Ternary Diophantine Equations of Signature $(p, p, 3)$

Michael A. Bennett, Vinayak Vatsal and Soroosh Yazdani

Abstract

In this paper, we develop machinery to solve ternary Diophantine equations of the shape $Ax^n + By^n = Cz^3$ for various choices of coefficients (A, B, C). As a byproduct of this, we show, if p is prime, that the equation $x^n + y^n = pz^3$ has no solutions in coprime integers x and y with $|xy| > 1$ and prime $n > p^{4p^2}$. The techniques employed enable us to classify all elliptic curves over $\mathbb{Q}$ with a rational 3-torsion point and good reduction outside the set $\{3, p\}$, for a fixed prime p.

1. Introduction

After the groundbreaking work of Wiles [Wi95] and subsequent full proof of the Shimura-Taniyama-Weil conjecture by Breuil, Conrad, Diamond and Taylor [BCDT01], there has been much interest in exploring the applications of techniques from Galois representations and modular forms to Diophantine equations (see e.g. [Da93a], [Da93b], [DG95], [DM97], [El03], [Iv03], [Kr96], [Kr98], [Kr97b], [Kr99], [Me99], [Ser87]), centering on ternary equations of the shape

$$Ax^p + By^q = Cz^r$$

for p, q and r positive integers with $1/p + 1/q + 1/r < 1$. We will refer to the triple (p, q, r) as the *signature* of the corresponding equation. In the case of signatures $(p, p, 2)$ and $(p, p, 3)$, work of Darmon [Da93a] and Darmon and Merel [DM97] provides a comprehensive analysis, provided $ABC = 1$. In [BS03], the first author, together with Chris Skinner, extended the techniques of [DM97] to apply to equations of signature $(p, p, 2)$ with arbitrary coefficients A, B, C. This paper is intended to be a companion piece to [BS03], where we apply these techniques in the case of signature $(p, p, 3)$, that is to equations of the form

$$Ax^n + By^n = Cz^3. \tag{1}$$

Our object is to provide sufficient criteria for (A, B, C) to guarantee that such an equation is insoluble in coprime nonzero integers (x, y, z) with $xy \neq \pm 1$. In contrast to [BS03], applying an idea used by Kraus [Kr97b] for signature (p, p, p), and Ivorra [Iv01] for signature $(p, p, 2)$, we are able to derive results for infinite families of coefficients (A, B, C). As an offshoot of our approach, in Section 6 we will completely classify elliptic curves over $\mathbb{Q}$ with a rational 3-torsion point and conductor $3^\tau p^\omega$ (where p is prime). This generalizes work of Hadano [Ha82].

Our main results from the standpoint of Diophantine equations are as follows :

Theorem 1.1. *If p and n are prime, and α is a nonnegative integer, then the Diophantine equation*

$$x^n + y^n = p^\alpha z^3$$

has no solutions in coprime integers x, y and z with $|xy| > 1$ and $n > p^{4p^2}$.

2000 Mathematics Subject Classification 11D41

Keywords: ternary Diophantine equations, Frey curves

The first author was supported in part by a grant from NSERC.

The second author was supported in part by grants from NSERC and the Sloan Foundation.

A novel feature of this theorem is its uniformity in the prime p, without additional hypotheses; this is not the case for analogous results on equations of signature (p,p,p) or $(p,p,2)$ (see [Kr97b] and [Iv01]). A corollary is

Corollary 1.2. *If p is prime, then the Diophantine equation*

$$x^n + y^n = p^\alpha z^3$$

has at most finitely many solutions in integers x, y, z, α and n with x and y coprime, $|xy| > 1$ and $n \geqslant 4$.

For $AB \neq 1$ in (1), we have

Theorem 1.3. *If p and n are prime such that $p \neq s^3 \pm 3^t$ for any integers s and t with $t \neq 1$, and α is a nonnegative integer, then the Diophantine equation*

$$x^n + p^\alpha y^n = z^3$$

has no solutions in coprime integers x, y and z with $|xy| > 1$ and $n > p^{2p}$.

Theorem 1.4. *If p and n are prime such that $p \neq 5, 3s^3 \pm 1, 9s^3 \pm 1$ for any integer s, and α, β are positive integers with β coprime to 3, then the Diophantine equation*

$$x^n + p^\alpha y^n = 3^\beta z^3$$

has no solutions in coprime integers x, y and z with $|xy| > 1$ and $n > p^{i28p}$.

For small values of A, B, C in (1), we can be rather more precise.

Theorem 1.5. *If $C \in \{1,2,3,5,7,11,13,15,17,19\}$, n is prime satisfying*

$$n > \max\{C, 4\}$$

and α and β are nonnegative integers, then the Diophantine equation

$$x^n + 3^\alpha y^n = C^\beta z^3$$

has no solutions in coprime integers x, y and z with $|xy| > 1$, unless

$$(|x|, |y|, \alpha, n, |C^\beta z^3|) = (2, 1, 1, 7, 125)$$

or, possibly, $(C,n) = (7,11)$, $(C,n) = (11,13)$ or $(\alpha, C) = (1,p)$ with $p = 2$ or $p \geqslant 11$.

Theorem 1.6. *If $n \geqslant 11$ is prime,*

$$p \in \{5,11,13,23,29,31,41,43,47,53,59,61,67,71,79,83,97\}$$

and α is a positive integer, then the Diophantine equation

$$x^n + p^\alpha y^n = z^3$$

has no solutions in coprime integers x, y and z with $|xy| > 1$, unless, possibly, n divides $p^2 - 1$, or

$$\begin{aligned}(p,n) \in \ & \{(13,19),(29,11),(43,13),(47,13),(59,11),\\ & (61,61),(67,73),(79,97),(97,13),(97,79)\}.\end{aligned}$$

Theorem 1.7. *If $n \geqslant 7$ is prime,*

$$p \in \{7,11,13\}$$

and α, β are positive integers with β coprime to 3, then the Diophantine equation

$$x^n + p^\alpha y^n = 3^\beta z^3$$

has no solutions in coprime integers x, y and z with $|xy| > 1$, unless, possibly, $(p,n) = (7,13)$ or $(p,n) = (13,7)$.

2. Elliptic Curves

Let us suppose that a, b, c, A, B and C are nonzero integers such that

$$Aa^n + Bb^n = Cc^3$$

for some prime integer $n \geqslant 5$. Assume Aa, Bb, and Cc are pairwise coprime, and, without loss of generality, that $Aa \not\equiv 0 \pmod 3$ and $Bb^n \not\equiv 2 \pmod 3$. Further, suppose that C is cube free and that A and B are nth power free. Following [DG95] and [DM97], we consider the elliptic curve

$$E = E(a, b, c) : y^2 + 3Ccxy + C^2Bb^n y = x^3. \tag{2}$$

In what follows, we will denote by $\mathrm{ord}_p(m)$ the largest nonnegative integer k such that p^k divides a given integer m. With the above assumptions, we have

LEMMA 2.1. *Let E be defined as in (2).*

(a) The discriminant $\Delta(E)$ of the curve E is given by

$$\Delta(E) = 3^3AB^3C^8(ab^3)^n,$$

while the j-invariant $j(E)$ satisfies

$$j(E) = 3^3\frac{Cc^3(9Aa^n + Bb^n)^3}{AB^3(ab^3)^n}.$$

(b) The conductor $N(E)$ of the curve E is

$$N(E) = Rad^*(ABab)Rad^*(C)^2\epsilon_3$$

where

$$Rad^*(M) = \prod_{p|M, p\neq 3} p$$

and

$$\epsilon_3 = \begin{cases} 3^2 & \text{If } 9 \mid (2 + C^2Bb^n - 3Cc), \\ 3^3 & \text{If } 3 \parallel (2 + C^2Bb^n - 3Cc) \\ 3^4 & \text{If } ord_3(Bb^n) = 1, \\ 3^3 & \text{If } ord_3(Bb^n) = 2, \\ 1 & \text{If } ord_3(Bb^n) = 3, \\ 3 & \text{If } ord_3(Bb^n) > 3, \\ 3^5 & \text{If } 3 \mid C. \end{cases}$$

In particular, E has split multiplicative reduction at each prime $p \neq 3$ dividing Bb, split multiplicative reduction at each prime dividing Aa congruent to 1, 4, 5, 7, 16, 17 or 20 modulo 21, and non-split multiplicative reduction at all other primes dividing Aa, except 3. Also, E has split multiplicative reduction at 3 if $ord_3(Bb^n) > 3$, and good reduction if $ord_3(Bb^n) = 3$.

(c) The curve E has a $\mathbb{Q}$-rational point of order 3.

Proof. Part (a) of the lemma is a routine calculation, while (c) follows from the fact that $(0, 0)$ is a rational point of order 3 on E. To deduce (b), we will employ Tate's algorithm, as explained in [Sil94]. We carry out this calculation in some detail as the actual reduction types of the elliptic curves under consideration will be of later use. We have (in the notation of [Sil94])

$$a_1 = 3Cc,\ a_3 = C^2Bb^n,\ b_2 = 9C^2c^2,\ b_4 = 3C^3Bcb^n,\ b_6 = C^4B^2b^{2n}$$

and $b_8 = 0$. Let us fix a prime $\pi \mid \Delta$. We consider the cases $\pi \mid Bb$, $\pi \mid Aa$, $\pi \mid C$ and $\pi = 3$ separately (this last situation may be simplified through application of work of Papadopolous [Pa93]). By $a_{i,j}$

or $b_{i,j}$, we will mean $a_i\pi^{-j}$ or $b_i\pi^{-j}$, respectively. Notice that

$$\gcd(a, B) = \gcd(a, C) = \gcd(b, A) = \gcd(b, C) = 1.$$

Case 1 : $\pi \mid Bb$, $\pi \neq 3$. Observe that $\pi \mid a_3, a_4, a_6$ while $\pi \not| b_2 = a_1^2$. We thus have the following reduction type and associated quantities :

$$\text{Type } \mathrm{I}_n, \qquad \mathrm{ord}_\pi(\Delta) = 3n \ \mathrm{ord}_\pi(b) + 3 \ \mathrm{ord}_\pi(B) = n, \qquad m = n, \qquad f = 1,$$

while $\mathrm{ord}_\pi(j) = -n = -3n \ \mathrm{ord}_\pi(b) - 3 \ \mathrm{ord}_\pi(B)$. We have split multiplicative reduction at π, since $T^2 + a_1T$ factors.

Case 2 : $\pi \mid Aa$, $\pi \neq 3$. In this case, we change variables, taking $y = Y + a_3$ and $x = X - \frac{a_1^2}{3}$ and consider the elliptic curve

$$E' : Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X^4 + a_6'.$$

where

$$a_1' = a_1, \ \ a_3' = \frac{27a_3 - a_1^3}{9}, \ \ a_2' = \frac{-a_1^2}{3}, \ \ a_4' = -\frac{a_1(27a_3 - a_1^3)}{27}$$

and

$$a_6' = -\frac{(27a_3 - a_1^3)(54a_3 - a_1^3)}{3^6}.$$

Since $27a_3 - a_1^3 = 27C^2Aa^n$, $\pi \mid a_3', a_4'$, and a_6'. Also note that $b_2' = (a_1')^2 + 4a_2' = -3C^2c^2$, whence $\pi \not| b_2'$. We thus have

$$\text{Type } \mathrm{I}_n, \qquad \mathrm{ord}_\pi(\Delta) = n \ \mathrm{ord}_\pi(a) + \mathrm{ord}_\pi(A) = n, \qquad m = n, \qquad f = 1$$

and $\mathrm{ord}_\pi(j) = -n = -n \ \mathrm{ord}_\pi(a) - \mathrm{ord}_\pi(A)$. The reduction at π is split precisely when $T^2 + a_1T - a_1^2/3$ splits $\pmod{\pi}$. Note that for $\pi = 2$ we have non-split reduction. For $\pi > 2$ we have

$$\begin{aligned} T^2 + a_1T - \frac{a_1^2}{3} &\equiv \left(T + \frac{\pi+1}{2}a_1\right)^2 - \left(\frac{1}{4} + \frac{1}{3}\right)a_1^2 \pmod{\pi} \\ &\equiv \left(T + \frac{\pi+1}{2}a_1\right)^2 - 21\left(\frac{a_1}{6}\right)^2 \pmod{\pi}. \end{aligned}$$

It follows that we have split multiplicative reduction if 21 is a quadratic residue $\pmod{\pi}$ (this includes $\pi = 7$), and we have non-split multiplicative reduction if 21 is a quadratic non-residue $\pmod{\pi}$. By quadratic reciprocity, we thus have split reduction when $\pi = 7$ or $\pi \equiv 1, 4, 5, 16, 17, 20 \pmod{21}$ and non-split reduction otherwise.

Case 3 : $\pi \mid C$, $\pi \neq 3$. In this case, we have two possibilities to consider. Either $\mathrm{ord}_\pi(C) = 1$, or $\mathrm{ord}_\pi(C) = 2$. In the first case,

$$\pi \mid a_3, a_4, b_2, \ \ \pi^2 \mid a_6, \ \ \pi^3 \mid b_6, b_8$$

and, since the polynomial $Y^2 + a_{3,2}Y$ splits and has distinct roots (since $\pi \not| Bb^n$ and $\pi^2 \parallel C$), we have the following reduction type :

$$\text{Type IV}^*, \qquad m = 7, \qquad f = \mathrm{ord}_\pi(\Delta) - 6 = 2, \qquad c = 3.$$

If, however, $\mathrm{ord}_\pi(C) = 2$, then our elliptic curve is not minimal. Applying the substitution $x = \pi^2X$ and $y = \pi^3Y$ leads us to

$$E' : Y^2 + a_{1,1}XY + a_{3,3}Y = X^3.$$

Since

$$\pi \mid a_{3,3}, a_{4,4}, b_{2,2}, \ \ \pi^2 \mid a_{6,6}, \ \ \pi^3 \mid b_{8,8},$$

but $\pi^3 \not| b_{6,6}$ (since $\mathrm{ord}_\pi(b_{6,6}) = 2\ \mathrm{ord}_\pi(a_{3,3}) = 2$), we have

$$\text{Type IV}, \qquad m = 3, \qquad f = \mathrm{ord}_\pi(\Delta_{12}) - 2 = 2, \qquad c = 3.$$

Next, we calculate the conductor at $\pi = 3$. Here, we may directly apply work of Papadopolous [Pa93].

Case 4 : $3 \mid Bb^n$**.** If $\mathrm{ord}_3(Bb^n) = 1$ or 2, then we have reduction types

$$\text{Type IV}, \qquad m = 3, \qquad f = \mathrm{ord}_3(\Delta) - 2 = 4, \qquad c = 3$$

and

$$\text{Type IV}^*, \qquad m = 7, \qquad f = \mathrm{ord}_3(\Delta) - 6 = 3, \qquad c = 3,$$

respectively. The latter statement follows from the fact that the polynomial $Y^2 + a_{3,2}Y$ splits and has distinct roots modulo 3 (since $3 \not| C$ and $9 \parallel Bb^n$). If $\mathrm{ord}_3(Bb^n) \geqslant 3$, then E is not minimal at 3 and hence, after substituting $x = 9X$ and $y = 27Y$, we consider

$$E' : Y^2 + a_{1,1}XY + a_{3,3}Y = X^3.$$

If $\mathrm{ord}_3(Bb^n) = 3$, the discriminant of E' has no 3-part, and hence $f = 0$. If $\mathrm{ord}_3(Bb^n) > 3$, since the prime 3 divides $a_{3,3}, a_{4,4}$ and $a_{6,6}$, but fails to divide $b_{2,2}$, we have reduction type

$$\text{Type I}_n, \qquad n = \mathrm{ord}_3(\Delta_{12}) = \mathrm{ord}_3(Bb^n) - 9, \qquad m = n, \qquad f = 1.$$

Case 5 : $3 \mid C$**.** If $3 \parallel C$, then

$$3 \mid a_3, a_4, b_2, \ \ 9 \mid a_6, \ \ 27 \mid b_6, b_8$$

and since the polynomial $Y^2 + a_{3,2}Y$ splits and has distinct roots (from $3 \not| Bb^n$ and $9 \parallel C$), we have

$$\text{Type IV}^*, \qquad m = 7, \qquad f = \mathrm{ord}_3(\Delta) - 6 = 5, \qquad c = 3.$$

If, however, $\mathrm{ord}_3(C) = 2$, then applying the substitution $x = 9X$ and $y = 27Y$ leads, as previously, to

$$E' : Y^2 + a_{1,1}XY + a_{3,3}Y = X^3.$$

Since

$$3 \mid a_{3,3}, a_{4,4}, b_{2,2}, \ \ 9 \mid a_{6,6}, \ \ 27 \mid b_{8,8},$$

but $27 \not| b_{6,6}$ ($\mathrm{ord}_3(b_{6,6}) = 2\ \mathrm{ord}_3(a_{3,3}) = 2$), we have reduction type

$$\text{Type IV}, \qquad m = 3, \qquad f = \mathrm{ord}_3(\Delta_{12}) - 2 = 5, \qquad c = 3.$$

Case 6 : $3 \not| a_3$**.** Since we assume that $a_3 \not\equiv -1 \pmod 3$, we may conclude that $a_3 \equiv 1 \pmod 3$. Writing $y = Y + 1$ and $x = X - 1$, our elliptic curve becomes

$$E' : Y^2 + a_1XY + (2 + a_3 - a_1)Y = X^3 - 3X^2 + (3 - a_1)X - (2 + a_3 - a_1)$$

and we have $3 \mid b_2' = a_1^2 - 12$. If $9 \not| (2 + a_3 - a_1)$, then we conclude that

$$\text{Type II}, \qquad m = 1, \qquad f = \mathrm{ord}_3(\Delta) = 3, \qquad c = 1.$$

If $9 \mid (2 + a_3 - a_1)$, then note that $3 \mid a_i$ for $i = 1, 2, 3, 4$, and 6 whereby

$$b_8 \equiv -(a_4')^2 \equiv 9(1 - Cc)^2 \pmod{27}.$$

Note that if 3 divides c then 27 fails to divide b_8. If 3 is coprime to c, then since $Cc^3 = Aa^n + Bb^n$, $Bb^n \equiv 1 \pmod 3$ and 3 fails to divide Aa^n, we conclude that $c \equiv -1 \pmod 3$, whence $27 \not| b_8$. It follows that, in this case, we obtain reduction type

$$\text{Type III}, \qquad m = 2, \qquad f = \mathrm{ord}_3(\Delta) - 1 = 2, \qquad c = 2.$$

This concludes the proof of Lemma 2.1. □

Immediate from Lemma 2.1, we have

Corollary 2.2. *If $n \geqslant 5$ is prime and $abAB$ is divisible by a prime $p \neq 3$, then*

$$ord_p(j(E)) < 0.$$

In particular, if $ab \neq \pm 1$ then E does not have complex multiplication.

Proof. The first part follows directly from part (a) of Lemma 2.1 and the fact that Aa, Bb and Cc are coprime. If $3 \mid ab$, then since $n \geqslant 5$, we have that $\mathrm{ord}_3(j(E)) < 0$. Therefore if $ab \neq \pm 1$, $j(E)$ can not be a rational integer. The desired result then is a consequence of the fact that the j-invariant of an elliptic curve with complex multiplication is an algebraic integer. □

3. Galois Representations

Let $E = E(a, b, c)$ for some primitive solution (a, b, c) to (1). We associate to the elliptic curve E a Galois representation

$$\rho_{E,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_n),$$

the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the n-torsion points $E[n]$ of the elliptic curve E. Recall that Aa, Bb, and Cc are pairwise coprime, and that C is cube free. Without loss of generality we may assume that A and B are nth-power free.

Lemma 3.1. *If $n \geqslant 5$ is a prime and if $ab \neq \pm 1$, then $\rho_{E,n}$ is absolutely irreducible, unless $ab = \pm 2$ and $(|AB|, |Cc^3|, n) = (27, 5, 5)$ or $(3, 125, 7)$.*

Proof. Since both the representation $\rho_{E,n}$ and n are odd, $\rho_{E,n}$ is absolutely irreducible precisely when it is irreducible. If $\rho_{E,n}$ is reducible, then E has a $\mathbb{Q}$-rational subgroup of order n, whereby, from part (c) of Lemma 2.1, E has a $\mathbb{Q}$-rational subgroup of order $3n$. By the work of Kubert [Ku76], Mazur [Ma78] and Kenku [Ke79], the rational points on $X_0(3n)$ are cuspidal for $n \geqslant 11$, a contradiction. In case $n = 5$, the four non-cuspidal rational points on $X_0(15)$ correspond to twists of curves of conductor 50, whereby E necessarily has one of the following four j-invariants :

$$-\frac{25}{2},\ -\frac{5^2 \cdot 241^3}{2^3},\ -\frac{5 \cdot 29^3}{2^5} \ \text{ and } \ \frac{5 \cdot 211^3}{2^{15}}.$$

Similarly, if $n = 7$, the four non-cuspidal rational points on $X_0(21)$ correspond to twists of the curve of conductor 162 denoted $162C$ in Cremona's tables. E therefore has one of the following four j-invariants :

$$\frac{3^3 \cdot 5^3}{2},\ -\frac{3^2 \cdot 5^6}{2^3},\ -\frac{3^3 \cdot 5^3 \cdot 383^3}{2^7} \ \text{ and } \ \frac{3^2 \cdot 5^3 \cdot 101^3}{2^{21}}.$$

Applying the formula for $j(E)$ in part (a) of Lemma 2.1 and using the coprimality of Aa, Bb and Cc, together with the fact that Aa is coprime to 3, leads to the conclusion that the only curves $E(a, b, c)$ with these j-invariants correspond to the equations

$$2 \cdot 1^5 + 27 \cdot (-1)^5 = 25 \cdot (-1)^3 \quad \text{and} \quad 1 \cdot 2^5 + 27 \cdot (-1)^5 = 5 \cdot 1^3,$$

in case $n = 5$, and to

$$2 \cdot 1^7 + 3 \cdot (-1)^7 = (-1)^3 \quad \text{and} \quad 1 \cdot 2^7 + 3 \cdot (-1)^7 = 1 \cdot 5^3,$$

in case $n = 7$. This completes the proof of Lemma 3.1. □

Here, the presence of non-cuspidal, non-CM rational points on $X_0(N)$ for $N \in \{15, 21\}$ leads to some minor complications. Corresponding issues are overlooked in the proofs of Theorem 2.2 of [DM97] and Corollary 3.1 of [BS03] (which require correction to account for "non-trivial" rational

points on $X_0(14)$ and $X_0(21)$, and on $X_0(14)$, respectively). These difficulties do not significantly affect the main results of either paper.

Following Serre [Ser87], we can associate to each representation $\rho_{E,n}$ an Artin conductor N_n^E. Work of Kraus enables us to calculate N_n^E exactly (here, we write f_p as shorthand for $\mathrm{ord}_p(N(E))$).

THEOREM 3.2. *(Kraus [Kr97a]) If $n \geqslant 5$ is prime, the Artin conductor of $\rho_{E,n}$ is equal to*

$$N_n^E = \prod_{p \neq n} p^{f_p - f_p'},$$

where f_p' is calculated as follows:

i) *If E has good or additive reduction at p then $f_p' = 0$.*

ii) *If E has multiplicative reduction at p then*

$$f_p' = \begin{cases} 0 & \text{if } n \text{ does not divide } v_p(\Delta(E)), \\ 1 & \text{if } n \text{ divides } v_p(\Delta(E)). \end{cases}$$

Here, $\Delta(E)$ is a minimal discriminant of E. Combining this with the proof of Lemma 2.1 (where we explicitly describe the relevant reduction types) yields

COROLLARY 3.3. *The Artin conductor of $\rho_{E,n}$ is*

$$N_n^E = Rad^*(AB)Rad^*(C)^2\epsilon_3'$$

where

$$\epsilon_3' = \begin{cases} 3^2 & \text{If } 9 \mid (2 + C^2Bb^n - 3Cc), \\ 3^3 & \text{If } 3 \parallel (2 + C^2Bb^n - 3Cc), \\ 3^4 & \text{If } ord_3(Bb^n) = 1, \\ 3^3 & \text{If } ord_3(Bb^n) = 2, \\ 1 & \text{If } ord_3(B) = 3, \\ 3 & \text{If } ord_3(Bb^n) > 3 \text{and } ord_3(B) \neq 3, \\ 3^5 & \text{If } 3 \mid C. \end{cases}$$

Let $\overline{\mathbb{F}_n}$ be an algebraic closure of the finite field $\mathbb{F}_n$ and ν be any prime of $\overline{\mathbb{Q}}$ extending n. To a holomorphic newform f of weight $k \geqslant 1$ and level N, we associate a continuous, semisimple representation

$$\rho_{f,\nu} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}_n})$$

unramified outside of Nn and satisfying, if $f(z) = \sum_{n=1}^{\infty} c_n q^n$ for $q := e^{2\pi i z}$,

$$\mathrm{trace}\rho_{f,\nu}(\mathrm{Frob}_p) \equiv c_p \pmod{\nu}$$

for all p coprime to Nn. Here, Frob_p is a Frobenius element at the prime p.

If the representation $\rho_{E,n}$, after extending scalars to $\overline{\mathbb{F}_n}$, is equivalent to $\rho_{f,\nu}$, for some newform f, then we say that $\rho_{E,n}$ is modular, arising from f.

LEMMA 3.4. *Suppose that $n \geqslant 5$ is a prime and that $\rho_{E,n}$ is associated to a primitive solution (a, b, c) with $ab \neq \pm 1$. Put*

$$N_n(E) = \begin{cases} N_n^E & \text{if } n \not\mid ABC, \\ nN_n^E & \text{if } n \mid AB, \\ n^2N_n^E & \text{if } n \mid C. \end{cases}$$

Then the representation $\rho_{E,n}$ arises from a cuspidal newform of weight 2, level $N_n(E)$ and trivial Nebentypus character, unless E corresponds to one of the equations

$$1 \cdot 2^5 + 27 \cdot (-1)^5 = 5 \cdot 1^3 \quad or \quad 1 \cdot 2^7 + 3 \cdot (-1)^7 = 1 \cdot 5^3.$$

Proof. By the recent proof of the Shimura-Taniyama-Weil conjecture [BCDT01], we have that E and hence the representation $\rho_{E,n}$ is modular. Since Lemma 3.1 implies, with the noted exceptions, that $\rho_{E,n}$ is absolutely irreducible, it is therefore a consequence of a theorem of Ribet [Ri90] that $\rho_{E,n}$ arises from a cuspidal newform with weight 2, level $N_n(E)$, and trivial Nebentypus character. □

4. Some useful propositions

In this section, we will collect a variety of results that enable us, under certain assumptions, to discount the possibility of $\rho_{E,n}$ arising from a particular newform of level $N_n(E)$. These correspond to Propositions 4.1, 4.3 and 4.6 of Bennett and Skinner [BS03], respectively, and possess very similar proofs. We will therefore, for the most part, only indicate where significant changes to the arguments of [BS03] are required.

Proposition 4.1. *Suppose $n \geqslant 5$ is a prime and that E is the curve associated to a primitive solution (a, b, c). If*

$$N_n(E) \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60\}$$

then $ab = \pm 1$, unless E corresponds to one of the equations

$$1 \cdot 2^5 + 27 \cdot (-1)^5 = 5 \cdot 1^3 \quad or \quad 1 \cdot 2^7 + 3 \cdot (-1)^7 = 1 \cdot 5^3.$$

Proof. This is immediate from Lemma 3.4 and the fact that there are no weight 2 cuspidal newforms at these levels. □

Proposition 4.2. *Suppose $n \geqslant 5$ is a prime and that E is a curve associated to a primitive solution (a, b, c) with $ab \neq \pm 1$ which does not correspond to one of the equations*

$$1 \cdot 2^5 + 27 \cdot (-1)^5 = 5 \cdot 1^3 \quad or \quad 1 \cdot 2^7 + 3 \cdot (-1)^7 = 1 \cdot 5^3.$$

Suppose further that $f = \sum_{m=1}^{\infty} c_m q^m$ is a newform of weight 2 and level $N_n(E)$ giving rise to ρ_n^E and that K_f is a number field containing the Fourier coefficients of f. If p is a prime, coprime to nN_n^E, then n divides

$$Norm_{K_f/\mathbb{Q}}(c_p - a_p)$$

where $a_p \in S_p$, with

$$S_p = \{x : |x| < 2\sqrt{p}, \ \ x \equiv p + 1 \pmod 3\} \cup \{p + 1\},$$

if $p \equiv 1, 4, 5, 7, 16, 17, 20 \pmod{21}$, and

$$S_p = \{x : |x| < 2\sqrt{p}, \ \ x \equiv p + 1 \pmod 3\} \cup \{p + 1, -p - 1\},$$

otherwise.

Proof. This follows, essentially, from the fact that, via part (c) of Lemma 2.1, the curves $E(a, b, c)$ all have rational 3-torsion. This enables us to restrict the Fourier coefficients of a newform that can give rise to ρ_n^E. To be precise, suppose that p is a prime of good reduction for E. Since E has a rational 3-torsion point, it follows that $3 \mid \#E(p)$ where $\#E(p)$ is the number of points on E over $\mathbb{F}_p$ and so the pth Fourier coefficient of E satisfies $a_p \equiv p + 1 \pmod 3$. If f is a newform giving rise to ρ_n^E, with pth Fourier coefficient c_p, then we have $c_p \equiv a_p \pmod \nu$ for a prime ν lying above n, and hence n divides $\mathrm{Norm}_{K_f/\mathbb{Q}}(c_p - a_p)$. By the Weil bounds, $|a_p| < 2\sqrt{p}$. If, on

the other hand, $p \mid ab$, then $\mathrm{trace}\rho_n^E(\mathrm{Frob}_p) = p+1$, if E has split multiplicative reduction at p, and $\mathrm{trace}\rho_n^E(\mathrm{Frob}_p) = -(p+1)$, if E has non-split multiplicative reduction at p. An application of Lemma 2.1 thus completes the proof. □

Proposition 4.3. *Suppose $n \geqslant 5$ is a prime and E is a curve associated to a primitive solution with $ab \neq \pm 1$. Suppose that ρ_n^E arises from a newform having CM by an order in an imaginary quadratic field K. Then one of the following holds:*

(a) $ab = \pm 2^r$, $r > 0$, $2 \not| ABC$, and 2 splits in K.

(b) $n = 5, 7$ or 13, n splits in K, and either the modular Jacobian $J_0(3n)$ has no quotient of rank 0 over K, or $ab = \pm 2^r 3^s$ with $s > 0$ and 3 ramifies in the field K.

Proof. This follows from a combination of the arguments leading to Proposition 4.6 of [BS03] and Proposition 4.2 of [DM97], themselves dependent upon Corollary 4.3 of [Ma78]. □

Exactly analogous to Proposition 4.4 of [BS03], we can in fact deduce the following result, though we will not have need for it in our deliberations; the proof depends upon somewhat careful consideration of potential reduction types.

Proposition 4.4. *Suppose $n \geqslant 5$ is a prime and E is a curve associated to a primitive solution (a, b, c). Suppose also that E' is another elliptic curve defined over $\mathbb{Q}$ such that $\rho_n^E \cong \rho_n^{E'}$. Then the denominator of the j-invariant $j(E')$ is not divisible by any odd prime $p \neq n$ dividing C.*

5. Theorems 1.5, 1.6 and 1.7

We will begin by proving Theorems 1.5, 1.6 and 1.7. The first of these is necessary for the subsequent proofs of Theorems 1.1, 1.3 and 1.4. To prove Theorem 1.5, we are led to consideration of modular forms of level N, in the following set

$$\{27, 36, 49, 75, 81, 108, 121, 147, 169, 225, 289, 361, 363, 441, 507, 588, 675, 867,\\ 1083, 1089, 1323, 1521, 2025, 2601, 3249, 3267, 4563, 7803, 9747\}$$

(from Proposition 4.1, we may immediately suppose that $N \neq 1, 3, 4, 9, 12$ and 25). To analyse forms at these levels, we utilize Stein's Modular Forms Database [St03], together with some auxilliary computations (for certain larger levels). Details for these latter calculations are available in [BVY03]. We find that the following forms have CM by an order of an imaginary quadratic field (here, we employ Stein's numbering conventions, though there may be some minor variation at levels 4563,

7803 and 9747) :

Newform	CM field	Newform	CM field
$27(1)$	$\mathbb{Q}(\sqrt{-3})$	$1089(5)$	$\mathbb{Q}(\sqrt{-11})$
$36(1)$	$\mathbb{Q}(\sqrt{-3})$	$1323(1,2,13)$	$\mathbb{Q}(\sqrt{-3})$
$49(1)$	$\mathbb{Q}(\sqrt{-7})$	$1521(1,2,7)$	$\mathbb{Q}(\sqrt{-3})$
$108(1)$	$\mathbb{Q}(\sqrt{-3})$	$1521(21)$	$\mathbb{Q}(\sqrt{-39})$
$121(1)$	$\mathbb{Q}(\sqrt{-11})$	$2601(21,22)$	$\mathbb{Q}(\sqrt{-3})$
$225(1,2)$	$\mathbb{Q}(\sqrt{-3})$	$3249(19,20)$	$\mathbb{Q}(\sqrt{-3})$
$225(6)$	$\mathbb{Q}(\sqrt{-15})$	$3267(1,2,4,12,17)$	$\mathbb{Q}(\sqrt{-3})$
$243(1,2)$	$\mathbb{Q}(\sqrt{-3})$	$3969(7,8,24)$	$\mathbb{Q}(\sqrt{-7})$
$361(1)$	$\mathbb{Q}(\sqrt{-19})$	$4563(3,6,9,12,17)$	$\mathbb{Q}(\sqrt{-3})$
$441(1,2)$	$\mathbb{Q}(\sqrt{-3})$	$4563(4,5)$	$\mathbb{Q}(\sqrt{-39})$
$441(5,7)$	$\mathbb{Q}(\sqrt{-7})$	$7803(3,10,13,20,23,32,33)$	$\mathbb{Q}(\sqrt{-3})$
$675(1,3,5)$	$\mathbb{Q}(\sqrt{-3})$	$7803(11,12)$	$\mathbb{Q}(\sqrt{-51})$
$675(17)$	$\mathbb{Q}(\sqrt{-15})$	$9747(2,5,15,21,22,35,36)$	$\mathbb{Q}(\sqrt{-3})$
$1089(1,2,12)$	$\mathbb{Q}(\sqrt{-3})$		

Applying Proposition 2.1 of Kamienny [Ka90], we may conclude that $J_0(39)$ has a finite quotient over both $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{-51})$. Further, since both the elliptic curve over $\mathbb{Q}$ denoted $21A$ in Cremona [Cr92], together with its $\mathbb{Q}(\sqrt{-3})$-quadratic twist (denoted $63A$) both have rank 0 over $\mathbb{Q}$, it follows that this curve has rank 0 over $\mathbb{Q}(\sqrt{-3})$. This ensures that $J_0(21)$ has a finite quotient over $\mathbb{Q}(\sqrt{-3})$. Similarly, the elliptic curve over $\mathbb{Q}$ denoted $15A$ in Cremona [Cr92], together with it's $\mathbb{Q}(\sqrt{-19})$-quadratic twist (denoted $5415K$) both have rank 0 over $\mathbb{Q}$ and hence $J_0(15)$ has a finite quotient over $\mathbb{Q}(\sqrt{-19})$. Checking the splitting of the primes $n = 5, 7$ and 13 in the fields represented in the above table, it follows that the forms tabulated above can not give rise to ρ_n^E unless one of the following occurs :

(i) $ab = \pm 2^r, r > 0$ and the newform is one of $49(1)$, $225(6)$, $441(5,7)$, $675(17)$ or $3969(7,8,24)$.

(ii) $n = 7$, $ab = \pm 2^r 3^s$ with $s > 0$ and the newform has CM by $\mathbb{Z}[\sqrt{-3}]$.

(iii) $n = 13$, $ab = \pm 2^r 3^s$ with $s > 0$ and the newform has CM by $\mathbb{Z}[\sqrt{-3}]$ or $\mathbb{Z}[\sqrt{-51}]$.

(iv) $n = 5$ and the newform is one of $121(1)$, $1089(5)$, $1521(21)$, $4563(4,5)$ or $7803(11,12)$.

In case (i) (or in cases (ii) and (iii), if, additionally, $r > 0$) our Frey curve $E = E(a,b,c)$ has multiplicative reduction at 2 and hence corresponding trace of Frobenius is ± 3. It follows that n divides $\mathrm{Norm}_{K_f/\mathbb{Q}}(c_2 \pm 3)$ and since, for the forms under consideration, excepting only $675(17)$ and the forms at level 3969, we have

$$c_2 \in \left\{0, \pm 1, \pm\sqrt{5}, \pm\sqrt{7}\right\},$$

this contradicts $n \geqslant 5$ prime. In the case of form $675(17)$, we have $c_2 = (-3 \pm \sqrt{5})/2$ and so n dividing $\mathrm{Norm}_{K_f/\mathbb{Q}}(c_2 \pm 3)$ implies $n = 19$. Similarly, for the level 3969 forms, consideration of c_2 leads to the conclusion that $n \in \{7, 37\}$. On the other hand, in every case, $c_7 = 0$ and the fact that $a_7 \in \{-4, -1, 2, 5\}$ together imply that $n = 5$, a contradiction.

If we are in situation (ii) or (iii) with $r = 0$, then $ab = \pm 3^s$ with $s > 0$ and we necessarily have $3^n \pm 1 = Cc^3$ with $n = 7$ or $n = 13$. It follows that

$$|C| \in \{2 \cdot 1093, 2^2 \cdot 547, 2 \cdot 797161, 2^2 \cdot 398581\},$$

in each case contradicting $|C| < 20$.

Finally, in case (iv), if $E(a, b, c)$ gives rise to the newform denoted 121(1) in Stein's tables, then there exist integers a, b and c for which $a^5 + 27b^5 = 11c^3$, a contradiction modulo 11. Similarly, form 1089(5) leads to $a^5 + 3^\delta b^5 = 11c^3$, with $\delta \in \{0, 2\}$, a contradiction unless $\delta = 0$. In the case of form 1521(21), we have $c_2 = \theta$ where $\theta^4 - 8\theta^2 + 3 = 0$ and so none of $\mathrm{Norm}_{K_f/\mathbb{Q}}(c_2 \pm 3)$ and $\mathrm{Norm}_{K_f/\mathbb{Q}}(c_2)$ are divisible by 5. Forms 4563(4) and 4563(5) have $c_2 = \theta$ where $\theta^4 - 11\theta^2 + 27 = 0$ and $\theta^4 - 5\theta^2 + 3 = 0$, respectively, and so, once again, $\mathrm{Norm}_{K_f/\mathbb{Q}}(c_2 \pm 3)$ and $\mathrm{Norm}_{K_f/\mathbb{Q}}(c_2)$ are coprime to 5. Forms 7803(11) and 7803(12) have $c_{11} = \pm\sqrt{17}$ and so, since $a_{11} \in \{0, \pm 3, \pm 6, \pm 12\}$,

$$\mathrm{Norm}_{K_f/\mathbb{Q}}(c_{11} - a_{11}) \in \{-17, -8, 19, 127\}.$$

In conclusion, the only newform listed in the previous table that can give rise to our representation is 1089(5), in which case we have $A = B = 1$, $C = 11$ and $n = 5$.

To complete the proof of Theorem 1.5 for the forms that do not have complex multiplication, we appeal to Proposition 4.2. In each case, we obtain a result at least as strong as that stated in Theorem 1.5. For example, in case $C = 11$ we consider forms at levels $N \in \{121, 363, 1089, 3267\}$ and find that Proposition 4.2 yields a contradiction for all prime $n \geqslant 7$, except for forms 1089(5,13,14) and 3267(1) (with $n = 7$), 363(8,9,10), 1089(17,19,21,23) and 3267(33) (with $n = 11$), and form 3267(25) (with $n = 13$). A similar analysis for the other values of C completes the proof of Theorem 1.5. Details are again available in [BVY03]. We note that our techniques do not prove decisive in case $C = 6, 10$ or 14. This reflects the fact that while, as we shall observe in Section 6, there are no elliptic curves over $\mathbb{Q}$ with rational a 3-torsion point, conductor $3^\tau p^2$ and lacking complex multiplication, the same is no longer true if we consider conductors of the form $2^\alpha 3^\tau p^2$.

Finally, to prove Theorems 1.6 and 1.7, we are led to consider newforms at level $N = 3^\delta p$ (with $\delta \in \{1, 2, 3\}$, if $\beta = 0$, and $\delta = 5$ if $\beta > 0$), for small prime p. Our argument is essentially identical to that described in the preceding paragraph; i.e. we appeal to Proposition 4.2. Again, details are available in [BVY03].

6. Elliptic curves with rational 3-torsion

In this section, we will apply Theorem 1.5 to completely characterize elliptic curves over $\mathbb{Q}$ that possess both a rational 3-torsion point and conductor $3^\tau p^\omega$ for nonnegative integers τ and ω, and p prime. Since curves of conductor $2^\omega 3^\tau$ have been classified by Coghlan [Co67] (see also [CS71] and Table 4a of [BK75]), we will henceforth assume that $p > 3$ and $\omega > 0$. We note that the special case $p = 5$ was considered previously by Hadano [Ha82]. We have the following proposition.

Proposition 6.1. *Suppose that $p > 3$ is prime and that $E/\mathbb{Q}$ is an elliptic curve with a rational 3-torsion point and conductor $3^\tau p^\omega$ (where τ is a nonnegative integer and $\omega \in \{1, 2\}$). Then E is isogenous over $\mathbb{Q}$ to a curve of the form*

$$y^2 + a_1 xy + a_3 y = x^3$$

with coefficients given in the following table:

p	a_1	a_3	N
any	0	$p^\alpha,\ \alpha \in \{1,2\}$	$3^t \cdot p^2,\ t \in \{2,3\}$
any	0	$3^t p^\alpha,\ t, \alpha \in \{1,2\}$	$3^5 \cdot p^2$
5	-18	9	$3^5 \cdot 5$
5	18	225	$3^5 \cdot 5$
7	6	1	$3^3 \cdot 7$
7	6	7	$3^3 \cdot 7$
19	2	1	19
37	4	1	37
$3s^3 \mp 1,\ s \in \mathbb{N}$	$\pm 9s$	9	$3^5 \cdot p$
$9s^3 \mp 1,\ s \in \mathbb{N}$	$\pm 9s$	3	$3^5 \cdot p$
$3s^3 \mp 1,\ s \in \mathbb{N}$	$9s$	$9p$	$3^5 \cdot p$
$9s^3 \mp 1,\ s \in \mathbb{N}$	$9s$	$3p$	$3^5 \cdot p$
$3^{2t+1} \pm 3^{t+1} + 1,\ t \in \mathbb{N}$	$3 \pm 3^{t+2}$	1	$3^2 \cdot p$
$s^3 \mp 3,\ s \in \mathbb{N}$	$\pm 3s$	3	$3^4 \cdot p$
$s^3 \mp 9,\ s \in \mathbb{N}$	$\pm 3s$	9	$3^3 \cdot p$
$s^3 \mp 3,\ s \in \mathbb{N}$	$3s$	p	$3^4 \cdot p$
$s^3 \mp 9,\ s \in \mathbb{N}$	$3s$	p	$3^3 \cdot p$
$s^3 \mp 3^t,\ s \in \mathbb{Z}, t \geqslant 4$	$\pm s$	3^{t-3}	$3 \cdot p$
$s^3 \mp 3^t,\ s \in \mathbb{Z}, t \geqslant 4$	$3s$	p	$3^2 \cdot p$

Proof. We begin our deliberations by supposing that E is an elliptic curve over $\mathbb{Q}$ with a rational 3-torsion point and conductor $3^\tau p^\omega$. E is thus isomorphic to a curve of the form

$$F : y^2 + a_1 xy + a_3 y = x^3$$

where a_1 and a_3 are integers (with, say, $a_3 > 0$). We further suppose that if $q | a_1$ then q^3 fails to divide a_3, since otherwise we may consider the isomorphic elliptic curve $F' : y^2 + (a_1/q)xy + (a_3/q^3)y = x^3$. It follows that the discriminant of F satisfies

$$\Delta(F) = a_3^3(a_1^3 - 27a_3) = \pm 3^\alpha p^\beta,$$

whereby we can write $a_3 = 3^\kappa p^\delta$ for nonnegative integers κ and δ. Here $\beta > 0$ since the same is true for ω. If $a_1 = 0$, then the above assumptions imply that $\kappa \in \{0,1,2\}$ and $\delta \in \{1,2\}$. In this case, E has CM by an order in $\mathbb{Q}(\sqrt{-3})$ and, via an application of Tate's algorithm, corresponding conductor $3^\tau p^2$ where $\tau = 2$ or 3 (if $\alpha = 0$), and $\tau = 5$ (if $\alpha > 0$).

For the remainder of this section, we will suppose that $a_1 \neq 0$. We have

$$a_1^3 = 3^{3+\kappa} p^\delta \pm 3^{\alpha - 3\kappa} p^{\beta - 3\delta}.$$

We will proceed by separating the proof into two cases, depending on whether or not p divides a_1. If $p \nmid a_1$, then there exists a nonzero integer x and a nonnegative integer m such that one of the following occurs :

$$\begin{array}{cc} (i) & x^3 = p^n \pm 3^m \\ (ii) & 3^m x^3 = p^n \pm 1 \\ (iii) & x^3 = 3^m p^n \pm 1, \end{array}$$

where

$$n = \begin{cases} \delta \ \text{ if } \ p \mid a_3 \\ \beta \ \text{ if } \ p \nmid a_3. \end{cases}$$

Applying Theorem 1.5, we conclude immediately that the largest prime factor of n is at most 3. We first suppose that $n \geqslant 2$. If we have a solution to equation (i) with n even, then we have an

integral solution to the equation $Y^2 = X^3 \pm 3^m$ with Y a power of p (for $p > 3$). Work of Coghlan [Co67] (see also Table 4a of [BK75]) implies that this cannot occur. If, on the other hand, $3 \mid n$ in equation (i), then there exist nonzero integers X and Y such that $X^3 - Y^3 = 3^m$ and $p \mid XY$. Factoring the left hand side of this equation enables us to conclude that $XY = -2$, contradicting the fact that $p \mid XY$.

If we have (ii) and n is even, then, since p is odd, we necessarily have $3^m x^3 = y^2 - 1$ for some odd integer y. Applying techniques based upon lower bounds for linear forms in elliptic logarithms (as implemented, say, in Simath [Sim98]; see the paper of Stroeker and Tzanakis [ST94] for a good exposition of this method), we find that the only such integers (x, y, m) are given by

$$(x, y, m) \in \{(2, \pm 3, 0), (2, \pm 5, 1), (0, \pm 1, m)\}.$$

It follows that the only solution to our original problem corresponds to $3 \cdot 2^3 = 5^2 - 1$. In this case, it is easy to see that necessarily either $a_1 = -18$ and $a_3 = 9$, or $a_1 = 18$ and $a_3 = 225$. In each case, E has conductor $3^5 \cdot 5$. If $3 \mid n$ in (ii), then there exist positive integers x and y with $p \mid y$ for which

$$y^3 - 3^m x^3 = \pm 1. \tag{3}$$

The inequality

$$\left|u^3 - 3v^3\right| \geqslant \max\{|u|, |v|\}^{0.24},$$

valid for all integers u, v (see Theorem 6.1 of [Be97]), implies that $(x, y, m) = (1, 2, 2)$, again contradicting $p \mid y$ for $p > 3$.

Finally, if we have a solution to (iii) with n even, then if m is even, we deduce the existence of a positive integer $y > 3$ such that $x^3 - y^2 = \pm 1$. An old result of Euler [Eu38] thus implies a contradiction. If n is even and m is odd, then $3y^2 = x^3 \pm 1$, whereby, via Simath, we find that there are no solutions with $y \neq 0$. If $3 \mid n$, then we again obtain a positive solution to (3), contrary to $p \mid y$, $p > 3$.

Next, suppose we have a solution to one of equations (i)–(iii) with $n = 1$. The corresponding conductors again may be computed via Tate's algorithm, as in Section 2. We need to consider $\delta = 0$ and $\delta \neq 0$ separately. In case (i), we have $p = x^3 \mp 3^m$. If $m = 0$, necessarily $p = 7$ (with $(a_1, a_3) = (6, 1)$ or $(6, 7)$ and $N = 3^3 \cdot 7$). If $m \in \{1, 2\}$, then $(a_1, a_3) = (\pm 3x, 3^m)$ or $(3x, p)$ and $N = 3^{5-m} \cdot p$. If $3 \mid m$ for $m > 0$, say $m = 3t$, it follows that $p = 3^{2t+1} \pm 3^{t+1} + 1$. We thus have either $a_1 = 3^t \pm 1$ and $a_3 = 3^{3t-3}$, or $a_1 = 3 \pm 3^{t+1}$ and $a_3 = p$. For the first pair (a_1, a_3), we find that, if $m = 3$ (so that $p = 19$ or $p = 37$), then $N = p$, while $m > 3$ a multiple of 3 yields conductor $N = 3 \cdot p$. For the second pair, we have $N = 3^2 \cdot p$ in all cases. Lastly, if $m \equiv \pm 1 \pmod 3$ and $m > 3$, we have either $a_1 = \pm x$ and $a_3 = 3^{m-3}$, or again $a_1 = 3x$ and $a_3 = p$. In the first case, we have $N = 3 \cdot p$, while the second yields $N = 3^2 \cdot p$.

In case (ii), we have $p = 3^m x^3 \mp 1$. If $3 \mid m$, we again find that $p = 7$, with $a_1 = 6$, $a_3 = 1$, or $a_1 = 6$, $a_3 = 7$ (so that $N = 3^3 \cdot 7$). Otherwise, if $m \equiv 1 \pmod 3$, we can write $p = 3s^3 \pm 1$ (for $s \in \mathbb{N}$) with $(a_1, a_3) = (\mp 9s, 9)$ or $(9s, 9p)$ and $N = 3^5 \cdot p$. If $m \equiv -1 \pmod 3$, we can write $p = 9s^3 \pm 1$ with $(a_1, a_3) = (\mp 9s, 3)$ or $(9s, 3p)$, and, again, $N = 3^5 \cdot p$.

If we have a solution to equation (iii) with $n = 1$, then $x^3 = 3^m p \pm 1$. The case $m = 0$ leads to the previously considered curves with $p = 7$, of conductor $3^3 \cdot 7$. If $m > 0$, after factoring $x^3 \mp 1$, we find that $m \geqslant 2$ and

$$p = 3^{2m-3} \pm 3^{m-1} + 1.$$

If $m = 2$, then $p = 7$ and so $(a_1, a_3) = (12, 1)$ or $(12, 63)$. These curves are isogenous to those previously encountered with $(a_1, a_3) = (6, 7)$ and $(6, 1)$, respectively. If $m \geqslant 3$, then $(a_1, a_3) = (3 \pm 3^m, 1)$ or $(3^{m-1} \pm 1, 3^{3m-6} \pm 3^{2m-4} + 3^{m-3})$. The first case leads to $N = 3^2 \cdot p$, while the second gives $N = 19$ or 37 (if $m = 3$), and $N = 3 \cdot p$ (if $m > 3$). The curves with conductor $3^2 \cdot p$

are isogenous to those with $(a_1, a_3) = (3 \pm 3^m, 1)$. The curves with conductor dividing $3 \cdot p$ may be readily shown to be isogenous to those with $(a_1, a_3) = (3^{m-2} \pm 1, 3^{3m-9})$. This completes our classification in case $p \not| a_1$.

If, on the other hand, p divides $a_1 \neq 0$ (so that, additionally, $p \mid a_3$) then

$$a_1^3 = 3^{\kappa+3}p^{\delta} \pm 3^{\alpha-3\kappa}p^{\beta-3\delta},$$

where $\delta \in \{1, 2\}$ (whence $\beta = 4\delta$). Since $a_1 \neq 0$, dividing the above equation by p^{δ} and a suitable power of 3 implies the existence of positive integers x and m such that

$$p^{3-\delta}x^3 = 3^m \pm 1.$$

Since the right hand side of this equation is even, x is necessarily even and hence $8 \mid 3^m \pm 1$. It follows that $p^{3-\delta}x^3 = 3^m - 1$, where $m = 2m_1$ for some nonnegative integer m_1. We thus have

$$p^{3-\delta}x^3 = (3^{m_1} - 1)(3^{m_1} + 1)$$

and, since $\gcd(3^{m_1} - 1, 3^{m_1} + 1) = 2$, either $3^{m_1} - 1 = 2^{\zeta}a^3$ or $3^{m_1} + 1 = 2^{\zeta}a^3$ for some positive integer a and $\zeta \in \{1, 2\}$. In either case, applying Theorem 1.5, we find that there are no solutions if m_1 is divisible by a prime exceeding 3. If m_1 is even, then again applying Simath to the elliptic curves

$$Y^2 = 2X^3 + 1, \;\; Y^2 = 2X^3 - 1, \;\; Y^2 = 4X^3 + 1 \;\text{ and }\; Y^2 = 4X^3 - 1,$$

we conclude that the only positive integers (X, Y) satisfying any of these equations are given by

$$(X, Y) \in \{(1, 1), (2, 2), (5, 11)\}.$$

None of these provide solutions to our original problem. If m_1 is divisible by 3, we are led to consider equations of the shape $b^3 - 2^{\zeta}a^3 = \pm 1$. The inequality

$$\left|u^3 - 2v^3\right| \geqslant \max\{|u|, |v|\}^{0.53},$$

valid for all integers u, v (again, see Theorem 6.1 of [Be97]) thus implies that $(a, b, \zeta) = (1, 1, 1)$, contradicting the fact that, in our situation, 3 divides b. It follows, since we have assumed $a_1 \neq 0$, that $m_1 = 1$, whereby $m = 2$, a contradiction. This completes our classification. □

7. Theorems 1.1, 1.3 and 1.4

To prove Theorems 1.1, 1.3 and 1.4, we will combine Proposition 6.1 with a result of Kraus (Lemme 1 of [Kr97b]) and the Proposition of Appendice II of Kraus and Oesterlé [KO92] (regarding this last assertion, note the comments in the Appendice of [Kr97b]). We define

$$\mu(N) = N \prod_{l|N} \left(1 + \frac{1}{l}\right),$$

where the product is over prime l.

Proposition 7.1. *(Kraus) Let N be a positive integer and $f = \sum_{n \geqslant 1} c_n q^n$ be a weight 2, level N newform, normalized so that $c_1 = 1$. Suppose that for every prime p with $p \leqslant \mu(N)/6$ we have $c_p \in \mathbb{Z}$. Then we may conclude that $c_n \in \mathbb{Z}$ for all $n \geqslant 1$.*

Proposition 7.2. *(Kraus and Oesterlé) Let k be a positive integer, χ a Dirichlet character of conductor N and $f = \sum_{n \geqslant 0} c_n q^n$ be a modular form of weight k, character χ for $\Gamma_0(N)$, with $c_n \in \mathbb{Z}$. Let p be a rational prime. If $c_n \equiv 0 \pmod{p}$ for all $n \leqslant \mu(N)k/12$, then $c_n \equiv 0 \pmod{p}$ for all n.*

We now proceed with the proofs of Theorems 1.1, 1.3 and 1.4; in each case, from Lemma 3.4, we may assume the existence of a weight 2, level N cuspidal newform f (with trivial character), where

$$N \in \left\{p, 3p, 9p, 27p, 243p, 3p^2, 9p^2, 27p^2\right\}.$$

If f has at least one Fourier coefficient that is not a rational integer, then, from Proposition 7.1, there is a prime l with

$$l \leqslant \begin{cases} 6p(p+1) & \text{if } N \in \left\{3p^2, 9p^2, 27p^2\right\} \\ 6(p+1) & \text{if } N \in \{p, 3p, 9p, 27p\} \\ 54(p+1) & \text{if } N = 243p, \end{cases} \tag{4}$$

such that $c_l \notin \mathbb{Z}$. It follows from Proposition 4.2 that n divides $\mathrm{Norm}_{K_f/\mathbb{Q}}(c_l - a_l)$, where a_l is the lth Fourier coefficient corresponding to the Frey curve $E(a, b, c)$. Since $a_l \in \mathbb{Z}$ (whereby $a_l \neq c_l$), if l is coprime to $3p$, the Weil bounds imply that

$$n \leqslant \left(l + 1 + 2\sqrt{l}\right)^{[K_f:\mathbb{Q}]} = \left(\sqrt{l} + 1\right)^{2[K_f:\mathbb{Q}]}, \tag{5}$$

where, as previously, K_f denotes the field of definition for the Fourier coefficients of the form f. Similarly, if $l = 3$, we have $n \leqslant 8^{[K_f:\mathbb{Q}]}$, while $l = p$ implies that $n \leqslant (2(p+1))^{[K_f:\mathbb{Q}]}$. Next, we note that $[K_f : \mathbb{Q}] \leqslant g_0^+(N)$ where $g_0^+(N)$ denotes the dimension (as a $\mathbb{C}$-vector space) of the space of cuspidal, weight 2, level N newforms. Applying Propositions 1.40 and 1.43 of Shimura [Sh71], together with the Théorème of Appendice I of [Kr97b], we find, if $p \equiv p_0 \pmod{12}$ with $0 < p_0 < 12$, that

$$g_0^+(3p^2) = \frac{p^2 - p - 7 + p_0}{6} \leqslant \frac{p^2 - p + 4}{6}.$$

Similarly

$$g_0^+(9p^2) \leqslant \frac{5p^2 - 11p + 14}{12}, \quad g_0^+(27p^2) \leqslant \frac{4p^2 - 4p - 3}{3}, \quad g_0^+(p) \leqslant \frac{p+1}{12},$$

$$g_0^+(3p) \leqslant \frac{p+5}{6}, \quad g_0^+(9p) \leqslant \frac{5p+1}{12}, \quad g_0^+(27p) \leqslant \frac{4p-2}{3} \text{ and } g_0^+(243p) = 12p - 12.$$

Combining these with inequalities (4) and (5), we may therefore conclude that

$$n \leqslant \begin{cases} \left(\sqrt{6p(p+1)} + 1\right)^{\frac{8p^2-8p-6}{3}} & \text{if } N \in \{3p^2, 9p^2, 27p^2\} \\ \left(\sqrt{6(p+1)} + 1\right)^{\frac{8p-4}{3}} & \text{if } N \in \{p, 3p, 9p, 27p\} \\ \left(\sqrt{54(p+1)} + 1\right)^{24p-24} & \text{if } N = 243p. \end{cases} \tag{6}$$

It follows, after routine calculation, that

$$n \leqslant \begin{cases} p^{4p^2} & \text{if } N \in \{3p^2, 9p^2, 27p^2\} \\ p^{2p} & \text{if } N \in \{p, 3p, 9p, 27p\} \\ p^{28p} & \text{if } N = 243p, \end{cases}$$

where these inequalities are a consequence of (6) for $p \geqslant 5$ (in case N is one of $3p^2, 9p^2$ or $27p^2$), $p \geqslant 43$ (if N is $p, 3p, 9p$ or $27p$) and $p \geqslant 17$ (if $N = 243p$). For smaller values of p, examination of Theorems 1.5, 1.6 and 1.7 completes our analysis.

It remains, then, to consider the case when the form f has rational integer Fourier coefficients c_n for all $n \geqslant 1$. In such a situation, f corresponds to an isogeny class of elliptic curves over $\mathbb{Q}$ with conductor N. Define

$$f^* = \sum_{n \geqslant 1, (n,3p)=1} c_n q^n \quad \text{and} \quad g^* = \sum_{n \geqslant 1, (n,6p)=1} \sigma_1(n) q^n,$$

where $\sigma_1(n)$ is the usual sum of divisors function; i.e. $\sigma_1(n) = \sum_{d|n} d$. Lemma 4.6.5 of Miyake [Mi88] ensures that f^* and g^* are weight 2 modular forms of level dividing $972p^3$. Applying Proposition 7.2 to $f^* - g^*$ and using the fact that $c_l \equiv l + 1 \pmod 3$, for all primes l, coprime to $3p$, one of the following necessarily occurs :

(i) There exists a prime l, coprime to $3p$ and satisfying $l \leqslant 324p^2(p+1)$ and $c_l \not\equiv l + 1 \pmod 3$.

(ii) $c_l \equiv l + 1 \pmod 3$ for all prime l coprime to $3p$.

In the former case, since n divides the (nonzero) integer $c_l - a_l$, we obtain the inequality

$$n \leqslant l + 1 + 2\sqrt{l} \leqslant 324p^2(p+1) + 1 + 18p\sqrt{p+1} < p^{2p}, \tag{7}$$

where the last inequality is valid for $p \geqslant 5$. In the latter situation, there necessarily exists a curve, say F, in the given isogeny class, with a rational 3-torsion point. Proposition 6.1 therefore immediately implies Theorems 1.3 and 1.4. Regarding Theorem 1.1, where $N \in \{3p^2, 9p^2, 27p^2\}$, we may apply Proposition 6.1 to conclude that F has CM by an order in $\mathbb{Q}(\sqrt{-3})$. From Proposition 4.3, it follows that $n \leqslant 13$. Combining this observation with (7) and the inequalities following (6) completes the proofs of Theorems 1.1, 1.3 and 1.4.

Corollary 1.2 is an easy consequence of Theorem 1.1, after applying a result of Darmon and Granville [DG95] (which implies, for fixed values of $n \geqslant 4$ and α, that the equation $x^n + y^n = p^\alpha z^3$ has at most finitely many solutions in coprime, nonzero integers x, y and z – note that there is no loss of generality in assuming $0 \leqslant \alpha \leqslant n - 1$). Analogous corollaries may be obtained in a straightforward fashion for Theorem 1.4 and 1.5.

8. Concluding remarks

Techniques are available to treat equation (1) for small values of the exponent n – in the case of signatures $(n, n, 2)$ or $(n, n, 3)$, the paper of Poonen [Po98] provides a good overview of such approaches (the reader may also profit from considering explicit Chabauty methods, as described in Bruin [Br99]). In case $n = 3$, the existence of infinitely many nontrivial solutions to (1) (if there are indeed any) is a classical problem, equivalent to a related elliptic curve having nonzero Mordell-Weil rank over $\mathbb{Q}$. Many papers on this subject exist, including comprehensive work, for small values of A, B, C, of Selmer (see e.g. [Sel51]). Combining these results with those of Section 1 enables one to derive slightly stronger versions of our theorems; by way of example, we can show

Theorem 8.1. *If C and n are integers with $1 \leqslant C \leqslant 5$ and $n \geqslant 3$, then the Diophantine equation $x^n + y^n = Cz^3$ has no solutions in coprime nonzero integers x, y and z with $|xy| > 1$.*

In general, as the case of p a Mersenne prime attests, the lower bound for n in Theorem 1.1 cannot be reduced to $n = o(\log p)$. Presumably a uniform bound of order $\log p$ is the true state of affairs, though a long way from being provable, with current techniques. In practice, as one may observe from the proofs of Theorems 1.5, 1.6 and 1.7, the methods of this paper yield bounds of much smaller order than those stated in Theorems 1.1, 1.3 and 1.4, at least provided we have at our disposal a set of basis elements for the Galois conjugacy classes of weight 2 newforms, at the levels of interest.

9. Acknowledgments

The authors would like to thank the anonymous referee for numerous helpful suggestions.

References

Be97 M.A. Bennett, Effective measures of irrationality for certain algebraic numbers, *J. Austral. Math. Soc.* 62 (1997), 329–344.

BS03 M.A. Bennett and C. Skinner, Ternary Diophantine equations via Galois representations and modular forms, *Canad. J. Math.*, 56 (2004), 23–54.

BVY03 M.A. Bennett, V. Vatsal and S. Yazdani, Electronic transcript of computations, http://www.math.ubc.ca/~bennett/BVY.html.

BK75 B.J. Birch and W. Kuyk (eds.), Modular functions of one variable IV, Lecture Notes in Math. 476, Berlin-Heidelberg, New York, Springer 1975.

BCDT01 C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* 14 (2001), 843–939.

Br99 N. Bruin, Chabauty methods and covering techniques applied to the generalised Fermat equation, Ph.D. Thesis, Leiden Univ. Leiden, Netherlands, 1999.

Co67 F. Coghlan, Elliptic curves with conductor $N = 2^a 3^b$, Ph.D. Thesis, Univ. Manchester, Manchester, 1967

CS71 F. Coghlan and N. Stephens, The Diophantine equation $x^3 - y^2 = k$, in Computers in Number Theory, A.O.L.Atkins and B.J. Birch (ed), Academic Press, London and New York, 1971.

Cr92 J. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, 1992.

Da93a H. Darmon, On the equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$, *Duke I.M.R.N.* 72 (1993), 263–274.

Da93b H. Darmon, The equation $x^4 - y^4 = z^p$, *C.R. Math. Rep. Acad. Sci. Canada* XV (1993), 286–290.

DG95 H. Darmon and A. Granville, On the equations $x^p + y^q = z^r$ and $z^m = f(x, y)$, *Bull. London Math. Soc.* 27 (1995), 513–544.

DM97 H. Darmon and L. Merel, Winding quotients and some variants of Fermat's Last Theorem, *J. Reine Angew. Math.* 490 (1997), 81–100.

Di96 F. Diamond, On deformation rings and Hecke rings, *Ann. of Math.* 144 (1996), 137–166.

Di95 F. Diamond, The refined conjecture of Serre, in *Elliptic Curves, Modular Forms, and Fermat's Last Theorem* (ed. J. Coates), International Press, Cambridge, MA, 1995.

El03 J. Ellenberg, Galois representations attached to Q-curves and the generalized Fermat equation $A^4 + B^2 = C^p$, *Amer. J. Math*, to appear.

Eu38 L. Euler, Theorematum quorundam arithmeticorum demonstrationes, *Comm. Acad. Sci. Petrop.* 10 (1738) (1747), 125–146.

Ha74 T. Hadano, On the conductor of an elliptic curve with a rational point of order 2, *Nagoya Math. J.* 53 (1974), 199–210.

Ha82 T. Hadano, Elliptic curves with a rational point of finite order, *Manuscripta Math.* 39 (1982), 49–79.

Iv01 W. Ivorra, personal communication.

Iv03 W. Ivorra, Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$, *Acta Arith.* 108 (2003), 327–338.

Ka90 S. Kamienny, Points on Shimura curves over fields of even degree, *Math. Ann.* 286 (1990), 731–734.

Ke79 M.A. Kenku, The modular curve $X_0(39)$ and rational isogenies, *Math. Proc. Cambridge Philos. Soc.* 85 (1979), 21–23.

Kr96 A. Kraus, Sur les équations $a^p + b^p + 15c^p = 0$ et $a^p + 3b^p + 5c^p = 0$, *C. R. Acad. Sci. Paris Sér. I Math.* 322 (1996), no. 9, 809–812.

Kr97a A. Kraus, Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique, *Dissertationes Math.* 364 (1997), 39pp.

Kr98 A. Kraus, Sur l'équation $a^3 + b^3 = c^p$, *Experiment. Math.* 7 (1998), no. 1, 1–13.

Kr97b A. Kraus, Majorations effectives pour l'équation de Fermat généralisée, *Canad. J. Math.* 49 (1997), no. 6, 1139–1161.

Kr99 A. Kraus, On the equation $x^p + y^q = z^r$: a survey, *Ramanujan J.* 3 (1999), no. 3, 315–333.

KO92 A. Kraus and J. Oesterlé, Sur une question de B. Mazur, *Math. Ann.* 293 (1992), 259–275.

Ku76 D. Kubert, Universal bounds on torsion of elliptic curves, *Proc. London Math. Soc.* (3) 33 (1976), 193–237.

Ma78 B. Mazur, Rational isogenies of prime degree, *Invent. Math.* 44 (1978) 129–162.

Me99 L. Merel, Arithmetic of elliptic curves and Diophantine equations, *J. Théor. Nombres Bordeaux* 11 (1999), 173–200.

Mi88 T. Miyake, *Modular Forms*, Springer-Verlag, Berlin and New York, 1988.

Mo84 F. Momose, Rational points on the modular curves $X_{Split}(p)$, *Comp. Math.* 52 (1984), 115–137.

Pa93 I. Papadopolous, Sur la classification de Neron des courbes elliptiques en caracteristique residuelle 2 et 3, *J. Number Th.* 44 (1993), 119–152.

Po98 B. Poonen, Some Diophantine equations of the form $x^n + y^n = z^m$, *Acta Arith.* 86 (1998), 193–205.

Ri90 K. Ribet, On modular representations of $\mathrm{Gal}(\overline{Q}/Q)$ arising from modular forms, *Invent. Math.* 100 (1990), 431–476.

Sel51 E. S. Selmer, The Diophantine equation $ax^3 + by^3 + cz^3 = 0$, *Acta Math.* 85 (1951), 203–362.

Ser87 J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. J.* 54 (1987), 179–230.

Sh71 G. Shimura, Arithmetic Theory of Automorphic Functions, Publ. Math. Soc. Japan, 1971.

Sil86 J. Silverman, *The Arithmetic of Elliptic Curves,* Graduate Texts in Math, vol. 106, Springer-Verlag, Berlin and New York, 1986.

Sil94 J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves,* Graduate Texts in Math, vol. 151, Springer-Verlag, Berlin and New York, 1994.

Sim98 SIMATH, A computer algebra system for number theoretic applications, Saarbrucken 1992–1998, simath@math.uni-sb.de

St03 W. Stein, Modular forms database, http://modular.fas.harvard.edu/Tables/

ST94 R. J. Stroeker and N. Tzanakis, Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms, *Acta Arith.* 67 (1994), 177–196.

Wi95 A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* (2) 141 (1995), no. 3, 443–551.

Michael A. Bennett bennett@math.ubc.ca
Department of Mathematics, University of British Columbia, Vancouver, B.C., V6T 1Z2 Canada

Vinayak Vatsal vatsal@math.ubc.ca
Department of Mathematics, University of British Columbia, Vancouver, B.C., V6T 1Z2 Canada

Soroosh Yazdani
Department of Mathematics, University of California, Berkeley, CA, U.S.A.