

(1) *There exist integers $a \geq 5$ and $b \geq 0$ such that*

$$q = 2^a 3^b + (-1)^\delta, \quad for \quad \delta \in \{0, 1\},$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4
$18q.1.a1$	$(-1)^{\delta+1}2^{a-1}3^{b+1}-1$	$2^{a-4}3^{b+2}q$
$18q.1.a2$	$(-1)^{\delta+1}2^{a-1}3^{b+1}-1$	$-2^{a-2}3^{b+2}q$
$18q.1.a3$	$(-1)^{\delta+1}2^{a-3}3^{b+1}-1$	$2^{2a-8}3^{2b+2}$
$18q.1.a4$	$(-1)^{\delta}2^{a-2}3^{b+1}-1$	$(-1)^{\delta}2^{a-2}3^{b+2}$
curve	a_6	Δ
$18q.1.a1$	0	$2^{2a-8}3^{2b+6}q^2$
$18q.1.a2$	$(-1)^{\delta}2^{a-4}3^{b+3}\left(2q-(-1)^{\delta}\right)q$	$2^{a-4}3^{b+6}q$
$18q.1.a3$	0	$(-1)^{\delta}2^{4a-16}3^{4b+6}q$
$18q.1.a4$	$2^{a-4}3^{b+3}(q-2(-1)^{\delta})$	$(-1)^{\delta+1}2^{a-4}3^{b+6}q^4$

(2) *There exists an odd integer $a \geq 5$ such that*

$$q = \frac{2^a + 1}{3}$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4
$18q.2.a1$	$-3 \cdot 2^{a-1} - 1$	$2^{a-4}3^3q$
$18q.2.a2$	$-3 \cdot 2^{a-1} - 1$	$-2^{a-2}3^3q$
$18q.2.a3$	$-3 \cdot 2^{a-3} - 1$	$2^{2a-8}3^2$
$18q.2.a4$	$3 \cdot 2^{a-2} - 1$	$2^{a-2}3^2$
curve	a_6	Δ
$18q.2.a1$	0	$2^{2a-8}3^8q^2$
$18q.2.a2$	$2^{a-4}3^4\left(2^{a+1}+1\right)q$	$2^{a-4}3^7q$
$18q.2.a3$	0	$2^{4a-16}3^7q$
$18q.2.a4$	$2^{a-4}3^3\left(2^a-1\right)$	$-2^{a-4}3^{10}q^4$

(3) *There exist integers $a \geq 5$ and $b \geq 1$, and $\delta_1, \delta_2 \in \{0,1\}$ such that*

$$q = (-1)^{\delta_1}2^a + (-1)^{\delta_2}3^b$$

and, writing $\delta = b + \delta_1 + \delta_2 + 1$, $\tilde{E}$ is one of the following :

curve	a_2	a_4
$18q.3.a1$	$-\frac{1}{4}+(-1)^{\delta}\left(3 \cdot 2^{a-2}+(-1)^{\delta_1}\frac{3q}{4}\right)$	$(-1)^{\delta_1}2^{a-4}3^2q$
$18q.3.a2$	$-\frac{1}{4}+(-1)^{\delta}\left(3 \cdot 2^{a-2}+(-1)^{\delta_1}\frac{3q}{4}\right)$	$(-1)^{\delta_1+1}2^{a-2}3^2q$
$18q.3.a3$	$-\frac{1}{4}+(-1)^{\delta}3 \cdot 2^{a-3}-(-1)^{b}\frac{3^{b+1}}{4}$	$2^{2a-8}3^2$
$18q.3.a4$	$-\frac{1}{4}+(-1)^{\delta+1}\left(3 \cdot 2^{a-1}+(-1)^{\delta_1+1}\frac{3q}{4}\right)$	$(-1)^{\delta_1+\delta_2}2^{a-2}3^{b+2}$
curve	a_6	Δ
$18q.3.a1$	0	$2^{2a-8}3^{2b+6}q^2$
$18q.3.a2$	$(-1)^{\delta+\delta_1+1}3^3 \cdot 2^{a-4}(2^{a+1}+(-1)^{\delta_1+\delta_2}3^b)q$	$2^{a-4}3^{4b+6}q$
$18q.3.a3$	0	$(-1)^{\delta_2}2^{4a-16}3^{b+6}q$
$18q.3.a4$	$(-1)^{\delta}3^{b+3} \cdot 2^{a-4}(3^b+(-1)^{1+\delta_1+\delta_2}2^a)$	$(-1)^{b+\delta}2^{a-4}3^{b+6}q^4$

(4) *There exist integers* $a \geq 7$, $b \geq 0$, $\delta_1, \delta_2 \in \{0,1\}$ *and* $d \equiv 1 \pmod 4$, *such that* $(\delta_1, \delta_2) \neq (1,1)$ *and, if we have* $a \equiv b \equiv 0 \pmod 2$, *then* $(\delta_1, \delta_2) = (0,0)$, *with*

$$q = (-1)^{\delta_1} d^2 + (-1)^{\delta_2} 2^a 3^b,$$

and $\tilde{E}$ *is one of the following :*

curve	a_2	a_4
$18q.4.a1$	$-\left(\frac{3d+1}{4}\right)$	$(-1)^{\delta_1+\delta_2+1} 2^{a-6} 3^{b+2}$
$18q.4.a2$	$-\left(\frac{3d+1}{4}\right)$	$(-1)^{\delta_1+\delta_2} 2^{a-4} 3^{b+2}$

curve	a_6	Δ
$18q.4.a1$	0	$(-1)^{\delta_1} 2^{2a-12} 3^{2b+6} q$
$18q.4.a2$	$(-1)^{\delta_1+\delta_2+1} 2^{a-6} 3^{b+3} d$	$(-1)^{\delta_1+\delta_2+1} 2^{a-6} 3^{b+6} q^2$

(5) *There exist integers* $a \geq 7$, $\delta_1, \delta_2 \in \{0,1\}$ *and* $d \equiv 1 \pmod 4$, *such that* $(\delta_1, \delta_2) \neq (1,1)$,

$$q = (-1)^{\delta_1} 3 d^2 + (-1)^{\delta_2} 2^a,$$

and $\tilde{E}$ *is one of the following :*

curve	a_2	a_4
$18q.5.a1$	$-\left(\frac{3d+1}{4}\right)$	$(-1)^{\delta_1+\delta_2+1} 2^{a-6} 3$
$18q.5.a2$	$-\left(\frac{3d+1}{4}\right)$	$(-1)^{\delta_1+\delta_2} 2^{a-4} 3$
$18q.5.b1$	$\frac{9d-1}{4}$	$(-1)^{\delta_1+\delta_2+1} 2^{a-6} 3^3$
$18q.5.b2$	$\frac{9d-1}{4}$	$(-1)^{\delta_1+\delta_2} 2^{a-4} 3^3$

curve	a_6	Δ
$18q.5.a1$	0	$(-1)^{\delta_1} 2^{2a-12} 3^3 q$
$18q.5.a2$	$(-1)^{\delta_1+\delta_2+1} 2^{a-6} 3^2 d$	$(-1)^{\delta_1+\delta_2+1} 2^{a-6} 3^3 q^2$
$18q.5.b1$	0	$(-1)^{\delta_1} 2^{2a-12} 3^9 q$
$18q.5.b2$	$(-1)^{\delta_1+\delta_2} 2^{a-6} 3^5 d$	$(-1)^{\delta_1+\delta_2+1} 2^{a-6} 3^9 q^2$

(6) *There exist integers* $a \geq 7$, $b \geq 1$ *and* $d \equiv 1 \pmod 4$, *with* a *odd, such that*

$$q = \frac{d^2 + 2^a}{3^b},$$

and $\tilde{E}$ *is one of the following :*

curve	a_2	a_4	a_6	Δ
$18q.6.a1$	$-\left(\frac{3d+1}{4}\right)$	$-2^{a-6} 3^2$	0	$2^{2a-12} 3^{b+6} q$
$18q.6.a2$	$-\left(\frac{3d+1}{4}\right)$	$2^{a-4} 3^2$	$-2^{a-6} 3^3 d$	$-2^{a-6} 3^{2b+6} q^2$

Theorem 3.2. *If* $q > 3$ *is prime, then there exists an elliptic curve* $E/\mathbb{Q}$ *of conductor* $36q$ *with at least one rational 2-torsion point precisely when either* E *is isogenous to one of (in Cremona's notation)*

$$180a, 252a \text{ or } 468d,$$

or E *is* $\mathbb{Q}$-*isomorphic to*

$$\tilde{E} \quad : \quad y^2 = x^3 + a_2 x^2 + a_4 x$$

and at least one of the following occurs:

(1) *There exist integers u and v with $u \equiv v \equiv 1 \pmod 4$ and $u^2 - 3v^2 = -2$, such that*
$$q = \frac{3v^2 - 1}{2}$$
and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$36q.1.a1$	$-3uv$	$3q^2$	$-2^4 3^3 q^4$
$36q.1.a2$	$6uv$	-3	$2^8 3^3 q^2$
$36q.1.b1$	$9uv$	$3^3 q^2$	$-2^4 3^9 q^4$
$36q.1.b2$	$-18uv$	-3^3	$2^8 3^9 q^2$

(2) *There exists an integer $d \equiv 1 \pmod 8$, such that*
$$q = \frac{3d^2 + 1}{4}$$
and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$36q.2.a1$	$-3d$	$3q$	$-2^4 3^3 q^2$
$36q.2.a2$	$6d$	-3	$2^8 3^3 q$
$36q.2.b1$	$9d$	$3^3 q$	$-2^4 3^9 q^2$
$36q.2.b2$	$-18d$	-3^3	$2^8 3^9 q$

(3) *There exists an odd integer $b \geq 1$ and an integer $d \equiv 1 \pmod 4$ such that*
$$q = \frac{d^2 + 3^b}{4} \equiv 3 \pmod 4$$
and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$36q.3.a1$	$-3d$	$3^2 q$	$-2^4 3^{b+6} q^2$
$36q.3.a2$	$6d$	-3^{b+2}	$2^8 3^{2b+6} q$

(4) *There exist integers $b \geq 1$, $\delta \in \{0, 1\}$ and $d \equiv 1 \pmod 4$, such that b is odd, $d \equiv 1 \pmod 4$,*
$$q = (-1)^\delta \left(d^2 - 4 \cdot 3^b \right)$$
and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$36q.4.a1$	$-3d$	3^{b+2}	$(-1)^\delta 2^4 3^{2b+6} q$
$36q.4.a2$	$6d$	$(-1)^\delta 3^2 q$	$2^8 3^{b+6} q^2$

(5) *There exist integers $b \geq 1$, $\delta \in \{0, 1\}$, $n \geq 7$ and $d \equiv 1 \pmod 4$, such that b is odd, every prime factor of n is at least 7,*
$$q^n = (-1)^\delta \left(d^2 - 4 \cdot 3^b \right)$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$36q.5.a1$	$-3d$	3^{b+2}	$(-1)^\delta 2^4 3^{2b+6} q^n$
$36q.5.a2$	$6d$	$(-1)^\delta 3^2 q^n$	$2^8 3^{b+6} q^{2n}$

(6) *There exists an integer $d \equiv 1 \pmod 4$, such that*

$$q = 3d^2 - 4$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$36q.6.a1$	$-3d$	3	$2^4 3^3 q$
$36q.6.a2$	$6d$	$3q$	$2^8 3^3 q^2$
$36q.6.b1$	$9d$	3^3	$2^4 3^9 q$
$36q.6.b2$	$-18d$	$3^3 q$	$2^8 3^9 q^2$

(7) *There exists an integer $d \equiv 1 \pmod 4$, and an even integer $b \geq 0$ such that*

$$q = d^2 + 4 \cdot 3^b,$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$36q.7.a1$	$-3d$	-3^{b+2}	$2^4 3^{2b+6} q$
$36q.7.a2$	$6d$	$3^2 q$	$-2^8 3^{b+6} q^2$

Theorem 3.3. *If $q > 3$ is prime, then there exists an elliptic curve $E/\mathbb{Q}$ of conductor $72q$ with at least one rational 2-torsion point precisely when either E is isogenous to one of (in Cremona's notation)*

$$360a, 360b, 360c, 360d, 936a, 936d, 936f, 2088b,$$
$$2088h, 3384a, 5256e, 13896f \text{ or } 83016c,$$

or E is $\mathbb{Q}$-isomorphic to

$$\tilde{E} \quad : \quad y^2 = x^3 + a_2 x^2 + a_4 x$$

and at least one of the following occurs:

(1) *There exists an odd integer $b \geq 1$ such that*

$$q = \frac{3^b + 1}{4}$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$72q.1.a1$	$24q - 3$	$2^2 3^{b+2} q$	$2^8 3^{2b+6} q^2$
$72q.1.a2$	$-48q + 6$	3^2	$2^{10} 3^{b+6} q$
$72q.1.a3$	$24q + 6$	3^{2b+2}	$2^{10} 3^{4b+6} q$
$72q.1.a4$	$6q - 3$	$3^2 q^2$	$-2^4 3^{b+6} q^4$

(2) *There exist integers $a \in \{2,3\}$, $b \geq 0$ and $\delta \in \{0,1\}$ such that*

$$q = 2^a \cdot 3^b + (-1)^\delta$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$72q.2.a1$	$(-1)^{\delta+1}2^{a+1}3^{b+1} - 3$	$2^a 3^{b+2} q$	$2^{2a+4}3^{2b+6}q^2$
$72q.2.a2$	$(-1)^\delta 2^{a+2}3^{b+1} + 6$	3^2	$2^{a+8}3^{b+6}q$
$72q.2.a3$	$(-1)^{\delta+1}2^{a-1}3^{b+1} - 3$	$2^{2a-4}3^{2b+2}$	$(-1)^\delta 2^{4a-4}3^{4b+6}q$
$72q.2.a4$	$(-1)^{\delta+1}2^{a+1}3^{b+1} + 6$	$3^2 q^2$	$(-1)^{\delta+1}2^{a+8}3^{b+6}q^4$

(3) *There exist integers $a \in \{2,3\}$, $b \geq 0$ and $\delta \in \{0,1\}$ such that*

$$q = 3^b + (-1)^\delta 2^a$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$72q.3.a1$	$(-1)^{b+1}3\left(3^b - (-1)^\delta 2^a\right)$	$(-1)^{\delta+1}2^a 3^{b+2}$	$2^{2a+4}3^{2b+6}q^2$
$72q.3.a2$	$(-1)^b 6\left(3^b - (-1)^\delta 2^a\right)$	$3^2 q^2$	$(-1)^{\delta+1}2^{a+8}3^{b+6}q^4$
$72q.3.a3$	$(-1)^b 6\left(3^b + (-1)^\delta 2^{a+1}\right)$	3^{2b+2}	$(-1)^\delta 2^{a+8}3^{4b+6}q$
$72q.3.a4$	$(-1)^{b+1}3\left(3^b + (-1)^\delta 2^{a-1}\right)$	$2^{2a-4}3^2$	$2^{4a-4}3^{b+6}q$

(4) *There exists an integer $d \equiv 1 \pmod 4$ such that*

$$q = 3d^2 + 4$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$72q.4.a1$	$3d$	-3	$2^4 3^3 q$
$72q.4.a2$	$-6d$	$3q$	$-2^8 3^3 q^2$
$72q.4.b1$	$-9d$	-3^3	$2^4 3^9 q$
$72q.4.b2$	$18d$	$3^3 q$	$-2^8 3^9 q^2$

(5) *There exist integers $a \in \{4,5\}$, $\delta \in \{0,1\}$ and $d \equiv 1 \pmod 4$, such that*

$$q = 3d^2 + (-1)^\delta 2^a$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$72q.5.a1$	$-3d$	$(-1)^{\delta+1}2^{a-2}3$	$2^{2a}3^3 q$
$72q.5.a2$	$6d$	$3q$	$(-1)^{\delta+1}2^{a+6}3^3 q^2$
$72q.5.b1$	$9d$	$(-1)^{\delta+1}2^{a-2}3^3$	$2^{2a}3^9 q$
$72q.5.b2$	$-18d$	$3^3 q$	$(-1)^{\delta+1}2^{a+6}3^9 q^2$

(6) *There exist an integer $d \equiv 5 \pmod 8$ such that*

$$q = \frac{3d^2 + 1}{4}$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$72q.6.a1$	$3d$	$3q$	$-2^4 3^3 q^2$
$72q.6.a2$	$-6d$	-3	$2^8 3^3 q$
$72q.6.b1$	$-9d$	$3^3 q$	$-2^4 3^9 q^2$
$72q.6.b2$	$18d$	-3^3	$2^8 3^9 q$

(7) *There exist odd integers $b \geq 1$ and $d \equiv 1 \pmod 4$ such that*

$$q = \frac{d^2 + 3^b}{4} \equiv 1 \pmod 4$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$72q.7.a1$	$3d$	$3^2 q$	$-2^4 3^{b+6} q^2$
$72q.7.a2$	$-6d$	-3^{b+2}	$2^8 3^{2b+6} q$

(8) *There exist odd integers $b \geq 1$ and $d \equiv 1 \pmod 4$ such that*

$$q = d^2 + 4 \cdot 3^b$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$72q.8.a1$	$3d$	-3^{b+2}	$2^4 3^{2b+6} q$
$72q.8.a2$	$-6d$	$3^2 q$	$-2^8 3^{b+6} q^2$

(9) *There exist integers $a \in \{4,5\}$, $b \geq 0$, $\delta_1, \delta_2 \in \{0,1\}$ and $d \equiv 1 \pmod 4$, such that $(\delta_1, \delta_2) \neq (1,1)$, b is odd if $a = 4$ and $\delta_1 \neq \delta_2$,*

$$q = (-1)^{\delta_1} d^2 + (-1)^{\delta_2} 2^a 3^b,$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$72q.9.a1$	$-3d$	$(-1)^{\delta_1+\delta_2+1} 2^{a-2} 3^{b+2}$	$(-1)^{\delta_1} 2^{2a} 3^{2b+6} q$
$72q.9.a2$	$6d$	$(-1)^{\delta_1} 3^2 q$	$(-1)^{\delta_1+\delta_2+1} 2^{a+6} 3^{b+6} q^2$

(10) *There exist integers $a \in \{4,5\}$, $b \geq 0$, $\delta \in \{0,1\}$, $d \equiv 1 \pmod 4$ and n, such that the least prime divisor of n is at least 7, b is odd if $a = 4$,*

$$q^n = (-1)^{\delta} \left(d^2 - 2^a 3^b \right),$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$72q.10.a1$	$-3d$	$2^{a-2} 3^{b+2}$	$(-1)^{\delta} 2^{2a} 3^{2b+6} q^n$
$72q.10.a2$	$6d$	$(-1)^{\delta} 3^2 q^n$	$2^{a+6} 3^{b+6} q^{2n}$

(11) *There exist integers $b \geq 0$ and $d \equiv 1 \pmod 4$ such that*

$$q = \frac{d^2 + 32}{3^b}$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$72q.11.a1$	$-3d$	$-2^3 3^2$	$2^{10} 3^{b+6} q$
$72q.11.a2$	$6d$	$3^{b+2} q$	$-2^{11} 3^{2b+6} q^2$

(12) *There exist integers $b \geq 0$, $d \equiv 1 \pmod 4$ and n, such that the least prime divisor of n is at least 7,*

$$q^n = \frac{d^2 + 32}{3^b}$$

and $\tilde{E}$ is one of the following :

curve	a_2	a_4	Δ
$72q.12.a1$	$-3d$	$-2^3 3^2$	$2^{10} 3^{b+6} q^n$
$72q.12.a2$	$6d$	$3^{b+2} q^n$	$-2^{11} 3^{2b+6} q^{2n}$

We should mention that while we are currently unable to rule out the existence of primes in families (10) and (12) in Theorem 3.3, we strongly suspect that there are no such primes. Further, we must confess that our notation can admit a certain amount of ambiguity as, for a given prime q, we could have multiple representations of q giving rise to non-isogenous curves with the same labels. By way of example,

(3.1) $$q = 10369 = 1^2 + 2^7 \cdot 3^4 = 65^2 + 2^{11} \cdot 3$$

and the curves denoted $18q.4.a$ corresponding to these two representations are non-isogenous. For $q \in S_i$ for a fixed $1 \leq i \leq 8$, however, it is straightforward to show that there are at most finitely many such distinct such representations – for all except $i = 2$, the parametrization monotonically increasing in the variables a, b, v and d. For $q \in S_2$, the same is easily seen to be true except, possibly, for the cases with $q = |2^a - 3^b|$. In this last situation, via a result of Tijdeman [24], we have

$$\left|2^a - 3^b\right| \geq 3^b b^{-\kappa},$$

for some effectively computable absolute positive constant κ, at least provided $b > 2$, and hence, again, q has only finitely many such representations (at most 3, in fact, by a result of the first author [2]).

Combining Theorems 3.1, 3.2 and 3.3, together with the definition of S_0, yields the following.

Corollary 3.4. *An elliptic curve $E/\mathbb{Q}$ is in S_0 precisely if E is either in one of the isogeny classes (in Cremona's notation)*

$$90c, 126b, 252a, 306c, 342f, 360a, 360d, 936d \text{ or } 5256e,$$

or E is isogenous to one of

$18q.1.a, 18q.2.a, 18q.3.a, 18q.4.a$ (with $\delta_1 = \delta_2 = 0, a$ even, b odd), $18.q.5.a$ and
$18.q.5.b$ (with, in both cases, $\delta_1 = \delta_2 = 0$ and a even), $36q.1.a, 36q.1.b, 36q.2.a,$
$36q.2.b, 36q.3.a, 72q.1.a, 72q.2.a, 72q.3.a, 72.q.4.a, 72.q.4.b, 72.q.5.a$ and $72q.5.b$
(with, in both cases, $\delta = 0$ and $a = 4$), $72q.6.a, 72q.6.b, 72.7.a, 72q.8.a$
and $72q.9.a$ (with $\delta_1 = \delta_2 = 0, a = 4, b$ odd).

4. Finishing the proof of Theorem 1.4

From the classification results of the preceding section, we need to show only that, for suitably large primes p, equation (1.2) has no solutions in coprime nonzero integers, with Frey-Hellegouarch curve F corresponding (in the sense of Section 2) to an elliptic curve E in one of the isogeny classes

$$90a, 90b, 126a, 180a, 198b, 198c, 198d, 198e, 306a, 306b,$$
(4.1)
$$342b, 342c, 360b, 360c, 414a, 468d, 936a, 936f, 1314a,$$
$$1314f, 2088b, 2088h, 3384a, 13896f \text{ or } 83016c,$$

or

$$18q.4.a \text{ (with } \delta_1 \neq \delta_2, \text{ or } \delta_1 = \delta_2 = 0 \text{ and either } a \text{ odd, or } b \text{ even)},$$
$$18.q.5.a \text{ and } 18q.5.b \text{ (with, in both cases, } \delta_1 \neq \delta_2, \text{ or } \delta_1 = \delta_2 = 0 \text{ and}$$
(4.2) $\quad a$ odd$)$, $18q.6.a, 36q.4.a$ $36q.5.a,$ $36q.6.a,$ $36q.6.b,$ $36q.7.a,$ $72.q.5.a$
$$\text{and } 72q.5.b \text{ (with, in both cases, } \delta = 1 \text{ or } a = 5), \ 72q.9.a$$
$$\text{(with } \delta_1 \neq \delta_2, \text{ or } \delta_1 = \delta_2 = 0 \text{ and either } a = 5, \text{ or } a = 4 \text{ and } b \text{ even)},$$
$$72q.10.a, \ 72q.11.a \text{ or } 72q.12.a.$$

Our key observation to start is that, from (2.1), the Frey-Hellegouarch curve $F = F_{A,B}^{(i)}$ has minimal discriminant of the shape $-3T^2$ for $T = 2^{6i-4}3q^\alpha C^p$. It follows that $E(\mathbb{F}_\ell)$ contains a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ for every prime $\ell \nmid 6q$ for which $\left(\frac{-3}{\ell}\right) = 1$; i.e. for $\ell \equiv 1 \pmod 6$. We thus have that

$$a_\ell(F) \equiv \ell + 1 \pmod 4 \tag{4.3}$$

for every such prime ℓ. If, for each curve E in the isogeny classes (4.1) and (4.2), we are able to find a prime $\ell \equiv 1 \pmod 6$ with $\ell \nmid 6q$, for which $a_\ell(E) \not\equiv \ell + 1 \pmod 4$, it follows from (2.3), (2.4), (4.3) and the Hasse bounds that

$$p \leq \ell + 1 + 2\sqrt{\ell}. \tag{4.4}$$

For curves E in the isogeny classes (4.1), we may check that it suffices to choose, in all cases,

$$\ell \in \{7, 13, 19, 31, 37\}.$$

To show that we can always find a suitable prime ℓ for E in the isogeny classes (4.2), let us suppose that, more generally, we have an elliptic curve E over $\mathbb{Q}$, with a rational 2-torsion point at, say, $(0,0)$, given by the model

$$E \ : \ y^2 = x^3 + ux^2 + vx. \tag{4.5}$$

For a prime of good reduction $\ell \geq 5$ for E, it follows that the Fourier coefficient $a_\ell(E)$ satisfies $a_\ell(E) \equiv \ell + 1 \pmod 4$ precisely when $E(\mathbb{F}_\ell)$ contains a subgroup isomorphic to either $\mathbb{Z}_2 \times \mathbb{Z}_2$ or to $\mathbb{Z}_4$. The first case occurs exactly when the cubic $x^3 + ux^2 + vx$ splits completely modulo ℓ, i.e. when

$$\left(\frac{\Delta(E)}{\ell}\right) = \left(\frac{u^2 - 4v}{\ell}\right) = 1.$$

To have the second case, there must exist a point P in $E(\mathbb{F}_\ell)$ with the property that $P \neq (0,0)$ but $2P = (0,0)$. From the standard duplication formula, the x-coordinate of the point $2P$ on E satisfies

$$x(2P) = \frac{x^4 - 2vx^2 + v^2}{4y^2} = \frac{(x^2 - v)^2}{4y^2}$$

and hence there can exist a point P with $x(2P) = 0$ precisely when v is a square modulo ℓ. In summary, we have that $a_\ell(E) \equiv \ell + 1 \pmod 4$ exactly when either

$$\left(\frac{\Delta(E)}{\ell}\right) = 1 \quad \text{or} \quad \left(\frac{v}{\ell}\right) = 1.$$

For the curves of conductor $36q$ and $72q$ ($36q.4.a$, $36q.5.a$, $36q.6.a$, $36q.6.b$, $72.q.4.a$, $72q.4.b$, $72q.8.a$, $72q.9.a$, $72q.10.a$ and $72q.11.a.$), our given models are already of the form $y^2 = x^3 + ux^2 + vx$, with $u = a_2(E)$ and $v = a_4(E)$. For our families of conductor $18q$ ($18q.4.a$, $18q.5.a$, $18q.5.b$ and $18q.6.a$), we need to move our nontrivial rational 2-torsion point to $(0,0)$ to obtain a (non-minimal) model of the shape (4.5) (the discriminant remaining invariant modulo squares). We summarize our results in the following table.

E	Additional conditions	$\left\{\left(\frac{v}{\ell}\right), \left(\frac{\Delta(E)}{\ell}\right)\right\}$
$18q.4.a$	unless $\delta_1 = \delta_2 = 0$, a even and b odd	$\left\{\left(\frac{(-1)^{\delta_1}q}{\ell}\right), \left(\frac{(-1)^{\delta_1+\delta_2+1}2^a3^b}{\ell}\right)\right\}$
$18q.5.a$ and b	unless $\delta_1 = \delta_2 = 0$, a even	$\left\{\left(\frac{(-1)^{\delta_1}3q}{\ell}\right), \left(\frac{(-1)^{\delta_1+\delta_2+1}2^a3}{\ell}\right)\right\}$
$18q.6.a$	none	$\left\{\left(\frac{3^bq}{\ell}\right), \left(\frac{-2}{\ell}\right)\right\}$
$36q.4.a$	none	$\left\{\left(\frac{(-1)^{\delta_1}q}{\ell}\right), \left(\frac{3}{\ell}\right)\right\}$
$36q.5.a$	none	$\left\{\left(\frac{3}{\ell}\right), \left(\frac{(-1)^{\delta}q}{\ell}\right)\right\}$
$36q.6.a$ and b	none	$\left\{\left(\frac{3q}{\ell}\right), \left(\frac{3}{\ell}\right)\right\}$
$36q.7.a$	none	$\left\{\left(\frac{-1}{\ell}\right), \left(\frac{q}{\ell}\right)\right\}$
$72q.5.a$ and b	$(\delta, a) = (0,5), (1,4)$ or $(1,5)$	$\left\{\left(\frac{3q}{\ell}\right), \left(\frac{(-1)^{\delta+1}2^a3}{\ell}\right)\right\}$
$72q.9.a$	unless $\delta_1 = \delta_2 = 0$, $a = 4$ and b odd	$\left\{\left(\frac{(-1)^{\delta_1}q}{\ell}\right), \left(\frac{(-1)^{\delta_1+\delta_2+1}2^a3^b}{\ell}\right)\right\}$
$72q.10.a$	none	$\left\{\left(\frac{(-1)^{\delta}q}{\ell}\right), \left(\frac{2^a3^b}{\ell}\right)\right\}$
$72q.11.a$ and $12a$	none	$\left\{\left(\frac{3^bq}{\ell}\right), \left(\frac{-2}{\ell}\right)\right\}$

For example, in case $E = 72q.12.a1$, we have, for $\ell \nmid 6q$,

$$\left(\frac{\Delta(E)}{\ell}\right) = \left(\frac{3^bq}{\ell}\right) \quad \text{and} \quad \left(\frac{v}{\ell}\right) = \left(\frac{a_4(E)}{\ell}\right) = \left(\frac{-2}{\ell}\right).$$

In particular, if we assume, say, that b is odd, for any prime $\ell \equiv 7 \pmod{24}$ such that q is a quadratic residue modulo ℓ, or prime $\ell \equiv 13 \pmod{24}$ with q a quadratic non-residue modulo ℓ, we have

$$(4.6) \qquad \left(\frac{\Delta(E)}{\ell}\right) = \left(\frac{v}{\ell}\right) = -1$$

and hence for such a prime ℓ, both $\ell \equiv 1 \pmod 6$ and

$$(4.7) \qquad a_\ell(E) \not\equiv \ell + 1 \pmod 4.$$

In both cases, we therefore obtain inequality (4.4). For the other isogeny classes in the above table, in each case there exists at least one pair of integers (ℓ_0, δ), with $\ell_0 \in \{1, 7, 13, 19\}$ and $\delta \in \{0, 1\}$, such that if

$$(4.8) \qquad \ell \equiv \ell_0 \pmod{24} \quad \text{and} \quad \left(\frac{q}{\ell}\right) = (-1)^\delta,$$

then (4.6) and (4.7) hold. To complete the proof of Theorem 1.4, from (4.4), we require a suitably strong upper bound for the smallest ℓ satisfying (4.8). Such a bound would follow from either a modified version of the arguments traditionally used to find smallest non-residues modulo q (though the additional constraint that $\ell \equiv \ell_0 \pmod{24}$ causes some complications), or from an explicit version of Linnik's theorem on the smallest prime in a given arithmetic progression (see e.g. [17] for an effective but inexplicit result along these lines). For our purposes (and since we require something completely explicit), we will instead appeal to a recent result of the first author, Martin, O'Bryant and Rechnitzer [5]; here, $\theta(x; k, a)$ denotes the sum of the logarithms of the primes $p \equiv a \pmod{k}$ with $p \leq x$.

Theorem 4.1 (B., Martin, O'Bryant and Rechnitzer [5]). *Let k and a be integers with $k \geq 3$ and $\gcd(a, k) = 1$. Then*

$$\left| \theta(x; k, a) - \frac{x}{\phi(k)} \right| < \frac{0.00164\, k}{\phi(k)} \frac{x}{\log x},$$

for all $x \geq x_0(k)$, where

$$(4.9) \qquad x_0(k) = \begin{cases} 7.5 \times 10^7, & \text{if } 3 \leq k \leq 266, \\ 2 \times 10^{10}/k, & \text{if } 267 \leq k \leq 10^5, \\ \exp(0.0442\sqrt{k}\log^3 k), & \text{if } k > 10^5. \end{cases}$$

With this result in hand, we may prove the following

Proposition 4.2. *Let $q \geq 7$ be prime and suppose that $\ell_0 \in \{1, 7, 13, 19\}$ and $\delta \in \{0, 1\}$. Then there exists a prime $\ell \neq q$ satisfying (4.8) with $\ell < e^q$.*

Proof. Given $\ell_0 \in \{1, 7, 13, 19\}$ and $\delta \in \{0, 1\}$, conditions (4.8) are equivalent, via the Chinese Remainder Theorem, to a congruence of the shape $\ell \equiv a \pmod{24q}$ for some integer $7 \leq a < 24q$ with $\gcd(a, 24q) = 1$. For $7 \leq q \leq 17$ and each of the 8 pairs (ℓ_0, δ), we verify by direct computation that we can always find an $\ell < e^q$ with (4.8) (this fails to be true for $q = 5$ and $\ell_0 = \delta = 1$, which is why we have omitted this value). If $q \geq 19$, then $e^q > x_0(24q)$ and hence we may apply Theorem 4.1 to conclude that

$$\left| \theta(e^q; 24q, a) - \frac{e^q}{4(q-1)} \right| < \frac{0.00984\, e^q}{q - 1},$$

whereby

$$\theta(e^q; 24q, a) > \frac{0.24\, e^q}{q - 1} > \log q.$$

It follows that there exists a prime $\ell \equiv a \pmod{24q}$ (which necessarily also satisfies (4.8)) with $\ell \neq q$ and $\ell < e^q$, as desired. $\qquad\square$

If $q = 5$, then, for $\ell_0 \in \{1, 7, 13, 19\}$ and $\delta \in \{0, 1\}$, we can always find an ℓ with (4.8) and $\ell \leq 241$. From (4.4), we thus have

$$p \leq 242 + 2\sqrt{241} < 5^{10}.$$

For $q \geq 7$, we apply Proposition 4.2 to (4.4) to conclude that

$$p < e^q + 1 + 2\sqrt{e^q} = (e^{q/2} + 1)^2 < q^{2q}.$$

This completes the proof of Theorem 1.4.

5. Sets of primes and trivial solutions

5.1. **Intersections of the S_i.** We would like to make a few remarks on the sets S_i. Firstly, we note that some of the S_i overlap substantially. Obviously, primes of the form $(3^b + 1)/4$ belong to both S_6 and S_7, while many primes in S_1 are also in S_4 (taking $d = 1$). Additionally, every prime $q \in S_5$ of the shape $q = 3d^2 + 2^a$ with $a = 2$ or $a \geq 8$, and $d = \pm 3^k$ for k an integer, is necessarily also in S_2.

For many other $i \neq j$, the intersection $S_i \cap S_j$ is rather small. For future use, it will be helpful for us to record an explicit statement along these lines.

Proposition 5.1. *We have*

$$S_1 \cap S_2 = \{5, 7, 11, 13, 23, 31, 37, 73\}, \ S_1 \cap S_3 = \{11\}, \ S_1 \cap S_5 = \{7, 31\},$$
$$S_1 \cap S_7 = \{7, 37, 127\}, \ S_1 \cap S_8 = \{13\}, \ S_2 \cap S_3 = \{11\}, \ S_3 \cap S_4 = \emptyset,$$
$$S_3 \cap S_5 = \{43\}, \ S_3 \cap S_7 = S_3 \cap S_8 = S_4 \cap S_5 = S_5 \cap S_8 = S_7 \cap S_8 = \emptyset.$$

Proof. The desired conclusions for $S_1 \cap S_2$, $S_1 \cap S_3$ and $S_2 \cap S_3$ all follow from combining Theorems 1, 2 and 3 of Tijdeman and Wang [25] with Theorems 3, 4 and 5 of Wang [26]. Further, the fact that

$$S_3 \cap S_4 = S_3 \cap S_8 = S_4 \cap S_5 = S_5 \cap S_8 = \emptyset$$

is immediate from considering the corresponding equations modulo 8.

If $q \in S_1 \cap S_5$, then there exist integers a, b, δ, d and a_5 with $a \in \{2, 3\}$ or $a \geq 5$, $b \geq 0$, $\delta \in \{0, 1\}$, $d \geq 1$ and $a_5 \in \{2, 4\}$ or $a_5 \geq 8$ even, such that $2^a 3^b + (-1)^\delta = 3d^2 + 2^{a_5}$. Modulo 4, we have that $\delta = 1$ and so, modulo 3, $b = 0$. It follows, modulo 8, that $a_5 = 2$, so that $2^a = 3d^2 + 5$. We have

Lemma 5.1. *If x and y are positive integers such that $2^x = 3y^2 + 5$, then*

$$(x, y) \in \{(3, 1), (5, 3), (9, 13)\}.$$

Proof. (of Lemma 5.1) Writing $x = 3x_1 + x_0$ for $x_0 \in \{0, 1, 2\}$, we have that a solution to the equation $2^x = 3y^2 + 5$ necessarily corresponds to an integer point on the (Mordell) elliptic curve $Y^2 = X^3 - 2^{2x_0} \cdot 3^3 \cdot 5$ (with $Y = 2^{x_0} \cdot 3^2 \cdot y$ and $X = 3 \cdot 2^{x_0 + x_1}$). We can find the integer points for each of these curves at `http://www.math.ubc.ca/~bennett/BeGa-data.html` (see [3] for more details), whereby the stated conclusion obtains. $\square$

From this lemma, we therefore have $S_1 \cap S_5 = \{7, 31\}$, as desired. If instead $q \in S_1 \cap S_7$, then we have integers a, b, δ and d, with $a \in \{2, 3\}$ or $a \geq 5$, $b \geq 0$, $\delta \in \{0, 1\}$, $d \geq 1$ and $2^a 3^b + (-1)^\delta = \frac{3d^2 + 1}{4}$. If $b = 0$, then, modulo 3, $\delta = 1$, whence $2^{a+2} = 3d^2 + 5$ and so, from Lemma 5.1, $a \in \{1, 3, 7\}$, corresponding to $q = 7$ and $q = 127$. If $b = 1$, then, again modulo 3, $\delta = 0$ and hence $d^2 = 2^{a+2} 3^{b-1} + 1$. An elementary factoring argument implies that $(a, b, d) = (1, 0, 3), (1, 2, 5)$ or $(2, 2, 7)$, corresponding to $q = 37$.

Suppose next that we have $q \in S_1 \cap S_8$, so that there exist integers a, b, δ, v with $a \in \{2, 3\}$ or $a \geq 5$, $b \geq 0$, $\delta \in \{0, 1\}$ and $2^a 3^b + (-1)^\delta = \frac{3v^2 - 1}{2}$. Modulo 4, $\delta = 0$ and hence $2^{a+1} 3^{b-1} + 1 = v^2$; again via factoring $v^2 - 1$ we find, after a little work, that $|v| = 3$ and $q = 13$. If $q \in S_3 \cap S_5$, there are integers a, d and a_5 with $a \geq 5$ odd, $d \geq 1$, $a_5 \in \{2, 4\}$ or $a_5 \geq 8$ even, and $\frac{2^a + 1}{3} = 3d^2 + 2^{a_5}$. Modulo 8, we have that $a_5 \geq 4$ and so

$$(5.1) \qquad\qquad 9d^2 = 2^a - 3 \cdot 2^{a_5} + 1.$$

We thus have $a \geq a_5 + 3$ and there must exist integers $\delta \in \{0, 1\}$ and positive $d_1 \equiv \pm 1 \pmod 6$ such that $3d = 2^{a_5 - 1} d_1 + (-1)^\delta$, whence

$$2^{a_5 - 2} d_1^2 + (-1)^\delta d_1 = 2^{a - a_5} - 3.$$

If $d_1 = 1$, then $\delta = 0$ and we have $2^{a_5 - 4} + 1 = 2^{a - a_5 - 2}$, so that $a_5 = 4$, $a = 7$, $d = 3$ and $q = 43$. If $d_1 > 1$, then $d_1 \geq 5$ and so $2^{a_5 - 2} 5^2 - 5 \leq 2^{a - a_5} - 3$. It follows that $a \geq 2a_5 + 2$ and hence $2^{a_5 - 2} \mid (-1)^\delta d_1 + 3$, say $(-1)^\delta d_1 + 3 = 2^{a_5 - 2} d_2$, for $d_2 \in \mathbb{Z}$. We thus have

$$2^{2a_5 - 4} d_2^2 - 3 \cdot 2^{a_5 - 1} d_2 + 9 + d_2 = 2^{a - 2a_5 + 2}.$$

Since $a_5 \geq 4$ and $a \geq 2a_5 + 2$, we have that $9 + d_2 \equiv 0 \pmod 8$. If $d_2 = -1$, $2^{2a_5 - 7} + 3 \cdot 2^{a_5 - 4} + 1 = 2^{a - 2a_5 - 1}$, contradicting $a_5 = 4$ or $a_5 \geq 8$. We thus have $d_2 = 7$ or $|d_2| \geq 9$, so that

$$2^{a - 2a_5 + 2} \geq 2^{2a_5 - 4} \cdot 7^2 - 3 \cdot 2^{a_5 - 1} \cdot 7 + 16 > 2^{2a_5 + 1},$$

and so $a \geq 4a_5 + 4$. Applying Corollary 1.7 of [1], since $a \geq 4a_5 + 4 \geq 24$, we have from (5.1) that

$$3 \cdot 2^{a_5} - 1 = \left| 9d^2 - 2^a \right| > 2^{0.26a} \geq 2^{1.04 a_5 + 1.04},$$

whereby $a_5 \leq 13$. A short check confirms that $S_3 \cap S_5 = \{43\}$, as stated.

For $q \in S_3 \cap S_7$, $q = \frac{2^a + 1}{3} = \frac{3d^2 + 1}{4}$ for $a \geq 5$ and d odd integers, so that $2^{a+2} + 1 = 9d^2$ and yet another elementary argument implies that $a = 1$, a contradiction. Let us therefore suppose, finally, that $q \in S_7 \cap S_8$. We thus have

$$4q = 3d^2 + 1 = 6v^2 - 2 = 2u^2 + 2,$$

for integers d, u and v, and so

$$(3dv)^2 = (2u^2 + 1)(u^2 + 2) = 2u^4 + 5u^2 + 2.$$

From Magma's *IntegralQuarticPoints* routine, we find that the only integer solution to the latter equation is with $|dv| = |u| = 1$. This completes the proof of Proposition 5.1. □

It should also be noted that representations within a given set S_i are sometime unique, but not always. In particular, it is straightforward to show that a given prime $q \in S_1$ has a single representation of the form $q = 2^a 3^b \pm 1$, with $b \geq 0$ and $a \in \{2, 3\}$ or $a \geq 5$, while a similar conclusion is immediate for primes $q \in S_i$ for $i \in \{3, 7, 8\}$. The situation in S_2 is slightly more complicated; combining work of Pillai [22] with Stroeker and Tijdeman [23], the only primes with multiple representations of the form $q = |2^a \pm 3^b|$, with $b \geq 1$ and $a \in \{2, 3\}$ or $a \geq 5$, are $q \in \{5, 13, 17, 23, 73\}$, corresponding to the identities

$$5 = 2^3 - 3 = 2^5 - 3^3 = 3^2 - 2^2,$$

$$13 = 2^8 - 3^5 = 2^2 + 3^2,$$

$$17 = 3^4 - 2^6 = 2^3 + 3^2,$$

$$23 = 2^5 - 3^2 = 3^3 - 2^2,$$

and

$$73 = 3^4 - 2^3 = 2^6 + 3^2.$$

5.2. **Limitations due to trivial solutions.** Notice that we have the identity

$$\left(\frac{d+1}{2}\right)^3 + \left(\frac{1-d}{2}\right)^3 = \frac{3d^2+1}{4}$$

and hence, for all exponents n, a coprime integer solution with $C = 1$ to the equation

$$A^3 + B^3 = q^\alpha \cdot C^n, \quad \text{whenever} \quad q^\alpha = \frac{3d^2+1}{4}.$$

We expect q^α to be of this shape infinitely often for $\alpha = 1$ and $\alpha = 2$ (these are precisely the primes in S_7 and S_8, respectively), though both of these results are a long way from provable with current technology.

We will term a solution to (1.2) with $C = 1$ *trivial*, whereby, for primes q as above, there exists a trivial solution for all prime exponents p. In particular, this means that one of the newforms $f \in S_2^+(N_F/\mathcal{R})$ (see Section 2) will correspond (via modularity) to the Frey curve F evaluated at the trivial solution. This is a major obstruction to the modular method; the techniques of this paper are unlikely to provide further information about (1.2) with $\alpha = 1$ for $q \in S_7$ and $\alpha = 2$ for $q \in S_8$.

A similar relation is the identity

$$(d+4)^3 + (4-d)^3 = 8\left(3d^2+16\right).$$

While this does not actually give trivial solutions to (1.2) in case $\alpha = 1$ and $q = 3d^2 + 16$ (a subset of the primes in S_5), it does appear to provide an obstruction to solving (1.4) for such primes, leading to Frey-Hellegouarch curves that play the role of the curve $72A1$ for equation (1.1).

6. Applying the symplectic criteria

Let E and F be elliptic curves over $\mathbb{Q}$ and suppose there exists an isomorphism $\phi : F[p] \to E[p]$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. Here, $F[p]$ and $E[p]$ are the p-torsion modules attached to F and E, respectively. Write $e_{E,p}$ and $e_{F,p}$ for the Weil pairings on $E[p]$ and $F[p]$, respectively. Then there exists an element $r(\phi) \in \mathbb{F}_p^\times$ such that

$$e_{E,p}\left(\phi(P), \phi(Q)\right) = e_{F,p}\left(P, Q\right)^{r(\phi)} \quad \text{for all} \ \ P, Q \in F[p].$$

If $r(\phi)$ is a square in $\mathbb{F}_p^\times$, we call the isomorphism ϕ *symplectic*; if $r(\phi)$ is a non-square, we call it *anti-symplectic*. We say that $E[p]$ and $F[p]$ are *symplectically (anti-symplectically) isomorphic* if there exists a symplectic (anti-symplectic) isomorphism ϕ between them. It is possible that $E[p]$ and $F[p]$ are both symplectically and anti-symplectically isomorphic, but this situation will not occur in the applications of these techniques in this paper.

6.1. **The symplectic argument.** To treat equation (1.2) for certain primes $q \in S_0$ and exponents $p \geq q^{2q}$ we need to use a number of local symplectic criteria to describe the symplectic type of the isomorphisms between the p-torsion modules $E[p]$ and $F[p]$, where F is our Frey-Hellegouarch curve and E is one of the curves in Corollary 3.4 (see Section 2 and Theorem 1.4). The idea is to use local information at different primes ℓ to obtain congruence conditions on the exponent p for which $E[p]$ and $F[p]$ are symplectically and anti-symplectically isomorphic. Then, our desired contradictions will arise each time we are able to prove that these constraints

are incompatible. This is, in essence, what is sometimes called the *symplectic argument*. One advantage we have here, working with equation (1.2) as opposed to equation (1.1), is that we will be able to apply the (local) criteria at the primes $\ell \in \{2, 3, q\}$ rather than just $\ell \in \{2, 3\}$.

6.2. **Notation.** Let ℓ be a prime and, for a nonzero integer t, define $\nu_\ell(t)$ to be the largest nonnegative integer such that $\ell^{\nu_\ell(t)}$ divides t. Let $E/\mathbb{Q}_\ell$ be an elliptic curve and write $c_4(E)$, $c_6(E)$ and $\Delta(E)$ for the usual invariants attached to a minimal model of E. Further, define the quantities $c_4(E)_\ell$, $c_6(E)_\ell$ and $\Delta(E)_\ell$ by

$$c_4(E) = \ell^{\nu_\ell(c_4(E))} c_4(E)_\ell, \ \ c_6(E) = \ell^{\nu_\ell(c_6(E))} c_6(E)_\ell \ \text{ and } \ \Delta(E) = \ell^{\nu_\ell(\Delta(E))} \Delta(E)_\ell.$$

Let $\mathbb{Q}_\ell^{\mathrm{un}}$ to be the maximal unramified extension of $\mathbb{Q}_\ell$. For an elliptic curve $E/\mathbb{Q}$ with potentially good reduction at ℓ we write $e(E, \ell)$ to denote the order of $\mathrm{Gal}(\mathbb{Q}_\ell^{\mathrm{un}}(E[p])/\mathbb{Q}_\ell^{\mathrm{un}})$ for $p \geq 3$ different from ℓ. It is well known that $e(E, \ell)$ is independent of p.

6.3. **The curves.** Except for the few isogeny classes given in Corollary 3.4 by their Cremona label, from Theorem 1.4, we are primarily interested in applying symplectic criteria to our Frey-Hellegouarch curve and the isogeny classes of curves

$$18q.1.a, 18q.2.a, 18q.3.a, 18q.4.a \text{ (with } \delta_1 = \delta_2 = 0, a \text{ even}, b \text{ odd)}, 18.q.5.a \text{ and}$$
$$18q.5.b \text{ (with, in both cases, } \delta_1 = \delta_2 = 0 \text{ and } a \text{ even)}, 36q.1.a, 36q.1.b, 36q.2.a,$$
$$36q.2.b, 36q.3.a, 72q.1.a, 72q.2.a, 72q.3.a, 72q.4.a, 72q.4.b, 72.q.5.a \text{ and } 72q.5.b$$
$$\text{(with, in both cases, } \delta = 0 \text{ and } a = 4), 72q.6.a, 72q.6.b, 72q.7.a, 72q.8.a$$
$$\text{and } 72q.9.a \text{ (with } \delta_1 = \delta_2 = 0, a = 4, b \text{ odd)}.$$

The relevant arithmetic data $c_4(E)$, $c_6(E)$ and $\Delta(E)$ is available in our Appendix and in the statements of Theorems 3.1, 3.2 and 3.3. In the remainder of this section we will apply the criteria to the curves listed above to obtain congruence conditions on p. Then, in Section 7, we complete the symplectic argument by deriving contradictions from these conditions, allowing us to finish the proofs of our main Diophantine statements. We start by proving the following proposition which holds for all our choices of E, independent of whether E has conductor $N_E = 18q$, $36q$ or $72q$.

Proposition 6.1. *Let (A, B, C) be a non-trivial primitive solution to (1.2) so that there is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules isomorphism $\phi : F[p] \to E[p]$, where F is the Frey-Hellegouarch curve and E is any elliptic curve in one of the isogeny classes above. Then*

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad \alpha \text{ is a square mod } p.$$

Proof. We have $\nu_q(N_F) = \nu_q(N_E) = 1$, so q is a prime of multiplicative reduction of both curves. We can always choose E such that $\nu_q(\Delta(E)) = 2$; moreover, we have $p \nmid \alpha$ and $\nu_q(\Delta(F)) = 2\alpha + 2p\nu_q(C)$. The conclusion now follows from a direct application of [20, Proposition 2] with the prime q. □

6.4. **Curves of conductor** $18q$**.** We summarize the necessary information about the invariants of the relevant elliptic curves.

Curve	$\nu_2(c_4)$	$\nu_2(c_6)$	$\nu_2(\Delta)$	$\nu_3(c_4)$	$\nu_3(c_6)$	$\nu_3(\Delta)$
$F_{A,B}^{(0)}$	0	0	$2p\nu_2(C) - 8$	$2 + \nu_3(AB)$	$3 + \nu_3(A^3 - B^3)$	$2p\nu_3(C) + 3$
$18q.1.a1\ (b = 0)$	0	0	$2a - 8$	3	≥ 7	6
$18q.1.a1\ (b \geq 1)$	0	0	$2a - 8$	2	3	$2b + 6$
$18q.2.a1$	0	0	$2a - 8$	2	3	8
$18q.3.a1$	0	0	$2a - 8$	2	3	$2b + 6$
$18q.4.a2$	0	0	$a - 6$	2	3	$b + 6$
$18q.5.a2$	0	0	$a - 6$	2	$3 + \nu_3(d)$	3
$18q.5.b2$	0	0	$a - 6$	4	$6 + \nu_3(d)$	9

Suppose (A, B, C) is a non-trivial primitive solution to (1.2) and the Frey-Hellegouarch curve F satisfies isomorphism (2.2) where f is the newform corresponding to one of the isogeny classes

$$18q.1.a, 18q.2.a, 18q.3.a, 18q.4.a, 18q.5.a \text{ or } 18q.5.b.$$

In particular, $F = F_{A,B}^{(0)}$, C is even and $B \equiv -1 \pmod 4$. Moreover, there is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules isomorphism $\phi : F[p] \to E[p]$, where E is one of the elliptic curves

$$18q.1.a1, 18q.2.a1, 18q.3.a1, 18q.4.a2, 18q.5.a2 \text{ or } 18q.5.b2.$$

6.4.1. *Applying the criteria at $\ell = 2$.* Since $\nu_2(N_E) = 1$ the prime $\ell = 2$ is of multiplicative reduction for E. From [20, Proposition 2] and the valuations given in the preceding table, it follows that either $p \nmid a - 4$ and

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad 4 - a \text{ is a square mod } p,$$

in case $E = 18q.1.a1, 18q.2.a1$ or $18q.3.a1$, or that $p \nmid a - 6$ and

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad 12 - 2a \text{ is a square mod } p,$$

in the other cases.

6.4.2. *Applying the criteria at $\ell = 3$.* We first consider E one of $18q.1.a1$ with $b = 0$, $18q.5.a2$ or $18q.5.b2$. We have that the corresponding j-invariant satisfies $\nu_3(j_E) > 0$, and hence E has potentially good reduction at 3. Indeed, for $E = 18q.1.a1$ (with $b = 0$), we have $\nu_3(\Delta(E)) = 6$ and $\nu_3(c_6(E)) \geq 7$ so that, from [18, p. 356], we conclude that $e(E, 3) = 2$.

For $E = 18q.5.a2$ and $E = 18q.5.b2$, we have $\nu_3(\Delta(E)) \in \{3, 9\}$ and the results of [18, p. 356] imply that $e(E, 3) \in \{4, 12\}$; furthermore, since $\nu_3(N_E) = 2$ we are in a case of tame reduction, whence $e(E, 3) = 4$. On the other hand, for our Frey-Hellegouarch curve F to have potentially good reduction at 3, we require that $3\nu_3(c_4(F)) \geq \nu_3(\Delta(F))$, or, equivalently, $\nu_3(C) = 0$. In this situation, $\nu_3(\Delta(F)) = 3$ and arguing exactly as for the previous curves we also conclude that $e(F, 3) = 4$. This contradicts $e(E, 3) = 2$, and hence $E \neq 18q.1.a1$ (with $b = 0$). We will now apply [14, Theorem 1] with F and $E = 18q.5.a2$ or $18q.5.b2$ (with, in both cases, $\delta_1 = \delta_2 = 0$ and a even). Let r and t be the quantities defined in the statement of that theorem. We have, since $3 \nmid C$,

$$\nu_3(\Delta(F)) = \nu_3(\Delta(18q.5.a2)) = 3 \text{ and } \nu_3(\Delta(18q.5.b2)) = 9,$$

whereby $r = 0$ if $E = 18q.5.a2$ and $r = 1$ if $E = 18q.5.b2$. Moreover, since $3 \nmid C$ and a is even, we may check that $\Delta(F)_3 \equiv \Delta(E)_3 \equiv 2$ (mod 3), i.e. $t = 0$ for both E. Finally, applying [14, Theorem 1], we conclude that ϕ is symplectic when $E = 18q.5.a2$ and, if $E = 18q.5.b2$, then ϕ is symplectic if and only if $(3/p) = 1$.

We now consider the remaining curves E of conductor $18q$ under consideration. We have, in all cases,

$$\nu_3(c_4(E)) = 2, \quad \nu_3(c_6(E)) = 3, \quad \nu_3(\Delta(E)) \geq 7 \ \text{ and } \ \nu_3(j_E) < 0,$$

and hence E has potentially multiplicative reduction at 3; after a quadratic twist (with corresponding elliptic curve denoted E_t) the reduction becomes multiplicative and we have

$$\nu_3(\Delta(E_t)) = \begin{cases} 2 \text{ if } E = 18q.2.a1, \\ b \text{ if } E = 18q.4.a2 \text{ (with } b \geq 1), \\ 2b \text{ if } E = 18q.1.a1 \text{ (and } b \geq 1) \text{ or } E = 18q.3.a1. \end{cases}$$

Furthermore, 3 must divide C (since otherwise F would have potentially good reduction) and twisting the Frey curve F by the same element (to obtain F_t), we find that $\nu_3(\Delta(F_t)) = -3 + 2p\nu_3(C)$.

If $E = 18q.1.a1$ with $b \geq 1$ or $E = 18q.3.a1$, it follows from [20, Proposition 2] applied to E_t and F_t that $p \nmid b$ and

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad -6b \text{ is a square mod } p.$$

Similarly, if $E = 18q.4.a2$ then $p \nmid b$ and

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad -3b \text{ is a square mod } p.$$

If $E = 18q.2.a1$, then

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad -6 \text{ is a square mod } p.$$

6.4.3. *Conclusions for level* $18q$. From the calculations above and Proposition 6.1 we can extract the following relations. If $E = 18q.1.a1$ or $18.3.a1$ then $b \geq 1$ and

$$(6.1) \qquad \left(\frac{4-a}{p}\right) = \left(\frac{\alpha}{p}\right) = \left(\frac{-6b}{p}\right),$$

while if $E = 18.4.a2$ or $E = 18q.2.a1$, then, respectively,

$$\left(\frac{12-2a}{p}\right) = \left(\frac{\alpha}{p}\right) = \left(\frac{-3b}{p}\right) \quad \text{or} \quad \left(\frac{4-a}{p}\right) = \left(\frac{\alpha}{p}\right) = \left(\frac{-6}{p}\right).$$

If $E = 18.5.a2$, we have that

$$\left(\frac{12-2a}{p}\right) = \left(\frac{\alpha}{p}\right) = 1.$$

6.5. **Curves of conductor** $36q$**.** We next proceed with the case of elliptic curves of conductor $36q$. We encounter the following invariants.

Curve	$\nu_2(c_4)$	$\nu_2(c_6)$	$\nu_2(\Delta)$	$\nu_3(c_4)$	$\nu_3(c_6)$	$\nu_3(\Delta)$
$F_{A,B}^{(1)}$	$4 + \nu_2(A)$	5	4	$2 + \nu_3(AB)$	$3 + \nu_3(A^3 - B^3)$	$2p\nu_3(C) + 3$
$36q.1.a2\,(3 \mid s)$	4	6	8	2	$4 + \nu_3(v)$	3
$36q.1.a2\,(3 \nmid s)$	4	6	8	2	3	3
$36q.1.b2\,(3 \mid s)$	4	6	8	4	$7 + \nu_3(v)$	9
$36q.1.b2\,(3 \nmid s)$	4	6	8	4	6	9
$36q.2.a1\,(3 \mid d)$	≥ 6	5	4	2	$4 + \nu_3(d)$	3
$36q.2.a1\,(3 \nmid d)$	≥ 6	5	4	≥ 3	3	3
$36q.2.b1\,(3 \mid d)$	≥ 6	5	4	4	$7 + \nu_3(d)$	9
$36q.2.b1\,(3 \nmid d)$	≥ 6	5	4	≥ 5	6	9
$36q.3.a1$	≥ 6	5	4	2	3	$b + 6$

Suppose (A, B, C) is a non-trivial primitive solution to (1.2) and the Frey-Hellegouarch curve F satisfies isomorphism (2.2) where f is the newform corresponding to one of the isogeny classes

$$36q.1.a, 36q.1.b, 36q.2.a, 36q.2.b \ \text{ or } \ 36q.3.a.$$

In particular, $F = F_{A,B}^{(1)}$, C is odd and $B \equiv 1 \pmod 4$. Moreover, there is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules isomorphism $\phi : F[p] \to E[p]$, where E is one of the elliptic curves

$$36q.1.a2, \ 36q.1.b2, \ 36q.2.a1, \ 36q.2.b1 \ \text{ or } \ 36q.3.a1.$$

6.5.1. *Applying the criteria at $\ell = 2$.* The table shows that $\nu_2(j(E)) > 0$ for all E, so that the curves have potentially good reduction. Since $\nu_2(N_E) = 2$ the reduction is tame and hence $e(E, 2) = 3$ for all E.

We will now apply [13, Theorem 1] at $\ell = 2$ with F and $E = 36q.1.a2$ or $36q.1.b2$. Let t and r be as in that theorem. Since $\nu_2(\Delta(F)) = 4$ and $\nu_2(\Delta(E)) = 8$, we have $r = 1$ for both E. Now, to determine the value of t, we must first appeal to [13, Theorem 3]. Indeed, the curve $36q.1.a2$ has

$$c_4(E)_2 = 3\left(16\left(\frac{3v^2 - 1}{2}\right)^2 - 1\right) \ \text{ and } \ c_6(E)_2 = -3^2 uv\left(32\left(\frac{3v^2 - 1}{2}\right)^2 + 1\right),$$

while for $36q.1.b2$,

$$c_4(E)_2 = 3^3\left(16\left(\frac{3v^2 - 1}{2}\right)^2 - 1\right) \ \text{ and } \ c_6(E)_2 = 3^5 uv\left(32\left(\frac{3v^2 - 1}{2}\right)^2 + 1\right).$$

We thus have, respectively,

$$c_4(E)_2 \equiv 13 \pmod{32} \ \text{ and } \ c_6(E)_2 \equiv 7uv \pmod{16},$$

and

$$c_4(E)_2 \equiv 21 \pmod{32} \ \text{ and } \ c_6(E)_2 \equiv 3uv \pmod{16}.$$

Since $u^2 - 3v^2 = -2$ with $u \equiv v \equiv 1 \pmod 4$, the u and v are terms in binary recurrence sequences and we may readily prove by induction that $uv \equiv 1 \pmod{16}$,

whereby it follows from [13, Theorem 3] that the curve $36q.1.a2$ has a 3-torsion point over $\mathbb{Q}_2$, while $36q.1.b2$ does not. For $F = F_{A,B}^{(1)}$, since $\nu_2(A) \geq 2$, we have

$$\nu_2(c_4(F)) \geq 6 \quad \text{and} \quad c_6(F)_2 = 3^3(A^3 - B^3) \equiv -3B \pmod{8},$$

whereby, from part (B2) of [13, Theorem 3], F has a 3-torsion point over $\mathbb{Q}_2$ precisely when we have $B \equiv 1 \pmod 8$. We thus conclude that, if $B \equiv 1 \pmod 8$ and $E = 36q.1.a2$ or $B \equiv 5 \pmod 8$ and $E = 36q.1.b2$, then $t = 0$ and

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad 2 \text{ is a square mod } p.$$

If $B \equiv 5 \pmod 8$ and $E = 36q.1.a2$, or $B \equiv 1 \pmod 8$ and $E = 36q.1.b2$, then $t = r = 1$ and so

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right).$$

Next, suppose that E is one of $36q.2.a1, 36q.2.b1$ or $36q.3.a1$, so that we always have $r = 0$. Then

$$c_6(E)_2 = -3^3 d \frac{(d^2 + 3)}{4} \equiv \begin{cases} 5 \pmod 8 \text{ if } d \equiv 1 \pmod{16}, \\ 1 \pmod 8 \text{ if } d \equiv 9 \pmod{16}, \end{cases}$$

$$c_6(E)_2 = 3^6 d \frac{(d^2 + 3)}{4} \equiv \begin{cases} 5 \pmod 8 \text{ if } d \equiv 9 \pmod{16}, \\ 1 \pmod 8 \text{ if } d \equiv 1 \pmod{16}, \end{cases}$$

and

$$c_6(E)_2 = -3^3 d \frac{(d^2 + 3^{b+2})}{4} \equiv \begin{cases} 5 \pmod 8 \text{ if } q \equiv d + 2 \pmod 8, \\ 1 \pmod 8 \text{ if } q \equiv d - 2 \pmod 8, \end{cases}$$

respectively. If any of

$$B \equiv 1 \pmod 8, \quad E = 36q.2.a1 \quad \text{and} \quad d \equiv 1 \pmod{16}, \text{ or}$$
$$B \equiv 5 \pmod 8, \quad E = 36q.2.a1 \quad \text{and} \quad d \equiv 9 \pmod{16}, \text{ or}$$
$$B \equiv 1 \pmod 8, \quad E = 36q.2.b1 \quad \text{and} \quad d \equiv 9 \pmod{16}, \text{ or}$$
$$B \equiv 5 \pmod 8, \quad E = 36q.2.b1 \quad \text{and} \quad d \equiv 1 \pmod{16}, \text{ or}$$
$$B \equiv 1 \pmod 8, \quad E = 36q.3.a1 \quad \text{and} \quad q \equiv d + 2 \pmod 8, \text{ or}$$
$$B \equiv 5 \pmod 8, \quad E = 36q.3.a1 \quad \text{and} \quad q \equiv d - 2 \pmod 8,$$

we therefore have that ϕ is always symplectic. If, however,

$$B \equiv 1 \pmod 8, \quad E = 36q.2.a1 \quad \text{and} \quad d \equiv 9 \pmod{16}, \text{ or}$$
$$B \equiv 5 \pmod 8, \quad E = 36q.2.a1 \quad \text{and} \quad d \equiv 1 \pmod{16}, \text{ or}$$
$$B \equiv 1 \pmod 8, \quad E = 36q.2.b1 \quad \text{and} \quad d \equiv 1 \pmod{16}, \text{ or}$$
$$B \equiv 5 \pmod 8, \quad E = 36q.2.b1 \quad \text{and} \quad d \equiv 9 \pmod{16}, \text{ or}$$
$$B \equiv 1 \pmod 8, \quad E = 36q.3.a1 \quad \text{and} \quad q \equiv d - 2 \pmod 8, \text{ or}$$
$$B \equiv 5 \pmod 8, \quad E = 36q.3.a1 \quad \text{and} \quad q \equiv d + 2 \pmod 8,$$

then

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad 3 \text{ is a square mod } p.$$

6.5.2. *Applying the criteria at $\ell = 3$.* For $E = 36q.3.a1$, we have $\nu_3(j(E)) < 0$ and so E has potentially multiplicative reduction at 3. After a suitable quadratic twist (denoted E_t) the reduction becomes multiplicative and $\nu_3(\Delta(E_t)) = b$. Therefore, the twisted Frey curve F_t must also have multiplicative reduction at 3 (since $p \geq 5$) and it satisfies $\nu_3(\Delta(F_t)) = 2p\nu_3(C) - 3$. Since $p \nmid \nu_3(\Delta(F_t))$, it follows from [20, Proposition 2] that $p \nmid b$ and

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad -3b \text{ is a square mod } p.$$

For all other cases of E we have $\nu_3(j(E)) \geq 0$ and $\nu_3(\Delta(E)) \neq 6$, whence E has potentially good reduction which does not become good after a quadratic twist. As before, since $\nu_3(N_E) = 2$ the reduction is tame, whereby $e(E, 3) = 4$. A similar argument guarantees that $e(F, 3) = 4$ when $3 \nmid C$, in which case, $\nu_3(\Delta(F)) = 3$ and $\Delta(F)_3 \equiv 2 \pmod 3$. To apply [14, Theorem 1] at $\ell = 3$ with F and each of the curves $E = 36q.1.a2, 36q.1.b2, 36q.2.a1$ or $36q.2.b1$, we first compute that $(r, t) = (0, 1), (1, 1), (0, 0)$ and $(1, 0)$, respectively. We conclude that if $E = 36q.2.a1$ then ϕ is symplectic, while, if $E = 36q.1.a2$,

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad 2 \text{ is a square mod } p.$$

If $E = 36q.1.b2$, then

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right)$$

and if $E = 36q.2.b1$, then

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad 3 \text{ is a square mod } p.$$

6.5.3. *Conclusions for level $36q$.* From the calculations above and Proposition 6.1 we can extract the following relations. If $E = 36q.1.a2$ and $B \equiv 1 \pmod 8$, we have

$$\left(\frac{\alpha}{p}\right) = \left(\frac{2}{p}\right)$$

while $E = 36q.1.a2$ and $B \equiv 5 \pmod 8$ implies that either

$$\left(\frac{\alpha}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1, \quad \text{or} \quad \left(\frac{\alpha}{p}\right) = \left(\frac{2}{p}\right) = -1, \left(\frac{3}{p}\right) = 1.$$

If $E = 36q.1.b2$ and $B \equiv 1 \pmod 8$, we have either

$$\left(\frac{\alpha}{p}\right) = 1, \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right), \quad \text{or} \quad \left(\frac{\alpha}{p}\right) = -1, \left(\frac{2}{p}\right) \neq \left(\frac{3}{p}\right).$$

If $E = 36q.1.b2$ and $B \equiv 5 \pmod 8$, we either have

$$\left(\frac{\alpha}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = 1 \quad \text{or} \quad \left(\frac{\alpha}{p}\right) = \left(\frac{2}{p}\right) = -1, \left(\frac{3}{p}\right) = 1.$$

If $E = 36q.2.a1$ and either $B \equiv 1 \pmod 8$, $d \equiv 1 \pmod{16}$, or $B \equiv 5 \pmod 8$, $d \equiv 9 \pmod{16}$, we have

$$\left(\frac{\alpha}{p}\right) = 1.$$

If $E = 36q.2.a1$ and either $B \equiv 1 \pmod 8$, $d \equiv 9 \pmod{16}$, or $B \equiv 5 \pmod 8$, $d \equiv 1 \pmod{16}$, we have

$$\left(\frac{\alpha}{p}\right) = \left(\frac{3}{p}\right) = 1.$$

If $E = 36q.2.b1$ and either $B \equiv 1 \pmod 8$, $d \equiv 9 \pmod{16}$, or $B \equiv 5 \pmod 8$, $d \equiv 1 \pmod{16}$, we have, again,

$$\left(\frac{\alpha}{p}\right) = \left(\frac{3}{p}\right) = 1,$$

while, if $E = 36q.2.b1$ and either $B \equiv 1 \pmod 8$, $d \equiv 1 \pmod{16}$, or $B \equiv 5 \pmod 8$, $d \equiv 9 \pmod{16}$, we have

$$\left(\frac{\alpha}{p}\right) = \left(\frac{3}{p}\right) = 1.$$

If $E = 36q.3.a1$ and either $B \equiv 1 \pmod 8$, $q \equiv d + 2 \pmod 8$, or $B \equiv 5 \pmod 8$, $q \equiv d - 2 \pmod 8$, we have

$$\left(\frac{\alpha}{p}\right) = \left(\frac{-3b}{p}\right) = 1,$$

while, if $E = 36q.3.a1$ and either $B \equiv 1 \pmod 8$, $q \equiv d - 2 \pmod 8$, or $B \equiv 5 \pmod 8$, $q \equiv d + 2 \pmod 8$, we have that

$$\left(\frac{\alpha}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{-3b}{p}\right).$$

6.6. **Curves of conductor** $72q$. We have the following data.

Curve	$\nu_2(c_4)$	$\nu_2(c_6)$	$\nu_2(\Delta)$	$\nu_3(c_4)$	$\nu_3(c_6)$	$\nu_3(\Delta)$
$F_{A,B}^{(1)}$	5	5	4	$2 + \nu_3(AB)$	$3 + \nu_3(A^3 - B^3)$	$2p\nu_3(C) + 3$
$72q.1.a1$	4	6	8	2	3	$2b + 6$
$72q.2.a1$	4	6	8 or 10	2	3	$2b + 6$
$72q.3.a1$	4	6	8 or 10	2	3	$2b + 6$
$72q.4.a2\ (3 \mid d)$	4	6	8	2	$4 + \nu_3(d)$	3
$72q.4.a2\ (3 \nmid d)$	4	6	8	≥ 3	3	3
$72q.4.b2\ (3 \mid d)$	4	6	8	4	$7 + \nu_3(d)$	9
$72q.4.b2\ (3 \nmid d)$	4	6	8	≥ 5	6	9
$72q.5.a2\ (3 \mid d)$	4	6	10	2	$4 + \nu_3(d)$	3
$72q.5.a2\ (3 \nmid d)$	4	6	10	≥ 3	3	3
$72q.5.b2\ (3 \mid d)$	4	6	10	4	$7 + \nu_3(d)$	9
$72q.5.b2\ (3 \nmid d)$	4	6	10	≥ 5	6	9
$72q.6.a1\ (3 \mid d)$	5	5	4	2	$4 + \nu_3(d)$	3
$72q.6.a1\ (3 \nmid d)$	5	5	4	≥ 3	3	3
$72q.6.b1\ (3 \mid d)$	5	5	4	4	$7 + \nu_3(d)$	9
$72q.6.b1\ (3 \nmid d)$	5	5	4	≥ 5	6	9
$72q.7.a1$	5	5	4	2	3	$b + 6$
$72q.8.a2$	4	6	8	2	3	$b + 6$
$72q.9.a2$	4	6	10	2	3	$b + 6$

Suppose (A, B, C) is a non-trivial primitive solution to (1.2) and the Frey-Hellegouarch curve F satisfies isomorphism (2.2) where f is the newform corresponding to one of the isogeny classes

$$72q.1.a, 72q.2.a, 72q.3.a, 72q.4.a, 72q.4.b, 72q.5.a, 72q.5.b,$$
$$72q.6.a, 72q.6.b, 72q.7.a, 72q.8.a \text{ or } 72q.9.a.$$

In particular, for this case we have $F = F_{A,B}^{(1)}$,

$$C \text{ is odd}, \qquad A \equiv 2 \pmod 4 \quad \text{and} \quad B \equiv 1 \pmod 4,$$

and there is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module isomorphism

$$\phi \ : \ F[p] \to E[p],$$

where E is one of the elliptic curves labelled

$$72q.1.a1, 72q.2.a1, 72q.3.a1, 72q.4.a2, 72q.4.b2, 72q.5.a2, 72q.5.b2,$$
$$72q.6.a1, 72q.6.b1, 72q.7.a1, 72q.8.a2 \text{ or } 72q.9.a2.$$

6.6.1. *Applying the criteria at $\ell = 2$.* Note that all the curves in the preceding table have potentially good reduction at $\ell = 2$ since their j-invariants satisfy $\nu_2(j) \geq 0$. We see, from [18, p. 358], that the Frey curve F satisfies $e(F, 2) = 24$; the same is immediately seen to be true also for E satisfying

$$(\nu_2(c_4(E)), \nu_2(c_6(E)), \nu_2(\Delta(E))) \in \{(4, 6, 10), (5, 5, 4)\}.$$

For the curves E in the table with

$$(\nu_2(c_4(E)), \nu_2(c_6(E)), \nu_2(\Delta(E))) = (4, 6, 8),$$

we further check that $\Delta(E)_2 \equiv 1 \pmod 4$ and hence we also have $e(E, 2) = 24$. We may therefore, in all cases, apply [12, Theorem 4] to find that, if $\nu_2(\Delta(E)) \in \{4, 10\}$, then ϕ is always symplectic, while, if $\nu_2(\Delta(E)) = 8$, then

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad 2 \text{ is a square mod } p.$$

6.6.2. *Applying the criteria at $\ell = 3$.* If $E = 72q.1.a1, 72q.2.a1, 72q.3.a1, 72q.7.a1$, $72q.8.a2$ or $72q.9.a2$, then E has potentially multiplicative reduction at 3 and so, after a suitable quadratic twist (denoted E_t) the reduction becomes multiplicative and $\nu_3(\Delta(E_t)) = b$ or $2b$. Therefore, $3 \mid C$ and the twisted Frey curve F_t must also have multiplicative reduction at 3 and satisfy $\nu_3(\Delta(F_t)) = 2p\nu_3(C) - 3$. Since $p \nmid \nu_3(\Delta(F_t))$, it follows from [20, Proposition 2] that $p \nmid b$ and

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad -3b \text{ is a square mod } p,$$

for $E = 72q.7.a1, 72q.8.a2$ and $72q.9.a2$, while

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad -6b \text{ is a square mod } p,$$

for $E = 72q.1.a1, 72q.2.a1$, and $72q.3.a1$.

For the curves $E = 72q.4.a2, 72q.4.b2, 72q.5.a2, 72q.5.b2, 72q.6.a1$ or $72q.6.b1$, the reduction at $\ell = 3$ is potentially good and tame (because $\nu_3(N_E) = 2$) and since $\nu_3(\Delta(E)) \neq 6$ we have $e(E, 3) = 4$. As before, it follows that $e(F, 3) = 4$ (so that $3 \nmid C$), and we may apply [14, Theorem 1]. Let r and t be as in that theorem. In all cases we have $t = 0$; furthermore, we have $r = 0$ for $E = 72q.4.a2$, $E = 72q.5.a2$

or $E = 72q.6.a1$, and $r = 1$ for $E = 72q.4.b2$, $E = 72q.5.b2$ or $E = 72q.6.b1$. It follows that ϕ is always symplectic in the first cases, while

$$\phi \text{ is symplectic} \quad \Longleftrightarrow \quad 3 \text{ is a square mod } p,$$

in the latter three.

6.6.3. *Conclusions for level* $72q$. From the calculations above we extract the following relations. For $E = 72q.1.a1$, or either of $E = 72q.2.a1$ or $E = 72q.3.a1$ with $a = 2$, it follows that

$$\left(\frac{\alpha}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{-6b}{p}\right),$$

while, for $E = 72q.2.a1$ or $E = 72q.3.a1$ with $a = 3$,

$$\left(\frac{\alpha}{p}\right) = \left(\frac{-6b}{p}\right) = 1.$$

If $E = 72q.4.a2$, we have

$$\left(\frac{\alpha}{p}\right) = \left(\frac{2}{p}\right) = 1,$$

while $E = 72q.5.a2$ or $E = 72q.6.a1$ give

$$\left(\frac{\alpha}{p}\right) = 1.$$

Taking $E = 72q.4.b2$ yields

$$\left(\frac{\alpha}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right),$$

while $E = 72q.5.b2$ or $E = 72q.6.b1$ give

$$\left(\frac{\alpha}{p}\right) = \left(\frac{3}{p}\right) = 1.$$

If $E = 72q.7.a1$ or $72q.9.a2$, we have

$$\left(\frac{\alpha}{p}\right) = \left(\frac{-3b}{p}\right) = 1.$$

Finally, if $E = 72q.8.a2$,

$$\left(\frac{\alpha}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{-3b}{p}\right).$$

7. Some applications of symplectic criteria

As the preceding section reveals, there are many results we could state now for the various families of primes S_i comprising the set S_0. For simplicity, we limit ourselves to the three statements we have mentioned in our introduction (Theorems 1.7, 1.8 and 1.9) and one result valid for small values of q (Theorem 7.1).

7.1. **Proof of Theorem 1.7.** If $q \notin S_0$, the desired conclusion is immediate from Theorem 1.4. Suppose, then, that $q \in S_0 \setminus T$ and that there exists a solution to (1.4) in coprime nonzero integers A, B and C and prime $p \geq q^{2q}$. In particular, we note, without further mention, that the primes p under consideration all satisfy $\gcd(p, 6q) = 1$. Also, we have that $p \nmid (4-a)b$, whenever these parameters appear in the sequel. From Section 2 and Theorem 1.4, it follows there exists an isomorphism $\phi : F[p] \rightarrow E[p]$, where F is the Frey-Hellegouarch curve and E is one of the curves in Corollary 3.4. Since $\alpha = 1$, we see from Proposition 6.1 that ϕ is symplectic. Furthermore, the shape of the primes in S_7 implies that $7, 19 \in S_7$ and E does not correspond to the isogeny classes $36.q.2.a$, $36.q.2.b$, $72.q.5.a$ or $72.q.5.b$. In conclusion, we need to consider E in the remaining conjugacy classes; in particular, we can either take E isogenous to one of

$$90c, \ 306c, \ 360a, \ 360d, \ 936d \ \text{ or } \ 5256e,$$

whereby $q \in \{5, 13, 17, 73\}$, or E isomorphic to one of the following curves:

$$18q.1.a1, 18q.2.a1, 18q.3.a1, 18q.4.a2 \ (\text{with } \delta_1 = \delta_2 = 0, a \text{ even}, b \text{ odd}), 18.q.5.a2 \text{ or}$$
$$18q.5.b2 \ (\text{with, in both cases}, \delta_1 = \delta_2 = 0 \text{ and } a \text{ even}), 36q.1.a2, 36q.1.b2, 36q.3.a1,$$
$$72q.1.a1, 72q.2.a1, 72q.3.a1, 72q.4.a2, 72q.4.b2, 72q.7.a1, 72q.8.a2 \text{ or}$$
$$72q.9.a2 \ (\text{with } \delta_1 = \delta_2 = 0, a = 4).$$

For $q \leq 73$, the desired conclusion will follow immediately from our Theorem 7.1, which we will prove later in this section. For the remaining possible types for q, we will place a number of conditions upon p to guarantee that, in each case, ϕ is anti-symplectic, providing the desired contradiction. These conditions will be of the form $\left(\frac{\kappa_i}{p}\right) = -1$, for, in each case, a finite collection of integers κ_i, and hence are each equivalent to p lying in certain residue classes modulo $8|\kappa_i|$. We remind the reader that a given prime q has at most finitely many (isogeny classes of) curves E associated to it. This will prove Theorem 1.7 provided we can show that these conditions are compatible, i.e. that we do not have three distinct indices i, say $i = 1, 2$ and 3, with $\kappa_1 \kappa_2 \kappa_3$ an integer square. In particular, compatibility is immediate if we have κ_i negative for each i. Our goal will be to show that, for a given prime in $q \in S_0 \setminus T$, we can always find a corresponding set of κ_i with either
    (i) κ_i negative for all i, or
    (ii) κ_i either positive and $\kappa_i \equiv 2 \pmod 4$, or κ_i negative and odd, or
    (iii) $\kappa_i \equiv 2 \pmod 4$ for all i.
  Combining the conclusions of subsections 6.4.3, 6.5.3 and 6.6.3, we can choose κ_i for which we require $\left(\frac{\kappa_i}{p}\right) = -1$, to contradict the fact that ϕ is symplectic, as

follows.

E	κ_i	E	κ_i
$18q.1.a1$	$4 - a$ or $-6b$	$72q.1.a1$	2 or $-6b$
$18q.2.a1$	$4 - a$ or -6	$72q.2.a1$	$-6b$
$18q.3.a1$	$4 - a$ or $-6b$	$72q.3.a1$	$-6b$
$18q.4.a2$	$12 - 2a$ or $-3b$	$72q.4.a2$	2
$18q.5.a2$	$12 - 2a$	$72q.4.b2$	2 or 3
$18q.5.b2$	$12 - 2a$	$72q.7.a1$	$-3b$
$36q.1.a2$	2	$72q.8.a2$	2 or $-3b$
$36q.1.b2$	6	$72q.9.a2$	$-3b$
$36q.3.a1$	$-3b$		

Here, the integers a and b are as given in the definitions of the curves E in Section 3. It is important to remember that, for a given q and corresponding type of curve E, we have not ruled out the possibility of there being more than one non-isogenous curve involved. As example (3.1) illustrates, there can certainly be non-isogenous curves associated to a fixed pair (q, E); in the case of (3.1), neither curve of the shape $E = 18q.4.a$ satisfies $a \equiv 0 \pmod 2, b \equiv 1 \pmod 2$.

From the preceding table, the only cases where we cannot choose κ_i to be negative are the primes q corresponding to $E = 36q.1.a2, 36q.1.b2, 72q.4.a2$ or $72q.4.b2$. The first two of these require $q \in S_8$, while the latter two arise from $q \in S_5$ of the form $q = 3d^2 + 4$ for integer d. In each of these cases, we can choose $\kappa_i \equiv 2 \pmod 4$ positive (see the table above).

To conclude the proof of Theorem 1.7, we need to show that for each q which can possibly correspond to any of

$$E \in E_0 = \{36q.1.a2, \ 36q.1.b2, \ 72q.4.a2 \ 72q.4.b2\},$$

if we have a solution to (1.4) that is associated to some $E \notin E_0$, then we can eliminate a positive proportion of prime exponent p by requiring that $\left(\frac{\kappa_i}{p}\right) = -1$ for κ_i either positive and $\kappa_i \equiv 2 \pmod 4$, or κ_i negative and odd (as in case (ii) of the preceding page), or all $\kappa_i \equiv 2 \pmod 4$ (as in case (iii)). In particular, we need to start by understanding $S_8 \cap S_i$ and $\{q \text{ prime} : q = 3d^2 + 4\} \cap S_i$; Proposition 5.1 is a good place to begin.

Suppose first that $q \in S_5$ and $q = 3d^2 + 4$ for an odd integer d. Modulo 8, we cannot have $q = 3d_1^2 + 2^\alpha$ for integer d_1 and $\alpha \geq 4$. Further, applying Proposition 5.1, we have that $q \notin S_i$ for each $i \in \{1, 3, 4, 8\}$. Since $q \in S_0 \setminus T$, we have that $q \notin S_7$. If $q \in S_2$, then $q = (-1)^{\delta_1} 2^{a_2} + (-1)^{\delta_2} 3^{b_2}$, for $a_2 \in \{2, 3\}$ or $a_2 \geq 5$, and $b_2 \geq 1$. Modulo 3, $\delta_1 \equiv a_2 \pmod 2$, while, modulo 8, either $a_2 = 2$, $\delta_1 = \delta_2 = 0$, $b_2 \equiv 1 \pmod 2$ and $d = 3^{(b_2-1)/2}$, or we have $a_2 \geq 3$, $b_2 \equiv 0 \pmod 2$ and $\delta_2 = 1$. In this latter case, we also have $\delta_1 = 0$, $a_2 \equiv 0 \pmod 2$ and hence

$$2^{a_2/2} - 3^{b_2/2} = 1 \quad \text{and} \quad 2^{a_2/2} + 3^{b_2/2} = q.$$

Since $a_2 \geq 6$, this first equation has no solutions (by an old result of Levi ben Gerson), whereby it follows that if $q = 3d^2 + 4 \in S_2$, then $d = 3^{(b_2-1)/2}$. If, further, $q = 3d^2 + 4 \in S_2 \cap S_6$, then

$$q = 3^{b_2} + 4 = \frac{d_6^2 + 3^{b_6}}{4},$$

for odd positive integers b_2, d_6 and b_6, so that

$$(7.1) \qquad d_6^2 = 4 \cdot 3^{b_2} - 3^{b_6} + 16.$$

In general, this equation has precisely the solutions

$$(d_6, b_2, b_6) = (1, 1, 3), \ (5, 1, 1), \ (11, 3, 1) \ \text{ and } \ (31, 5, 3)$$

in odd positive integers; none of these correspond to a prime values of $q > 73$. To prove this, note that an elementary argument easily yields that $b_2 > b_6$ unless $|d_6| \le 5$. We may thus write $d_6 = 3^{b_6} \cdot k_1 + (-1)^\delta 4$, for some $\delta \in \{0, 1\}$ and $k_1 \equiv \pm 1 \pmod 6$ a positive integer. Substituting into (7.1), we have

$$3^{b_6} k_1^2 + (-1)^\delta 8 \cdot k_1 = 4 \cdot 3^{b_2 - b_6} - 1.$$

If $k_1 = 1$, then, modulo 3, we have $3^{b_6 - 1} + 3 = 4 \cdot 3^{b_2 - b_6 - 1}$, corresponding to $(d_6, b_2, b_6) = (31, 5, 3)$. If $k_1 > 1$ then $k_1 \ge 5$ and necessarily $b_2 > 2b_6$. It follows that we can write $(-1)^\delta 8 \cdot k_1 + 1 = 3^{b_6} \cdot k_2$ for a (nonzero) integer $k_2 \equiv 3 \pmod 8$, so that

$$(7.2) \qquad \left(3^{b_6} k_2 - 1\right)^2 + 64 k_2 = 256 \cdot 3^{b_2 - 2b_6}.$$

We check that the only solution to this equation with $k_2 \in \{-13, -5, 3, 11\}$ corresponds to $(d_6, b_2, b_6) = (11, 3, 1)$; otherwise, after a little work, we may suppose that $b_2 > 4b_6$ and hence that $-2k_2 3^{b_6} + 64 k_2 + 1$ is divisible by 3^{2b_6} (and hence $|2k_2 3^{b_6} - 64 k_2 - 1| \ge 3^{2b_6}$). It follows that either $b_6 \le 3$, or that we have $|k_2| > 3^{b_6 - 1}$. From (7.2), after a little more work, we may thus conclude that either $b_6 \in \{1, 3\}$, or that $b_2 \ge 6b_6 - 7$.

On the other hand, applying Theorem 1.5 of [1], with (in the notation of that theorem)

$$(a, y, x_0, m_0, \Delta, \alpha, s) = (1, 3, 3788, 15, -37, 3.1, 2),$$

we find that

$$\left| \sqrt{3} - \frac{p}{2 \cdot 3^k} \right| > e^{-170} \, 3^{-1.64281k},$$

for p and k positive integers with $k \ge 4775$. It follows that

$$\left| p^2 - 4 \cdot 3^{2k+1} \right| > 4 \cdot e^{-170} \, 3^{0.35719k},$$

provided $k \ge 4775$. Applying this with $p = d_6$ and $b_2 = 2k + 1$, (7.1) thus implies that either $b_6 \in \{1, 3\}$ or we have

$$3^{(b_2+7)/6} \ge 3^{b_6} > 4 \cdot e^{-170} \, 3^{0.35719(b_2-1)/2},$$

whence $b_2 \le 12979$. A brute-force search confirms that (7.1) has only the listed solutions.

In conclusion, then, if $q = 3d^2 + 4$ for integer d, we have one of the following situations. Either $q \notin S_i$ for $i \ne 5$ and hence corresponds to only $E = 72q.4.a2$ and $E = 72q.4.b2$, or $q \in S_2 \cap S_5$ corresponds to precisely

$$E \in \{72q.3.a1, 72q.4.a2, 72q.4.b2\},$$

or $q \in S_5 \cap S_6$, with

$$E \in \{36q.3.a1, 72q.4.a2, 72q.4.b2\},$$

for, possibly, several different curves of the shape $36q.3.a1$, depending on the number of distinct ways to represent $q = \frac{d_{6,i}^2 + 3^{b_i}}{4}$, for integers $d_{6,i}$ and b_i. In the first case, we deduce a contradiction for every p with $\left(\frac{2}{p}\right) = -1$. In the second, we require

$$\left(\frac{2}{p}\right) = \left(\frac{-6b}{p}\right) = -1,$$

where $q = 3^b + 4$ (and b is odd). Finally, for the third case, we suppose that

$$\left(\frac{2}{p}\right) = \left(\frac{-3b_1}{p}\right) = \cdots = \left(\frac{-3b_t}{p}\right) = -1,$$

where

$$q = 3d^2 + 4 = \frac{d_{6,i}^2 + 3^{b_i}}{4}, \quad \text{for } i = 1, \ldots, t.$$

Here, the exponents b_i are necessarily odd. In each case, these choices for p contradict the fact that the p-torsion of our Frey-Hellegouarch curve F is symplectically isomorphic to that of E.

Let us next suppose that $q \in S_8$ with $q > 73$. From Proposition 5.1, it follows that $q \notin S_i$, for $i \in \{1, 3, 5, 7\}$. By definition, there exist integers u and v such that $q = (3v^2 - 1)/2$ where $u^2 - 3v^2 = -2$. The positive integers $v = v_k$ satisfying this latter equation also satisfy the binary recurrence

$$(7.3) \qquad v_{k+1} = 4v_k - v_{k-1}, \quad \text{for } k \geq 1, \quad \text{where } v_0 = 1, v_1 = 3.$$

In particular, we have that $v_k \equiv 0 \pmod 3$ precisely when $k \equiv 1 \pmod 4$. For such k, we may readily show via induction that $v_k \equiv \pm 3 \pmod{13}$ and hence that $3v_k^2 - 1 \equiv 0 \pmod{13}$. It follows that, in order to have $q = (3v^2 - 1)/2$ prime with $u^2 - 3v^2 = -2$ for some integer u, we require that either $q = 13$, or that $v \equiv \pm 1 \pmod 3$ (whereby $q \equiv 1 \pmod 9$). If, for our $q \in S_8$ with $q > 73$, we have $q = 2^a + 3^b$ for integers $a \geq 2$ and $b \geq 1$, then, modulo 4, b is necessarily even, so that we require $2^a \equiv 1 \pmod 9$, whence $a \equiv 0 \pmod 6$. It follows that $2^a + 3^b \equiv 2, 3$ or $5 \pmod 7$. On the other hand, again from considering the recursion (7.3), we find that $q \equiv \pm 1 \pmod 7$, a contradiction. If, instead, we have $q = 2^a - 3^b$, for $a \geq 2$ and $b \geq 1$, then, modulo 12, a is even and b is odd. If $b = 1$, then we have $2^{a+1} = 3v^2 + 5$ and so, from Lemma 5.1, since $q > 73$, a contradiction. If we suppose that $b \geq 2$, then, modulo 9, we again require that $a \equiv 0 \pmod 6$, so that $2^a - 3^b \equiv 0, 3, 5, 9$ or $11 \pmod{13}$. On the other hand, from (7.3), we have that $q \equiv \pm 1 \pmod{13}$, a contradiction.

It follows that, if $q \in S_2 \cap S_8$ with $q > 73$, then there exist integers $a \geq 2$ and $b \geq 1$, with $q = 3^b - 2^a$. Arguing as previously, modulo $2^2 \cdot 3^3 \cdot 7$, we find that $a \equiv 3 \pmod 6$ and $b \equiv 2 \pmod 6$. Working modulo 73, we find from (7.3) that $q \equiv \pm 1, \pm 34, \pm 35 \pmod{73}$ which shows that, in fact, $b \equiv 2 \pmod{12}$.

We thus have, for $q \in S_8$, that E is necessarily one of

$$18q.3.a1, 18q.4.a2, 36q.1.a2, 36q.1.b2, 72q.3.a1, 72q.7.a1 \text{ or } 72q.9.a2,$$

where $E = 18q.3.a1$ and $72q.3.a1$ correspond to $q \in S_2$, $E = 18q.4.a2$ and $72q.9.a2$ come from $q \in S_4$, $E = 72q.7.a1$ arises from $q \in S_6$ and both $E = 36q.1.a2$ and $36q.1.b2$ occur for every $q \in S_8$. From our previous discussion, if $E = 18q.3.a1$, there exist integers $a_2 \geq 5$ and $b_2 \geq 3$ with $a_2 \equiv 3 \pmod 6$, $b_2 \equiv 2 \pmod{12}$ and $q = 3^{b_2} - 2^{a_2}$. If we choose p such that $\left(\frac{4-a_2}{p}\right) = -1$ (where $4 - a_2$ is negative

and odd), we again contradict the fact that the p-torsion of our Frey-Hellegouarch curve F is symplectically isomorphic to that of E. If $E = 18q.4.a2$, we have that $q = d_4^2 + 2^{a_4}3^{b_4}$ for integers d_4, a_4 and b_4 (not necessarily unique), with $a_4 \geq 8$ even and b_4 odd. In this case, we constrain p to satisfy $\left(\frac{-3b_4}{p}\right) = -1$. Similarly, for $E = 36q.1.a2$ or $36q.1.b2$, we impose the conditions

$$\left(\frac{2}{p}\right) = \left(\frac{6}{p}\right) = -1,$$

while, for $E = 72q.3.a1$, we have $q = 3^{b_2} - 8$ with $b_2 \equiv 2 \pmod{12}$, and choose

$$\left(\frac{-6b_2}{p}\right) = \left(\frac{-3b_2/2}{p}\right) = -1;$$

note that, importantly for us, $-3b_2/2$ is odd. If $E = 72q.7.a1$, we can write $q = \frac{d^2 + 3^{b_6}}{4}$ with b_6 odd and take $\left(\frac{-3b_6}{p}\right) = -1$. Finally, if $E = 72q.9.a2$, we have $q = d_4^2 + 2^4 3^{b_4}$ for integers d_4 and b_4 (not necessarily unique), with b_4 odd, and can derive a contradiction by choosing p such that $\left(\frac{-3b_4}{p}\right) = -1$. In summary, if $q \in S_8$, we reach our desired conclusion by choosing our finite set of κ_i as in case (ii). This completes the proof of Theorem 1.7.

7.2. **Proof of Theorem 1.8.** Let $q = 2^a 3^b - 1$ with $a \geq 5$ and $b \geq 1$ be a prime. Then $q \in S_1$ and hence, from Proposition 5.1, $q \notin S_i$ for $i \in \{2, 3, 5, 7, 8\}$. On the other hand, $q \notin S_i$ for $i \in \{4, 6\}$, since $q \equiv 2 \pmod 3$. It follows that, in this case, a solution to (1.2) with $p \geq q^{2q}$ necessarily corresponds to an elliptic curve in the isogeny class $18q.1.a$. The result now follows from the equalities in (6.1).

7.3. **Proof of Theorem 1.9.** Suppose that A, B and C are coprime, nonzero integers satisfying (1.5) with $p \geq 17$, and write F for the corresponding Frey-Hellegouarch curve. Note that, for $q = 5$, we are led to consider levels $90, 180$ and 360. For these levels, each weight 2, cuspidal newform f corresponds to one of the 9 isogeny classes of elliptic curves $E/\mathbb{Q}$ given in Cremona's notation by

$$90a, \ 90b, \ 90c, \ 180a, \ 360a, \ 360b, \ 360c, \ 360d \ \text{ and } \ 360e.$$

For E in the isogeny classes $90a, 90b, 180a, 360b$ and $360c$, we find that $a_7(E) = 2$ and hence, it follows from (4.3), the Hasse bound and the level lowering condition that

$$2 \equiv 0, \pm4, \pm8 \pmod{p}.$$

This gives a contradiction with $p \geq 17$.

Next, we treat the isogeny class $360e$. Taking $E = 360e2$, we find that $e(E, 3) = 2$. In the beginning of Section 6.4.2, it is explained that either F has potentially multiplicative reduction at $\ell = 3$ or potentially good reduction with $e(F, 3) = 4$, a contradiction in either cases.

Finally, suppose that E is in one of the isogeny classes $90c, 360a$ and $360d$, say, $E = 90c2, 360a2$ or $360d2$. We will apply [12, Theorem 4] and [20, Proposition 2] with $\ell \in \{2, 3, q\}$. In all cases, from [20, Proposition 2] with $\ell = q$, we have that our isomorphism between $F[p]$ and $E[p]$ is necessarily symplectic. If $E = 90c2$, we may thus further appeal to [20, Proposition 2] with $\ell = 2$ and $\ell = 3$ (after suitable

twist) to conclude that

$$(7.4) \qquad \left(\frac{-1}{p}\right) = \left(\frac{-2}{p}\right) = 1.$$

For $E = 360a2$, we apply [12, Theorem 4] and [20, Proposition 2] with $\ell = 3$, whereby

$$(7.5) \qquad \left(\frac{2}{p}\right) = \left(\frac{-3}{p}\right) = 1.$$

If $E = 360d2$, we apply [20, Proposition 2] with $\ell = 3$ to conclude that

$$(7.6) \qquad \left(\frac{-6}{p}\right) = 1.$$

We reach our desired conclusion upon observing that, if $p \equiv 13, 19$ or $23 \pmod{24}$, then each of (7.4), (7.5) and (7.6) fails to hold.

7.4. **Further results for small primes q.** To conclude this paper, we will provide some more explicit results for small values of q. We obtain these by proceeding in a similar fashion to the proof of Theorem 1.9. Making the further assumption that $p \geq q^{2q}$, we reduce the calculation to consideration of elliptic curves E with non-trivial rational 2-torsion, conductor in the set $\{18q, 36q, 72q\}$ and such that $\Delta(E)$ is of the shape T^2 or $-3T^2$ for some integer T (i.e. those corresponding to primes in S_0). We summarize our results as follows.

Theorem 7.1. *If p and q are primes with $p \geq q^{2q}$, then there are no coprime, nonzero integers A, B and C satisfying equation* (1.4) *with q in the following table and p satisfying the listed conditions.*

q	p	q	p
5	$13, 19, 23 \pmod{24}$	47	$5, 11, 13, 17, 19, 23 \pmod{24}$
11	$13, 17, 19, 23 \pmod{24}$	59	$5, 7, 11, 13, 19, 23 \pmod{24}$
13	$11 \pmod{12}$	67	$7, 11, 13, 29, 37, 41, 43, 59, 67, 71, 89, 101, 103 \pmod{120}$
17	$5, 17, 23 \pmod{24}$	71	$5 \pmod{6}$
23	$19, 23 \pmod{24}$	73	$41, 71, 89 \pmod{120}$
29	$7, 11, 13, 17, 19, 23 \pmod{24}$	79	$5, 7, 11, 13, 19, 23 \pmod{24}$
31	$5, 11 \pmod{24}$	89	$13, 17, 19, 23 \pmod{24}$
41	$5, 7, 11, 17, 19, 23 \pmod{24}$	97	$11 \pmod{12}$

Here, we have omitted both primes for which Theorem 1.4 applies directly (i.e. $q = 53$ and 83, according to Corollary 1.6) and also primes for which the symplectic method fails to eliminate exponents, i.e. $q \in \{7, 19, 37, 43, 61\}$. For these latter primes, observe that, in each case, q is of the shape $(3d^2 + 1)/4$ or $3d^2 + 16$ for an integer d; as explained in Section 5.2, these are those primes for which there exists a solution to (1.4) (with $C = 1$) for every exponent p (whereby we expect our techniques to fail), together with those for which we have a "trivial" solution to the related equation $A^3 + B^3 = 8qC^p$, again for every p.

8. APPENDIX : c-INVARIANTS

8.1. Conductor $18q$. We have

Curve	c_4	Curve	c_4
$18q.1.a1$	$3^2 \cdot \left(2^{2a}3^{2b} + (-1)^{\delta}2^a3^b + 1\right)$	$18q.3.a3$	$3^2 \cdot \left(2^{2a-4} + (-1)^{\delta_1+\delta_2}2^a3^b + 3^{2b}\right)$
$18q.1.a2$	$3^2 \cdot \left(2^{2a+4}3^{2b} + (-1)^{\delta}2^{a+4}3^b + 1\right)$	$18q.3.a4$	$3^2 \cdot \left(2^{2a} + (-1)^{1+\delta_1+\delta_2}7 \cdot 2^{a+1}3^b + 3^{2b}\right)$
$18q.1.a3$	$3^2 \cdot \left(2^{2a-4}3^{2b} + (-1)^{\delta}2^a3^b + 1\right)$	$18q.4.a1$	$(-1)^{\delta_1}3^2 \left(q - (-1)^{\delta_2}2^{a-2}3^b\right)$
$18q.1.a4$	$3^2 \cdot \left(2^{2a}3^{2b} + (-1)^{\delta+1}7 \cdot 2^{a+1}3^b + 1\right)$	$18q.4.a2$	$(-1)^{\delta_1}3^2 \left(q - (-1)^{\delta_2}2^{a+2}3^b\right)$
$18q.2.a1$	$3^2 \cdot \left(2^{2a} + 2^a + 1\right)$	$18q.5.a1$	$3^2 \left(d^2 + (-1)^{\delta_1+\delta_2}2^{a-2}\right)$
$18q.2.a2$	$3^2 \cdot \left(2^{2a+4} + 2^{a+4} + 1\right)$	$18q.5.a2$	$3^2 \left(d^2 - (-1)^{\delta_1+\delta_2}2^a\right)$
$18q.2.a3$	$3^2 \cdot \left(2^{2a-4} + 2^a + 1\right)$	$18q.5.b1$	$3^4 \left(d^2 + (-1)^{\delta_1+\delta_2}2^{a-2}\right)$
$18q.2.a4$	$3^2 \cdot \left(2^{2a} - 7 \cdot 2^{a+1} + 1\right)$	$18q.5.b2$	$3^4 \left(d^2 - (-1)^{\delta_1+\delta_2}2^a\right)$
$18q.3.a1$	$3^2 \cdot \left(2^{2a} + (-1)^{\delta_1+\delta_2}2^a3^b + 3^{2b}\right)$	$18q.6.a1$	$3^2 \left(d^2 + 3 \cdot 2^{a-2}\right)$
$18q.3.a2$	$3^2 \cdot \left(2^{2a+4} + (-1)^{\delta_1+\delta_2}2^{a+4}3^b + 3^{2b}\right)$	$18q.6.a2$	$3^2 \left(d^2 - 3 \cdot 2^a\right)$

Curve	c_6
$18q.1.a1$	$(-1)^{\delta+1}3^3 \left(2^{a+1}3^b + (-1)^{\delta}\right)\left(2^a3^b + (-1)^{\delta+1}\right)\left(2^{a-1}3^b + (-1)^{\delta}\right)$
$18q.1.a2$	$3^3 \left(2^{a+1}3^b + (-1)^{\delta}\right)\left(2^{2a+5}3^{2b} + (-1)^{\delta}2^{a+5}3^b - 1\right)$
$18q.1.a3$	$(-1)^{\delta+1}3^3 \left(2^{a-1}3^b + (-1)^{\delta}\right)\left(2^{2a-5}3^{2b} + (-1)^{\delta+1}2^a3^b - 1\right)$
$18q.1.a4$	$(-1)^{\delta+1}3^3 \left(2^a3^b + (-1)^{\delta+1}\right)\left(2^{2a}3^{2b} + (-1)^{\delta}17 \cdot 2^{a+1}3^b + 1\right)$
$18q.2.a1$	$-3^3 \left(2^{a+1} + 1\right)\left(2^a - 1\right)\left(2^{a-1} + 1\right)$
$18q.2.a2$	$-3^3 \left(2^{a+1} + 1\right)\left(2^{2a+5} + 2^{a+5} - 1\right)$
$18q.2.a3$	$-3^3 \left(2^{a-1} + 1\right)\left(2^{2a-5} - 2^a - 1\right)$
$18q.2.a4$	$-3^3 \left(2^a - 1\right)\left(2^{2a} + 17 \cdot 2^{a+1} + 1\right)$
$18q.3.a1$	$(-1)^{\delta}3^3 \left(2^{a+1} + (-1)^{\delta_1+\delta_2}3^b\right)\left(2^a - (-1)^{\delta_1+\delta_2}3^b\right)\left(2^{a-1} + (-1)^{\delta_1+\delta_2}3^b\right)$
$18q.3.a2$	$(-1)^{\delta}3^3 \left(2^{a+1} + (-1)^{\delta_1+\delta_2}3^b\right)\left(2^{2a+5} + (-1)^{\delta_1+\delta_2}2^{a+5}3^b - 3^{2b}\right)$
$18q.3.a3$	$(-1)^{b+1}3^3 \left((-1)^{\delta_1+\delta_2}2^{a-1} + 3^b\right)\left(2^{2a-5} - (-1)^{\delta_1+\delta_2}2^a3^b - 3^{2b}\right)$
$18q.3.a4$	$(-1)^{b}3^3 \left(3^b + (-1)^{b+\delta}2^a\right)\left(2^{2a} + (-1)^{\delta_1+\delta_2}17 \cdot 2^{a+1}3^b + 3^{2b}\right)$
$18q.4.a1$	$3^3d \left(d^2 + (-1)^{\delta_1+\delta_2}2^{a-3}3^{b+2}\right)$
$18q.4.a2$	$3^3d \left(d^2 + (-1)^{\delta_1+\delta_2}2^a3^{b+2}\right)$
$18q.5.a1$	$3^3d \left(d^2 + (-1)^{\delta_1+\delta_2}2^{a-3}3\right)$
$18q.5.a2$	$3^3d \left(d^2 + (-1)^{\delta_1+\delta_2}2^a3\right)$
$18q.5.b1$	$-3^6d \left(d^2 + (-1)^{\delta_1+\delta_2}2^{a-3}3\right)$
$18q.5.b2$	$-3^6d \left(d^2 + (-1)^{\delta_1+\delta_2}2^a3\right)$
$18q.6.a1$	$3^3d \left(d^2 + 2^{a-3}3^2\right)$
$18q.6.a2$	$3^3d \left(d^2 + 2^a3^2\right)$

8.2. Conductor $36q$. We have

Curve	c_4	Curve	c_4
$36q.1.a1$	$2^4 3 \left(q^2 - 1\right)$	$36q.4.a1$	$2^4 3^2 \left(d^2 - 3^{b+1}\right)$
$36q.1.a2$	$2^4 3 \left(16q^2 - 1\right)$	$36q.4.a2$	$2^4 3^2 \left(d^2 + 4 \cdot 3^{b+1}\right)$
$36q.1.b1$	$2^4 3^3 \left(q^2 - 1\right)$	$36q.5.a1$	$2^4 3^2 \left(d^2 - 3^{b+1}\right)$
$36q.1.b2$	$2^4 3^3 \left(16q^2 - 1\right)$	$36q.5.a2$	$2^4 3^2 \left(d^2 + 4 \cdot 3^{b+1}\right)$
$36q.2.a1$	$2^2 3^2 \left(d^2 - 1\right)$	$36q.6.a1$	$2^4 3^2 \left(d^2 - 1\right)$
$36q.2.a2$	$2^4 3^2 \left(4d^2 + 1\right)$	$36q.6.a2$	$2^4 3^2 \left(d^2 + 4\right)$
$36q.2.b1$	$2^2 3^4 \left(d^2 - 1\right)$	$36q.6.b1$	$2^4 3^4 \left(d^2 - 1\right)$
$36q.2.b2$	$2^4 3^4 \left(4d^2 + 1\right)$	$36q.6.b2$	$2^4 3^4 \left(d^2 + 4\right)$
$36q.3.a1$	$2^2 3^2 \left(d^2 - 3^{b+1}\right)$	$36q.7.a1$	$2^4 3^2 \left(d^2 + 3^{b+1}\right)$
$36q.3.a2$	$2^4 3^2 \left(4d^2 + 3^{b+1}\right)$	$36q.7.a2$	$2^4 3^2 \left(d^2 - 4 \cdot 3^{b+1}\right)$

Curve	c_6	Curve	c_6
$36q.1.a1$	$-2^5 3^2 rs \left(q^2 + 2\right)$	$36q.4.a1$	$2^5 3^3 d \left(2d^2 - 3^{b+2}\right)$
$36q.1.a2$	$-2^6 3^2 rs \left(32q^2 + 1\right)$	$36q.4.a2$	$2^6 3^3 d \left(d^2 - 4 \cdot 3^{b+2}\right)$
$36q.1.b1$	$2^5 3^5 rs \left(q^2 + 2\right)$	$36q.5.a1$	$2^5 3^3 d \left(2d^2 - 3^{b+2}\right)$
$36q.1.b2$	$2^6 3^5 rs \left(32q^2 + 1\right)$	$36q.5.a2$	$2^6 3^3 d \left(d^2 - 4 \cdot 3^{b+2}\right)$
$36q.2.a1$	$-2^3 3^3 d \left(d^2 + 3\right)$	$36q.6.a1$	$2^5 3^3 d \left(2d^2 - 3\right)$
$36q.2.a2$	$-2^6 3^3 d \left(8d^2 + 3\right)$	$36q.6.a2$	$2^6 3^3 d \left(d^2 - 12\right)$
$36q.2.b1$	$2^3 3^6 d \left(d^2 + 3\right)$	$36q.6.b1$	$-2^5 3^6 d \left(2d^2 - 3\right)$
$36q.2.b2$	$2^6 3^6 d \left(8d^2 + 3\right)$	$36q.6.b2$	$-2^6 3^6 d \left(d^2 - 12\right)$
$36q.3.a1$	$-2^3 3^3 d \left(d^2 + 3^{b+2}\right)$	$36q.7.a1$	$2^5 3^3 d \left(2d^2 + 3^{b+2}\right)$
$36q.3.a2$	$-2^6 3^3 d \left(8d^2 + 3^{b+2}\right)$	$36q.7.a2$	$2^6 3^3 d \left(d^2 + 4 \cdot 3^{b+2}\right)$

8.3. **Conductor** $72q$. We have

Curve	c_4	Curve	c_4
$72q.1.a1$	$2^4 3^2 \left(3^{2b} + 3^b + 1\right)$	$72q.5.b1$	$2^4 3^4 \left(d^2 + (-1)^\delta 2^{a-2}\right)$
$72q.1.a2$	$2^4 3^2 \left(16 \cdot 3^{2b} + 16 \cdot 3^b + 1\right)$	$72q.5.b2$	$2^4 3^4 \left(d^2 - (-1)^\delta 2^a\right)$
$72q.1.a3$	$2^4 3^2 \left(16 \cdot 3^{2b} + 16 \cdot 3^b + 1\right)$	$72q.6.a1$	$2^2 3^2 \left(d^2 - 1\right)$
$72q.1.a4$	$2^4 3^2 \left(16 \cdot 3^{2b} + 16 \cdot 3^b + 1\right)$	$72q.6.a2$	$2^4 3^2 \left(4d^2 + 1\right)$
$72q.2.a1$	$2^4 3^2 \left(2^{2a} 3^{2b} + (-1)^\delta 2^a 3^b + 1\right)$	$72q.6.b1$	$2^2 3^4 \left(d^2 - 1\right)$
$72q.2.a2$	$2^4 3^2 \left(2^{2a+4} 3^{2b} + (-1)^\delta 2^{a+4} 3^b + 1\right)$	$72q.6.b2$	$2^4 3^4 \left(4d^2 + 1\right)$
$72q.2.a3$	$2^4 3^2 \left(2^{2a-4} 3^{2b} + (-1)^\delta 2^a 3^b + 1\right)$	$72q.7.a1$	$2^2 3^2 \left(d^2 - 3^{b+1}\right)$
$72q.2.a4$	$2^4 3^2 \left(2^{2a} 3^{2b} + (-1)^\delta 7 \cdot 2^{a+1} 3^b + 1\right)$	$72q.7.a2$	$2^4 3^2 \left(4d^2 - 3^{b+1}\right)$
$72q.3.a1$	$2^4 3^2 \left(3^{2b} + (-1)^\delta 2^a 3^b + 2^{2a}\right)$	$72q.8.a1$	$2^4 3^2 \left(d^2 + 3^{b+1}\right)$
$72q.3.a2$	$2^4 3^2 \left(3^{2b} - (-1)^\delta 7 \cdot 2^{a+1} 3^b + 2^{2a}\right)$	$72q.8.a2$	$2^4 3^2 \left(d^2 - 4 \cdot 3^{b+1}\right)$
$72q.3.a3$	$2^4 3^2 \left(3^{2b} + (-1)^\delta 2^{a+4} 3^b + 2^{2a+4}\right),$	$72q.9.a1$	$2^4 3^2 \left(d^2 + (-1)^{\delta_1 + \delta_2} 2^{a-2} 3^{b+1}\right)$
$72q.3.a4$	$2^4 3^2 \left(3^{2b} + (-1)^\delta 2^a 3^b + 2^{2a-4}\right)$	$72q.9.a2$	$2^4 3^2 \left(d^2 + (-1)^{\delta_1 + \delta_2 + 1} 2^a \cdot 3^{b+1}\right)$
$72q.4.a1$	$2^4 3^2 \left(d^2 + 1\right)$	$72q.10.a1$	$2^4 3^2 \left(d^2 - 2^{a-2} 3^{b+1}\right)$
$72q.4.a2$	$2^4 3^2 \left(d^2 - 4\right)$	$72q.10.a2$	$2^4 3^2 \left(d^2 + 2^a \cdot 3^{b+1}\right)$
$72q.4.b1$	$2^4 3^4 \left(d^2 + 1\right)$	$72q.11.a1$	$2^4 3^2 \left(d^2 + 24\right)$
$72q.4.b2$	$2^4 3^4 \left(d^2 - 4\right)$	$72q.11.a2$	$2^4 3^2 \left(d^2 - 96\right)$
$72q.5.a1$	$2^4 3^2 \left(d^2 + (-1)^\delta 2^{a-2}\right)$	$72q.12.a1$	$2^4 3^2 \left(d^2 + 24\right)$
$72q.5.a2$	$2^4 3^2 \left(d^2 - (-1)^\delta 2^a\right)$	$72q.12.a2$	$2^4 3^2 \left(d^2 - 96\right)$

Curve	c_6
$72q.1.a1$	$2^5 3^3 (3^b - 1)(3^b + 2)(2 \cdot 3^b + 1)$
$72q.1.a2$	$2^6 3^3 (2 \cdot 3^b + 1)\left(32 \cdot 3^{2b} + 32 \cdot 3^b - 1\right)$
$72q.1.a3$	$2^6 3^3 (2 \cdot 3^b + 1)\left(32 \cdot 3^{2b} + 32 \cdot 3^b - 1\right)$
$72q.1.a4$	$2^6 3^3 (2 \cdot 3^b + 1)\left(32 \cdot 3^{2b} + 32 \cdot 3^b - 1\right)$
$72q.2.a1$	$-2^6 3^3 ((-1)^\delta 2^{a+1} 3^b + 1)\left(2^{2a-1} 3^{2b} + (-1)^\delta 2^{a-1} 3^b - 1\right)$
$72q.2.a2$	$-2^6 3^3 ((-1)^\delta 2^{a+1} 3^b + 1)\left(2^{2a+5} 3^{2b} + (-1)^\delta 2^{a+5} 3^b - 1\right)$
$72q.2.a3$	$2^5 3^3 ((-1)^\delta 2^{a-1} 3^b + 1)\left(-2^{2a-4} 3^{2b} + (-1)^\delta 2^{a+1} 3^b + 2\right)$
$72q.2.a4$	$-2^6 3^3 ((-1)^\delta 2^a 3^b - 1)\left(2^{2a} 3^{2b} + (-1)^\delta 17 \cdot 2^{a+1} 3^b + 1\right)$
$72q.3.a1$	$2^6 3^3 (-1)^b (3^b - (-1)^\delta 2^a)\left(2^{2a} + (-1)^\delta 5 \cdot 2^{a-1} 3^b + 3^{2b}\right)$
$72q.3.a2$	$2^6 3^3 (-1)^b (3^b - (-1)^\delta 2^a)\left(2^{2a} + (-1)^\delta 17 \cdot 2^{a+1} 3^b + 3^{2b}\right)$
$72q.3.a3$	$-2^6 3^3 (-1)^b (3^b + (-1)^\delta 2^{a+1})\left(2^{2a+5} + (-1)^\delta 2^{a+5} 3^b - 3^{2b}\right)$
$72q.3.a4$	$2^5 3^3 (-1)^b (3^b + (-1)^\delta 2^{a-1})\left(-2^{2a-4} + (-1)^\delta 2^{a+1} 3^b + 2 \cdot 3^{2b}\right)$
$72q.4.a1$	$-2^5 3^3 d\left(2d^2 + 3\right)$
$72q.4.a2$	$-2^6 3^3 d\left(d^2 + 12\right)$
$72q.4.b1$	$2^5 3^6 d\left(2d^2 + 3\right)$
$72q.4.b2$	$2^6 3^6 d\left(d^2 + 12\right)$
$72q.5.a1$	$-2^5 3^3 d\left((-1)^\delta 2d^2 + 3 \cdot 2^{a-2}\right)$
$72q.5.a2$	$-2^6 3^3 d\left((-1)^\delta d^2 + 3 \cdot 2^a\right)$
$72q.5.b1$	$2^5 3^6 d\left((-1)^\delta 2d^2 + 3 \cdot 2^{a-2}\right)$
$72q.5.b2$	$2^6 3^6 d\left((-1)^\delta d^2 + 3 \cdot 2^a\right)$
$72q.6.a1$	$2^5 3^3 d\left(\frac{d^2+3}{4}\right)$
$72q.6.a2$	$2^6 3^3 d\left(8d^2 + 3\right)$
$72q.6.b1$	$-2^5 3^6 d\left(\frac{d^2+3}{4}\right)$
$72q.6.b2$	$-2^6 3^6 d\left(8d^2 + 3\right)$
$72q.7.a1$	$2^5 3^3 d\left(\frac{d^2+3^{b+2}}{4}\right)$
$72q.7.a2$	$2^6 3^3 d\left(8d^2 + 3^{b+2}\right)$
$72q.8.a1$	$-2^5 3^3 d\left(2d^2 + 3^{b+2}\right)$
$72q.8.a2$	$-2^6 3^3 d\left(d^2 + 4 \cdot 3^{b+2}\right)$
$72q.9.a1$	$2^6 3^3 d\left(d^2 + (-1)^{\delta_1+\delta_2} 2^{a-3} 3^{b+2}\right)$
$72q.9.a2$	$2^6 3^3 d\left(d^2 + (-1)^{\delta_1+\delta_2} 2^a \cdot 3^{b+2}\right)$
$72q.10.a1$	$2^6 3^3 d\left(d^2 - 2^{a-3} 3^{b+2}\right)$
$72q.10.a2$	$2^6 3^3 d\left(d^2 - 2^a \cdot 3^{b+2}\right)$
$72q.11.a1$	$2^6 3^3 d\left(d^2 + 36\right)$
$72q.11.a2$	$2^6 3^3 d\left(d^2 + 288\right)$
$72q.12.a1$	$2^6 3^3 d\left(d^2 + 36\right)$
$72q.12.a2$	$2^6 3^3 d\left(d^2 + 288\right)$

References

[1] M. Bauer and M. A. Bennett, Applications of the Hypergeometric Method to the Generalized Ramanujan-Nagell Equation, *Ramanujan J.* 6 (2002), 209–270.

[2] M. A. Bennett, Pillai's conjecture revisited, *J. Number Th.* 98 (2003), 228–235.

[3] M. A. Bennett and A. Ghadermarzi, Mordell's equation : a classical approach, *LMS J. Comput. Math.* 18 (2015), 633–646.

[4] M.A. Bennett, F Luca and J. Mulholland, Twisted extensions of the cubic case of Fermat's Last Theorem, *Ann. Sci. Math. Québec* 35 (2011), 1–15.

[5] M.A. Bennett, G. Martin, K. O'Bryant and A. Rechnitzer, Explicit bounds for primes in arithmetic progressions, in preparation.

[6] 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.

[7] C. Bruni, Twisted Extensions of Fermat's Last Theorem, PhD Thesis, University of British Columbia, 2015, 299 pp.

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

[9] J. E. Cremona, Algorithms for Modular Elliptic Curves, 2nd ed., Cambridge University Press, 1997.

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

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

[12] N. Freitas, On the Fermat-type equation $x^3 + y^3 = z^p$, *Commentarii Mathematici Helvetici* 91 (2016), 295–304.

[13] N. Freitas and A. Kraus, On symplectic isomorphisms of the p-torsion of elliptic curves, preprint.

[14] N. Freitas and A. Kraus, On symplectic isomorphisms of the p-torsion of elliptic curves II, in preparation.

[15] N. Freitas, B. Naskręcki and M. Stoll, The generalized Fermat equation with exponents $2, 3, n$. preprint available at `http://www.math.ubc.ca/~nuno/preprint3.pdf`

[16] E. Halberstadt and A. Kraus, Courbes de Fermat: résultats et problèmes, *J. Reine Angew. Math.* 548 (2002), 167–234.

[17] D. R. Heath-Brown, Siegel zeros and the least prime in an arithmetic progression, *Quart. J. Math. Oxford Ser. (2)*, 41 (1990), 405–418.

[18] A. Kraus, Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, *Manuscripta Math.* 69 (1990), no. 4, 353–385.

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

[20] A. Kraus and J.Oesterle, Sur une question de B. Mazur, *Math. Ann.* 293 (1992), 259–275.

[21] J. Mulholland, Elliptic Curves with Rational 2-torsion and Related Ternary Diophantine Equations, PhD Thesis, University of British Columbia, 2006, 340 pp.

[22] S. S. Pillai, On the equation $2^x - 3^y = 2^X + 3^Y$, *Bull. Calcutta Math. Soc.* 37, (1945). 15–20.

[23] R. J. Stroeker and R. Tijdeman, Diophantine Equations, In: Computational Methods in Number Theory, Math. Centre Tracts 155, Centr. Math. Comp. Sci., Amsterdam, 1982, 321–369.

[24] R. Tijdeman, On integers with many small prime factors, *Compositio Math.* 26 (1973), 319–330

[25] R. Tijdeman and L. Wang, Sums of products of powers of given prime numbers, *Pacific J. Math.* 132 (1988), 177–193.

[26] L. Wang, Four term equations, *Indagationes Math.* 92 (1989), 355–361.

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

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

Department of Mathematics, University of British Columbia, Vancouver, B.C., V6T 1Z2 Canada
  URL: http://www.math.ubc.ca/∼bennett/

  E-mail address: cbruni@uwaterloo.ca

Centre for Education in Mathematics and Computing, University of Waterloo, Waterloo, Ontario, N2L 3G1 Canada
  URL: http://www.cemc.uwaterloo.ca/∼cbruni/

  E-mail address: nuno@math.ubc.ca

Department of Mathematics, University of British Columbia, Vancouver, B.C., V6T 1Z2 Canada
  URL: http://www.math.ubc.ca/∼nuno/